



Public Safety Assistant (PSA)

Administrator's Guide

Telepartner International

November 2001

DISCLAIMER

Information in this document is subject to change without notice. Telepartner International North America, Inc. provides this manual “as is” without warranty of any kind, either expressed or implied, but not limited to implied merchantability and fitness for a particular purpose. Telepartner International may improve or change the product at any time and without further notice; this document does not represent a commitment on the part of Telepartner International. The software described in this document is furnished under a license agreement or non-disclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

Copyright 1999-2001 Telepartner International, Inc.

All Rights Reserved Worldwide.

Can be used and copied only in accordance
with a valid license and non-disclosure agreement.

Telepartner International holds the copyright on this manual and reserves all rights. You may not copy, photocopy, translate or reduce to any electronic medium or machine-readable form any part of this document, without prior written consent from Telepartner International.

Comments and suggestions are welcome and can be directed to:

Telepartner International, Inc.
Att: Documentation Department.
Century Executive Park
100 Corporate Place
Rocky Hill, CT 06067
860-513-4060

TRADEMARKS

Public Safety Assistant - PSA, TeleServer, TeleServer Message Switch, and TeleServer Management Workstation are trademarks of Telepartner International.

Other products and names are trademarks or copyrights of their respective vendors or developers.

CONTENTS



.....	I
DISCLAIMER	II
TRADEMARKS	II
CONTENTS	I
OVERVIEW OF THE TELEPARTNER PUBLIC SAFETY ASSISTANT	1
Navigating within the PSA Application.....	2
Customizing the PSA Application	2
Viewing the Toolbar and Status Bar.....	2
Exiting the PSA Application	2
COLLECT	3
Vehicle Lookup.....	3
Stolen/Wanted/Missing Lookup.....	7
Boat Record Lookup.....	10
Gun/Article/Security Record Lookup	11
Criminal Lookup	15
Inmate Record Lookup.....	17
Judicial Protective Order Lookup.....	19
NICB Vehicle Record Lookup.....	20
Message Lookup	20
TRAFFIC STOPS	22
Searching for a Traffic Stop Report.....	22
Results for a Traffic Stop Report Search.....	23
Generating a Traffic Stop Report Summary Chart View	23
MESSAGING	25
Reading a Message	26
Composing a Message.....	26
Reviewing Messages.....	27
Filtering Your Messages.....	27
Using the History Tab.....	27
MONITORING	29

AGENCY ADMINISTRATION	30
GROUP ADMINISTRATION.....	30
Viewing Existing Groups.....	30
Adding a New Group	31
Modifying a Group	31
Deleting a Group	32
USER ADMINISTRATION	32
Viewing Existing Users.....	33
Adding a New User	33
Modifying User Properties	34
Deleting a User.....	35
MONITOR USERS	35
Forcing Off an Active User	36
DATASOURCES ADMINISTRATION	36
INBASKET ADMINISTRATION	38
Viewing Existing InBaskets.....	39
Adding a New InBasket	40
Modifying an InBasket	40
Deleting an InBasket	42
Changing the agency default InBasket.....	42
Viewing and modifying the Supervisor Watch List.....	42
Viewing and modifying the default InBasket for Officers	43
Moving Reports from one InBasket to another	44
DATA SHARING RULES ADMINISTRATION	44
Viewing and Modifying Data Sharing Rules	44
SYSTEM ADMINISTRATION	46
ADMINISTRATORS.....	46
Adding an Administrator	47
Deleting an Administrator	47
SECURITY ROLES.....	48
Adding a Security Role.....	48
Modifying a Security Role.....	48
Deleting a Security Role.....	49
AGENCY ADMINISTRATION	49
Adding a New Agency	49
Modifying an Agency	50
Deleting an Agency	50
VIEW PRIVILEGES.....	50
MONITOR SWITCH	51
GLOBAL DATASOURCE ADMINISTRATION	52
Adding a DataSource Type to a Global DataSource Logon ID	53
Deleting a Global DataSource Logon ID or DataSource Type	53
MANAGEMENT REPORTS	54
REPORT SEARCH	54
READING A REPORT	56
Report Search Query Results	56
View Incident Summary.....	56
Reports Search Incident Details.....	57
Report Search Events For This Record	58
List of Report Events	58
REPORT BY OFFICER.....	59
Report by Officer Search Query Results	60
Report by Officer Search Incident Details	61

Report by Officer Search Incident Details	62
Report by Officer Search Record Events	62
COMMON SEARCHES	63
Common Search Query Results	64
Common Search Incident Details	65
Common Search Incident Details	66
Narrative – from report filed Common Search Report Events	66
OFFICER EVENTS	67
Officer Events Query Results	67
Officer Event Incident Details	68
Officer Event Incident Events	69
Officer Event Report Events	69
Officer Activity Summary	70
Officer Activity Summary Query Results	70
AUDIT COLLECT	71
Audit COLLECT Query Results	72
AUDIT MESSAGING	72
Audit Messaging Query Results	73
AUDIT OFFICER ACTIVITY	74
Audit Officer Activity Query Results	75
AGENCY ACTIVITY SUMMARY	75
Audit Agency Activity Query Results	76
PSA MESSAGES	77

OVERVIEW OF THE TELEPARTNER PUBLIC SAFETY ASSISTANT

Telepartner's Public Safety Assistant (PSA™) software product is a browser-based suite of utilities with a common look and feel that assist public safety agencies in the daily operation of the CAPTAIN system.

The PSA application uses a two-paned window to present the entire suite of applications in one main window. The left pane contains a navigation bar that provides menu access to all the utilities available in the PSA suite. The right pane serves as a workspace for the utility windows.

The navigation bar has seven main menus that let you access the PSA suite of utilities:



- **COLLECT** – allows an agency to query license, vehicle and boat registration information; NIB vehicle records; guns, articles and securities; stolen vehicles, boats, plates, wanted persons, missing persons; protective orders; criminal records; inmate information, and messages.
- **Traffic Stops** – allows an Agency to search, display, and print traffic stop information
- **Messaging** – allows an Agency to send, receive, and view messages from all users logged onto the TeleServer Message Switch.
- **Monitoring** – allows an Agency to monitor the activity of users on the TeleServer Message Switch. Note: In this release only Messaging is supported.
- **Agency Administration** – allows an Agency Administrator to manage users and groups, monitor the users, and manage external Agency DataSources on the TeleServer Message Switch.
- **System Administration** – allows a System Administrator to manage all Agencies, security roles, privileges, and external global DataSources, and also monitor events on the TeleServer Message Switch.
- **Management Reports** – allows an Agency to search, display, and print audit log information relating to incident and accident reports, and warrants. It is also a useful administration tool for managing individual incident and accident reports and warrants.

Navigating within the PSA Application

In addition to using the navigation bar to move between the PSA utilities, you can use the PSA Navigator window.



➔ **To access the PSA Navigator:**

- Press **F2** or choose Navigator from the Windows menu. Click a utility to jump to that utility.

Customizing the PSA Application

You can customize the main window of the PSA application in several ways.

Resizing the Navigation Bar Pane

You can resize the navigation bar to provide more desktop space for the right pane window, which can be particularly important when you're monitoring a large amount of information.

➔ **To resize the navigation bar:**

- Hold the cursor over the bar separating the two panes until it changes to a 2-headed arrow, and click and drag to resize the window.

Viewing the Toolbar and Status Bar

You can show or hide both the toolbar and the status bar using a command on the View menu. Hiding these objects increases the display area available in the main window.

➔ **To show/hide the toolbar and status bar:**

- Choose Toolbar or Status Bar from the View menu to show or hide either object. When a checkmark displays next to either menu item, the associated object displays on the main menu.

Exiting the PSA Application

➔ **To exit the PSA application:**

- Choose Exit from the File menu.

COLLECT

The **COLLECT** utility is a graphical user interface into Connecticut's On-Line Law Enforcement Communications Teleprocessing (COLLECT) system for the most common queries.



The COLLECT Lookup queries are:

- license and vehicle registration information
- wanted or missing persons; stolen vehicles, plates, or boats
- boat registration and out-of-state boat information
- guns, articles, and securities
- criminal records, in CT only, by name or SPBI number
- inmate information by name, SSN, or inmate number with mugshot
- judicial protective orders, by name or by docket number
- shipping, export, impound, salvage, and international index files
- messages sent less than eight weeks ago

Vehicle Lookup

The Vehicle Lookup submenu lets you query vehicle information from the motor vehicle files and from the COLLECT and NCIC person and vehicle files. You can make queries by registration number, by vehicle identification number (VIN), by vehicle owner, by operator number, or by operator name.



You can query motor vehicle, COLLECT, and NCIC person and vehicle files for:

- vehicle registration information
- vehicle ID information
- vehicle owner information
- driver's name information
- driver's license number information

➔ **To perform a Vehicle Lookup by registration:**

1. In the navigation window on the window, click COLLECT, then click Vehicle Lookup.
2. Click the By Registration link.

 A dark blue form titled "Vehicle Lookup By Registration" in yellow. It contains four input fields: "Reg:" (text), "Type:" (dropdown), "State:" (dropdown), and "Year:" (text with "(yyyymmdd)" to its right). Below the fields are two buttons: "Submit" and "Reset".

3. In the *Vehicle Lookup By Registration* screen, enter the vehicle registration number in the *Reg* field (a required field).
4. Enter any additional information about the vehicle:
 - Click the *Type* down arrow and select the type of the vehicle from the drop-down list (e.g., AM=Ambulance, CO=Commercial, and FM=Farm).
 - Click the *State* down arrow and select the state that issued the registration number from the drop-down list.
 - In the *Year* field, enter the year the registration was issued, as a 4-digit date, a 2-digit month, and a 2-digit day (YYYYMMDD) format.
5. Click the **Submit** button.

PSA displays motor vehicle information about the specified registration number.

➔ **To perform a Vehicle Lookup by Vehicle ID (VIN):**

1. In the navigation window on the window, click COLLECT, then click Vehicle Lookup.
2. Click the *By VIN* link.

Vehicle Lookup By Vehicle ID

VIN: Make:

State: Year: (yyyymmdd)

3. In the *Vehicle Lookup by Vehicle ID* screen, enter the vehicle ID number in the *VIN* field (a required field).
4. Enter any additional information about the vehicle:
 - Click the *State* down arrow and select the state that issued the registration number from the drop-down list.
 - Click the *Make* down arrow and select the type of the vehicle from the drop-down list (e.g., AM=Ambulance, CO=Commercial, and FM=Farm).
 - In the *Year* field, enter the year the registration was issued, as a 4-digit date, a 2-digit month, and a 2-digit day (YYYYMMDD) format.
5. Click the Submit button to run your query.

PSA displays motor vehicle information about the specified VIN number.

➔ **To perform a Vehicle Lookup by owner:**

1. In the navigation window on the window, click COLLECT, and then click Vehicle Lookup.
2. Click the By Owner link.

Vehicle Lookup By Owner

Name (Last,First): [View previous entries](#)

DOB: (yyyymmdd)

Sex:

- In the *Vehicle Lookup by Owner* screen, enter the name of the vehicle owner, last name first (a required field).

Note: Click the **View previous entries** button to open a window displaying any names that have already been used in a *By Owner* search. Click a name in this window to insert it in the Name field.

- Enter any additional information about the vehicle owner:
 - In the *DOB* field, enter the Date of Birth of the vehicle owner, in a 4-digit year, 2-digit month, and 2-digit day (YYYYMMDD) format.
 - Click the *Sex* down arrow and select the gender of the owner from the drop-down list.
- Click the **Submit** button to run your query.

PSA displays motor vehicle information about the specified vehicle owner.

➔ **To perform a Vehicle Lookup by driver's name:**

- In the navigation window on the window, click COLLECT, then click Vehicle Lookup.
- Click the By Name link.

Driver Lookup By Name

Name (Last,First): **DOB:** (yyyymmdd)

State: **Sex:**

3. In the *Driver Lookup by Name* screen, enter the name of the vehicle driver, last name first (a required field).
4. Enter any additional information about the vehicle driver:
 - In the *DOB* field, enter the Date of Birth of the vehicle owner, in a 4-digit year, 2-digit month, and 2-digit day (YYYYMMDD) format.
 - Click the *State* down arrow and select the state in which the driver holds a driver's license from the drop-down list.
 - Click the *Sex* down arrow and select the gender of the driver from the drop-down list.
5. Click the **Submit** button to run your query.

PSA displays motor vehicle information about the specified vehicle driver.

➔ **To perform a Vehicle Lookup by driver's license:**

1. In the navigation window on the window, click COLLECT, then click Vehicle Lookup.
2. Click the By License link.

3. In the *Driver Lookup by License* screen, enter the operator license number (*OLN*) of the vehicle driver (a required field).
4. Enter any additional information about the vehicle driver:
 - Click the *State* down arrow and select the state that issued this driver's license from the drop-down list.
5. Click the **Submit** button to run your query.

PSA displays motor vehicle information about the specified driver's license.

Stolen/Wanted/Missing Lookup

The Person/Vehicle/Boat Lookup submenu lets you query COLLECT data regarding wanted and missing persons, and stolen vehicles, plates, and boats.

➔ **To perform a person, vehicle, or boat information lookup:**

1. In the navigation window on the left, click COLLECT, then click Stolen/Wanted/Missing.

Person/Vehicle/Boat Lookup

Person Lookup

Name: DOB: Sex: Race:
 SOC: Operator License: MISC: FBI:
 ZIP: Street:

Vehicle Lookup

Veh-Reg: Type: State:
 Exp-date: Year: Make:
 Model: Style:

Boat Lookup

Boat-Reg: Type: State: Exp-date:
 Year: Make: Length: Color:
 BHN:

ORI: Case No: Date Entered:

**Message#:

2. In the *Person/Vehicle/Boat Lookup* screen, enter any missing, wanted, and/or stolen data for the type of query you're running:

For a missing or wanted person lookup:

- In the *Name* field, enter the name of the person, last name first.
- In the *SOC* field, enter the person's Social Security Number (xxx-xx-xxxx).
- In the *ZIP* field, enter the zip code of the person's street address.
- In the *DOB* field, enter the person's date of birth, in 4-digit year, 2-digit month, and 2-digit day (YYYYMMDD) order.
- In the *Operator License* field, enter the person's driver's license number.
- In the *Street* field, enter the person's street address.
- Click the *Sex* down arrow and select the person's gender from the drop-down list.
- In the *MISC #* field, enter a number pertaining to the person, such as a selective service number, a passport number, an alien registration number, or a motor vehicle ID card number.
- In the *Race* field, enter the person's ethnic origin: black, white, Indian (American or Alaskan), Asian or Pacific Islander, or unknown
- In the *FBI* field, enter the number issued by the FBI for a past criminal record.

For a stolen vehicle lookup:

- In the *Veh-Reg* field, enter the vehicle's motor vehicle registration number.
- In the *Exp-Date* field, enter the expiration date of the vehicle's registration..
- In the *Model* field, enter the vehicle model name or number.
- Click the *Type* down arrow and select the vehicle type from the drop-down list (e.g., AM=Ambulance, CO=Commercial, and FM=Farm).
- In the *Year* field, enter the model year of the vehicle as a 4-digit year.
- In the *Style* field, enter the style of the vehicle (e.g., 2-door or 4-door).
- Click the *State* down arrow and select the state that issued the vehicle's registration from the drop-down list.
- Click the *Make* down arrow and select the manufacturer of the vehicle from the drop-down list.

For a stolen boat lookup:

- In the *Boat-Reg* field, enter the boat's state registration number.
 - In the *Year* field, enter the model year of the boat.
 - Click the *Type* down arrow and select the boat's type from the drop-down list.
 - In the *Make* field, enter the make of the boat.
 - In the *BHN* field, enter the boat's Boat Haul Number.
 - Click the *State* down arrow and select the state that issued the boat's registration from the drop-down list.
 - In the *Length* field, enter the length of the boat, in feet.
 - in the *Exp-Date* field, enter the expiration date of the boat's registration.
 - In the *Color* field, enter the main color of the boat.
3. At the bottom of the screen, in the *ORI* field, enter the Originating Agency ID.
 4. In the *Case No.* field, enter the case number or a comment stating why this lookup is being performed.
 5. In the *Date Entered* field, enter today's date.
 6. In the *Message #* field, enter the 7-digit number identifying the record in COLLECT (required field).
 7. Click the **Submit** button to run your query.

PSA displays the available data regarding the missing or wanted person, or the stolen vehicle or boat.

Boat Record Lookup

The Boat Lookup utility lets you query boat registration information by name, state, registration number, and boat haul number (BHN).



You can:

- query NLETS boat registration data by boat and owner information.
- query NCIC boat registration data by boat haul number.

➔ **To perform an NLETS Registration Boat Lookup:**

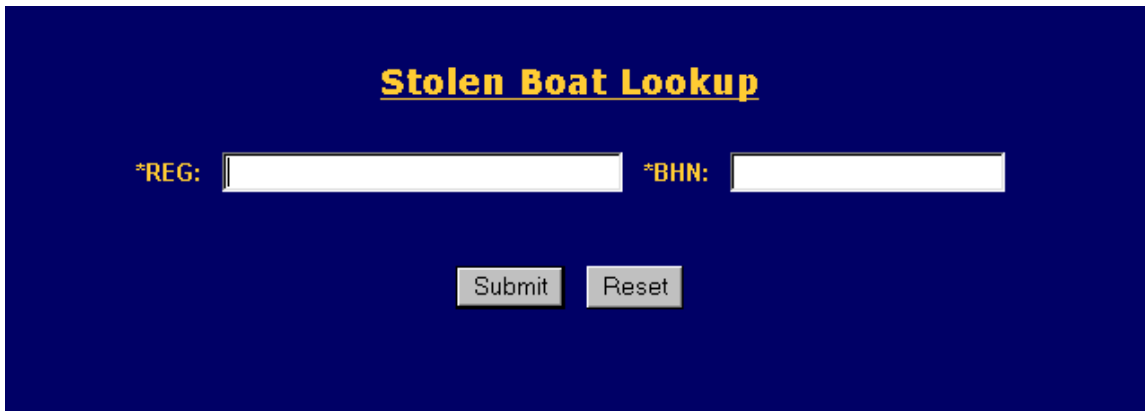
1. In the navigation window on the left, click COLLECT, then click Boat Lookup.
2. Click the NLETS Registration link.

3. In the *Boat Registration Lookup* screen, enter the required information:
 - In the *Name* field, enter the name of the registered owner of the boat.
 - Click the *State* down arrow and select the state in which the boat is registered from the drop-down list.
 - In the *BHN* field, enter the Boat Haul Number for this boat.
 - In the *Reg* field, enter the boat's state registration number.
4. Enter any additional information about the boat's owner:
 - In the *DOB* field, enter the Date of Birth of the boat's registered owner, in 4-digit year, 2-digit month, and 2-digit day (YYYYMMDD) order.
5. Click the **Submit** button to run your query.

PSA displays the available NLETS information about the specified boat.

➔ **To perform an NCIC Stolen Boat Lookup:**

1. In the navigation window on the left, click COLLECT, then click Boat Lookup.
2. Click the NCIC Stolen Boat link.



3. In the *Stolen Boat Lookup* screen, enter the required information:
 - In the *REG* field, enter the boat's state registration number.
 - In the *BHN* field, enter the Boat Haul Number for this boat.
4. Click the **Submit** button to run your query.

PSA displays the available NCIC information about the specified boat.

Gun/Article/Security Record Lookup

The Gun/Article/Security Lookup utility lets you query gun, article, or security information. You can also make inquiries on modus operandi (MO), case number, or by system message number.



You can:

- query by gun serial number and other information.
- query by article information.
- query by security or cash information.
- query by modus operandi (MO) information

- query by case number
- query by system message number.

➔ **To perform a gun lookup:**

1. From the navigation window, click COLLECT, then Gun/Article/Security Lookup.
2. Click the Gun link.

Gun Lookup

Serial#:

Make: Sort by Code
 Sort by Description

CAL:

3. In the *Gun Lookup* screen, enter the serial number of the gun (required field).
4. Enter any additional gun information you have available:
 - To enter the make of the gun, click the appropriate radio button (*Sort by Code* or *Sort by Description*). Then click the *Make* down arrow and select the appropriate gun make (either a code or a description) from the drop-down list.
 - Click the *CAL* down arrow and select the gun's caliber from the drop-down list.
5. Click the **Submit** button to run your query.

The available data about the gun displays.

➔ **To perform an article lookup:**

1. From the navigation window, click COLLECT, then Gun/Article/Security Lookup.
2. Click the Article link.

Article Lookup

Serial#:

Type: Sort by Code Sort by Description

3. In the *Article Lookup* screen, enter the required information:
4. In the *Serial* field, enter the serial number of the article.
5. To enter the type of the article, click the appropriate radio button (*Sort by Code* or *Sort by Description*). Then click the *Type* down arrow and select the appropriate article type (either a code or a description) from the drop-down list.
6. Click the **Submit** button to run your query.

PSA displays the available data about the article.

➔ **To perform a security lookup for stolen money:**

1. From the navigation window, click COLLECT, then Gun/Article/Security Lookup.
2. Click the Security link.

3. In the *Security Lookup* screen, enter the required information:
 - In the *Serial* field, enter the serial number of the security note.
 - Click the *Type* down arrow and select the security type from the drop-down list.
4. Enter any additional security information you have available:
 - In the *DEN* field, enter the denomination of the stolen bills.
5. Click the **Submit** button to run your query.

PSA displays the available data about the security or bills.

➔ **To perform an MO lookup:**

1. From the navigation window, click COLLECT, then Gun/Article/Security Lookup.
2. Click the By MO link.

Gun Article Security Lookup By MO

AreaOfTheft: **Method:**

Point: **Instrument:**

3. In the *Gun Article Security Lookup by MO* screen, click the *Area Of Theft* down arrow and select the location of the theft from the drop-down list (required field).
4. Enter any additional information about the theft you have available:
 - Click the *Point* down arrow and select the point of entry from the drop-down list.
 - Click the *Method* down arrow and select the method from the drop-down list.
 - Click the *Instrument* down arrow and select the instrument used in the theft from the drop-down list.
5. Click the **Submit** button to run your query.

PSA displays the available data about the MO.

➔ **To perform a case number lookup:**

1. From the navigation window, click COLLECT, then Gun/Article/Security Lookup.
2. Click the By Case Number link.

Gun Article SecurityLookup By Case No

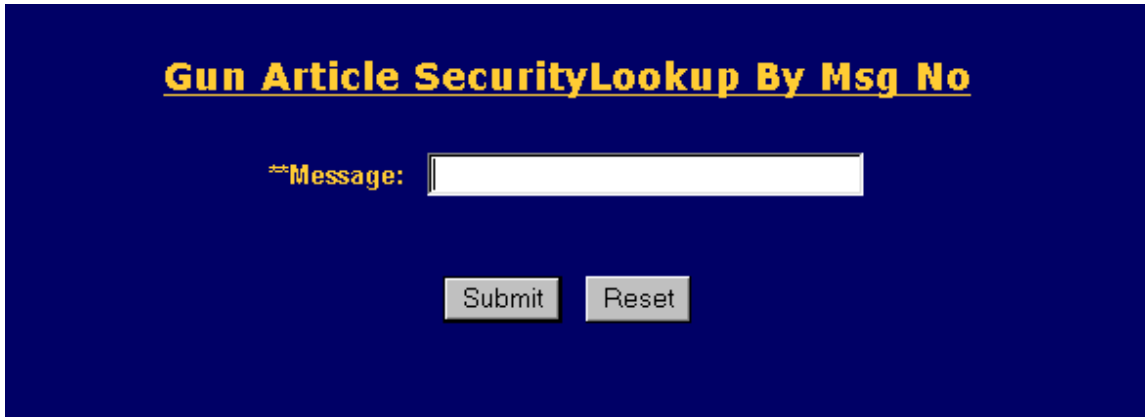
***LCL** ***ORI**

3. In the *Gun Article Security Lookup By Case No* screen, enter the required information:
 - In the *LCL* field, enter the case number of gun, article, or security lookup.
 - In the *ORI* field, enter the originating Agency's ID number.
4. Click the **Submit** button to run your query.

PSA displays the available data about the case number.

➔ **To perform a message number lookup:**

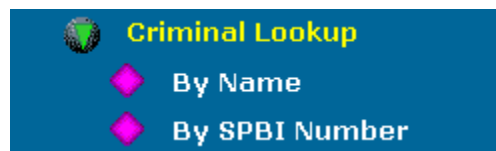
1. From the navigation window, click COLLECT, then Gun/Article/Security Lookup.
2. Click the By Msg Number link.



3. In the *Gun Article Security Lookup By Msg No* screen, enter the desired message number (required field).
 4. Click the **Submit** button to run your query.
- PSA displays the available data about the message.

Criminal Lookup

The Criminal Lookup allows you to query criminal record in CT only by name or SPBI number.



You can:

- query criminal records by name.
- query criminal records by SPBI number.

➔ **To perform a criminal information lookup by name:**

1. From the navigation window, click COLLECT, then Criminal Lookup.
2. Click the By Name link.

Criminal Info Lookup By Name

**Name (Last,First):

**DOB (yyyymmdd): OR Year Of Birth

**Requester (Last,First):

**Operator (Last):

**Case No. Comment:

3. In the *Criminal Info Lookup By Name* screen, enter the required information:
 - In the *Name* field, enter the individual's name, last name first.
 - in the *DOB* field, enter the individual's date of birth, in 4-digit year, 2-digit month, and 2-digit day (YYYYMMDD) order.
 - In the *Requester* field, enter the name, last name first, of the person who requested this criminal lookup.
 - In the *Operator* field, enter the name, last name first, of the person performing this criminal lookup.
 - In the *Case No. Comment* field, enter the case number or a comment stating why this criminal lookup is being performed.
4. Enter any additional information you have about the individual:
 - In the OR Year of Birth field, enter the individual's year of birth, if you don't know the date of birth.
5. Click the **Submit** button to run your query.

PSA displays the available data about the specified individual.

➔ **To perform a criminal information lookup by SPBI number:**

1. From the navigation window, click COLLECT, then Criminal Lookup.
2. Click the By SPBI Number link.

Criminal Info Lookup By SPBI

SPBI : Requester:

Operator: CaseNO:

3. In the *Criminal Info Lookup By SPBI* screen, enter the required information:
 - In the *SPBI* field, enter the state police ID number.
 - In the *Operator* field, enter the name, last name first, of the person performing this criminal lookup.
 - In the *Requester* field, enter the name, last name first, of the person who requested this criminal lookup.
 - In the *Case NO* field, enter the case number or a comment stating why this criminal lookup is being performed.

4. Click the **Submit** button to run your query.

PSA displays the available SPBI data about the specified individual.

Inmate Record Lookup

The Inmate Lookup utility lets you query inmate information by name, SSN, or inmate number with mugshot.



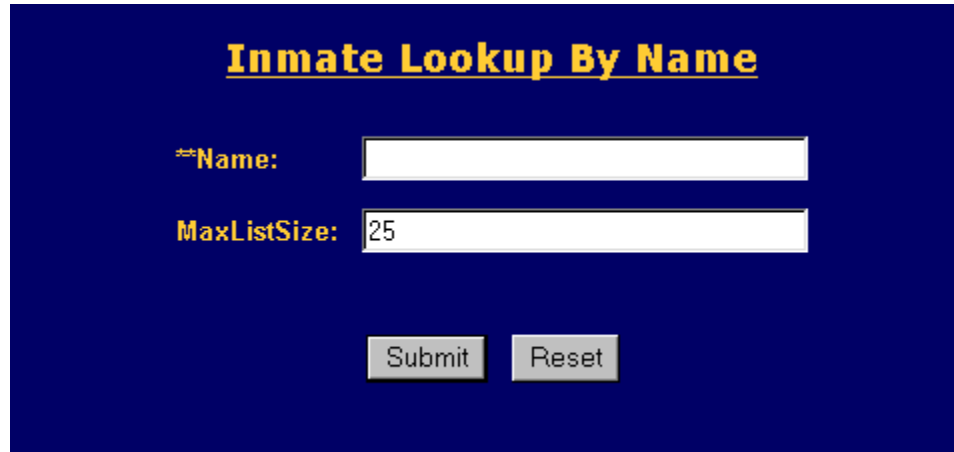
You can:

- query by name
- query by Social Security Number
- query by photo ID

➔ **To perform an inmate information lookup by name:**

1. In the navigation window on the left, click COLLECT, then Inmate Lookup.

2. Click the [By Name](#) link.



Inmate Lookup By Name

Name:

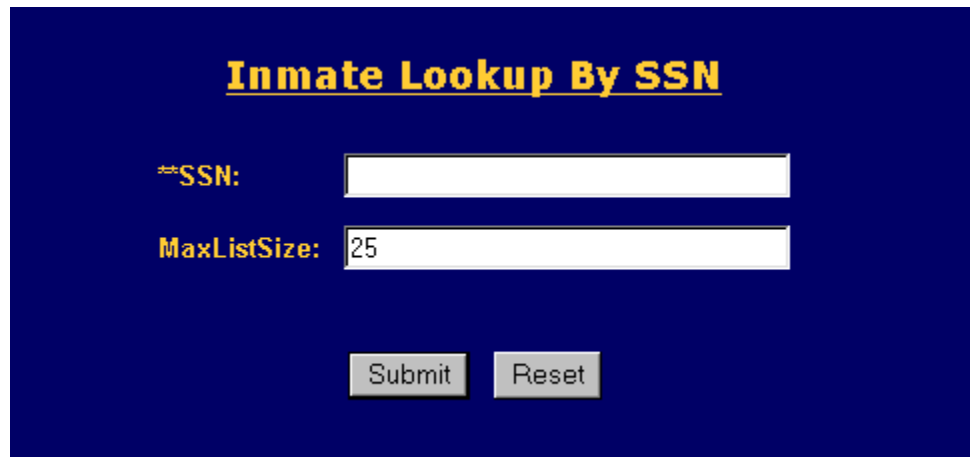
MaxListSize:

3. In the *Inmate Lookup By Name* screen, enter the inmate's name in the *Name* field (required field).
4. Enter any additional information available:
 - In the *MaxListSize* field, enter the maximum number of records to retrieve.
5. Click the **Submit** button to run your query.

PSA displays the available inmate data.

➔ **To perform an inmate information lookup by Social Security Number:**

1. In the navigation window on the left, click [COLLECT](#), then [Inmate Lookup](#).
2. Click the [By SSN](#) link.



Inmate Lookup By SSN

SSN:

MaxListSize:

3. In the *Inmate Lookup By SSN* screen, enter the inmate's Social Security Number in the *SSN* field (required field).
4. Enter any additional information available:
 - In the *MaxListSize* field, enter the maximum number of records to retrieve.
5. Click the **Submit** button to run your query.

PSA displays the available inmate data.

➔ **To perform an inmate information lookup by photo ID:**

1. In the navigation window on the left, click COLLECT, then Inmate Lookup.
2. Click the By PhotoID link.

3. In the *Inmate Photo ID Lookup* screen, enter the inmate's number in the *InmateNo* field (required field).
4. Click the **Submit** button to run your query.

PSA displays the available inmate data.

Judicial Protective Order Lookup

The Judicial Protective Order Lookup utility lets you query protective orders by name or by docket number.

➔ **To perform a Judicial Protective Order information lookup:**

1. In the navigation window on the left, click COLLECT, then Judicial Protective.

2. In the *Judicial Protective Order Lookup* screen, enter the required information:
 - In the *Name* field, enter the individual's name.

- In the *DOB* field, enter the individual's Date of Birth , in 4-digit year, 2-digit month, and 2-digit day (YYYYMMDD) order.
 - In the *Docket* field, enter the court case docket number.
3. Enter any additional information available:
 - Click the *Sex* down arrow and select the individual's gender from the drop-down list.
 4. Click the **Submit** button to run your query.
- PSA displays the available Protective Order data.

NICB Vehicle Record Lookup

The NICB Vehicle Record Lookup utility lets you query NICB's shipping, export, impound, salvage, and international index files for vehicle information.

➔ **To perform an NICB vehicle record lookup:**

1. In the navigation window on the left, click COLLECT, then click NICB Vehicle Record.



The screenshot shows a dark blue background with the title "Vehicle Record File Lookup" in yellow text. Below the title, there are two input fields: "VIN:" followed by a text box, and "SEL:" followed by a dropdown menu. At the bottom, there are two buttons: "Submit" and "Reset".

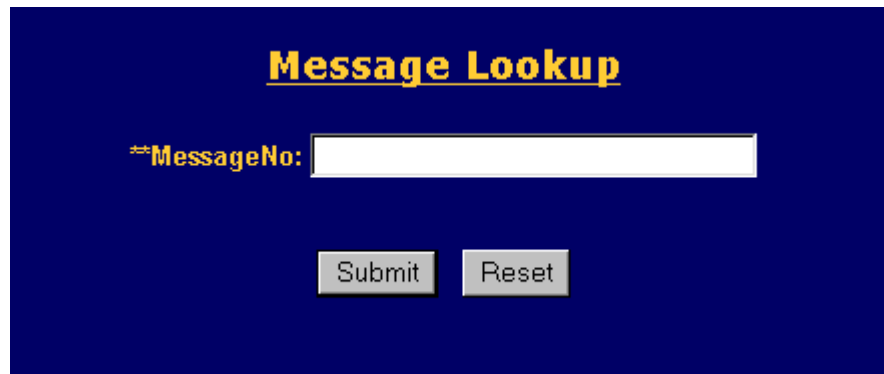
2. In the *Vehicle Record File Lookup* screen, enter the vehicle ID (VIN) number in the *VIN* field (required field).
 3. Enter any additional information available:
 - In the *SEL* field, enter Y to include shipping, salvage, and international files in the query.
 4. Click the **Submit** button to run your query.
- PSA displays the NICB vehicle data.

Message Lookup

The Message Lookup utility lets you query a message sent less than eight weeks ago.

➔ **To perform a message information lookup:**

1. In the navigation window on the left, click COLLECT, then click Message Lookup.



Message Lookup

MessageNo:

2. In the *Message Lookup* screen, enter the message number in the *MessageNo* field (required field).
2. Click the **Submit** button to run your query.

PSA displays the available message data.

TRAFFIC STOPS

The Traffic Stops utility allows a PSA user to query and generate traffic stop reports.



Traffic Stop utility options include:

- Search Traffic Stop reports by date.
- Generate Traffic Stop Totals report.

Searching for a Traffic Stop Report

The Search Traffic Stop Report option lets you search for specific Traffic Stop reports.

➔ **To perform a Traffic Stop report search:**

1. In the navigation window on the left, click [Traffic Stop](#), then click [Search Traffic Stop Report](#).

2. In the *Search Traffic Stop Reports* screen, enter the search criteria to retrieve specific reports.
 - In the *Start Date/Time* field, enter the beginning date of the traffic stop reports to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
 - In the *End Date/Time* field, enter the ending date of the traffic stop reports to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
3. Click the **Submit** button to search for the report(s) with the specified dates.

Results for a Traffic Stop Report Search

The Search Traffic Stop Report results displays statistics on the following data items mandated by the P.A. 99-198.

These data items are:

UserID	CAPTAIN user ID	*
	<i>User ID is only available to originating agency</i>	
Date	Incident Date	
Event	Event number associated with traffic stop	
Race	Asian, Black, American Indian/Alaskan, White, Unknown	
Ethnicity	Hispanic, Not Hispanic, Unknown	
Age	Individuals age	
Gender	Male, Female, Unknown	
Stop Nature	Investigation, Violation, Equipment	
Search	Yes, No	
Disposition	Infraction, Misdemeanor, No Disposition, UAR, Verbal Warning, Written Warning	
Entry Source	Dispatch, Mobile Data Terminal, Paper, Stand alone PC	
ORI	Department/ORI # originating the report	
Town	Town in which the incident occurred	

Generating a Traffic Stop Report Summary Chart View

The Traffic Stop Report Summary Chart View option lets you generate a Traffic Stop Totals report in chart format.

➔ **To generate a Traffic Stop racial totals report:**

1. In the navigation window on the left, click [Traffic Stop](#), then click [Generate Traffic Stop Totals](#).

Traffic Stop Report Summary Chart View

Enter search criteria

Start Date/Time: / / :

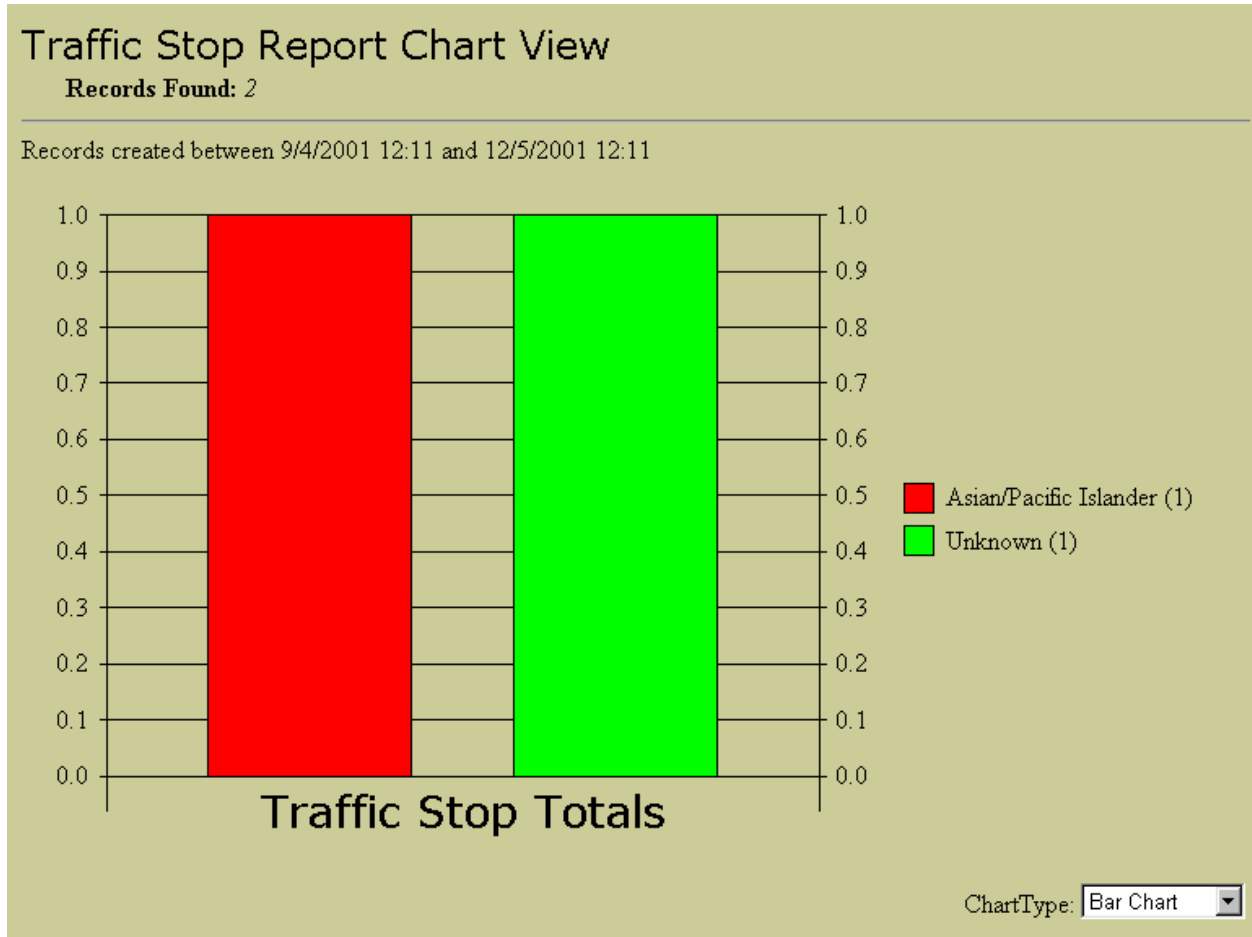
Date/Time format: MM/DD/YYYY hh:mm

End Date/Time: / / :

2. In the *Search Traffic Reports Summary Chart View* screen, enter the information required to generate a report.

- In the *Start Date/Time* field, enter the beginning date of the traffic stops to include in the report, in MM/DD/YYYY format and the time in HH:MM format.
 - In the *End Date/Time* field, enter the ending date of the traffic stops to include in the report, in MM/DD/YYYY format and the time in HH:MM format.
3. Click the **Submit** button to generate the racial totals report.

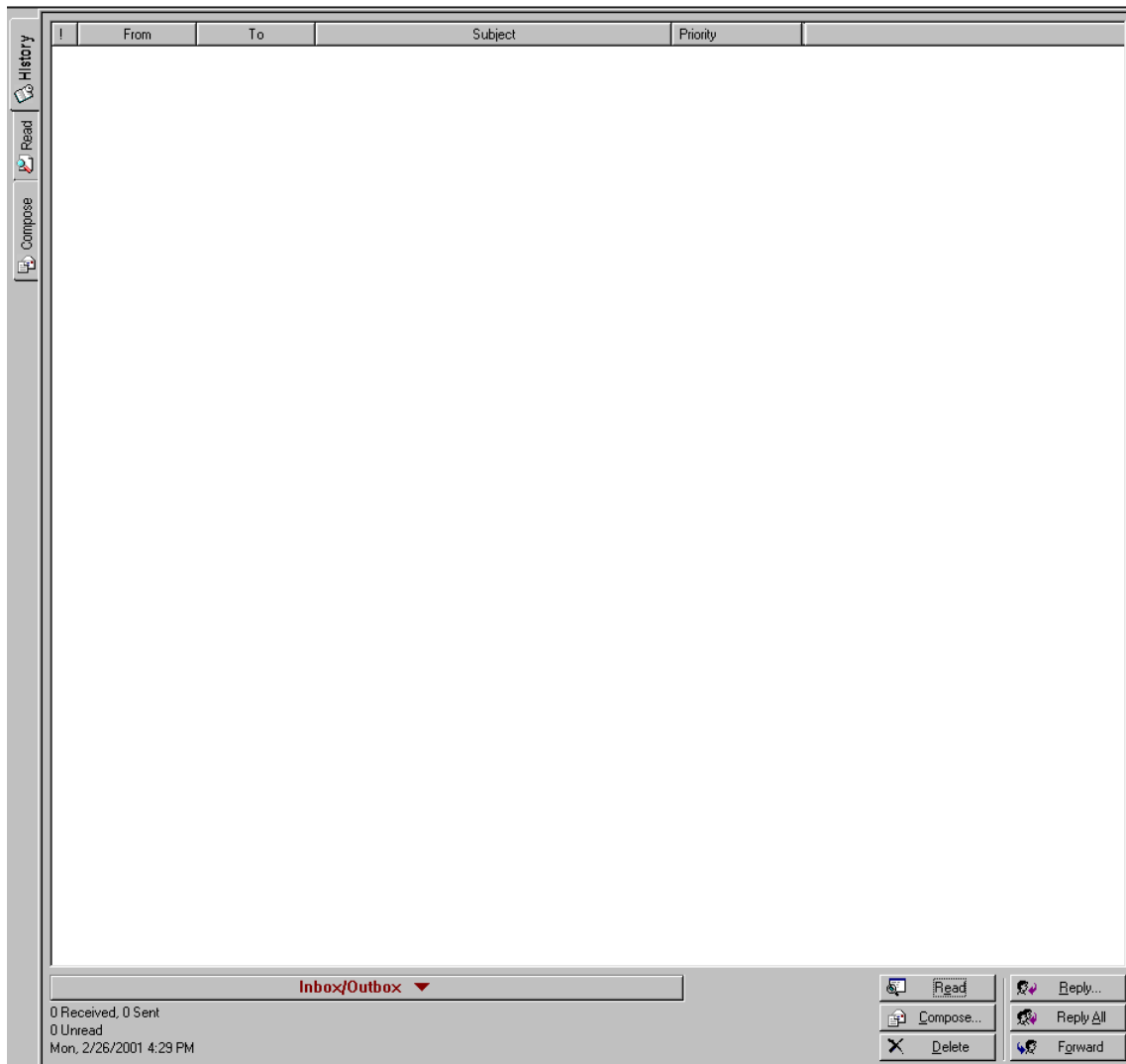
The Search Traffic Stop Report results displays the totals in a chart:



In addition the totals can be displayed in 3D Bar Chart or a Pie Chart by clicking on the ChartType.

MESSAGING

The Messaging utility allows you to send messages, receive messages, and view messages from all users logged onto the TeleServer Message Switch.



The Messaging window contains three tabs on the left-hand side that let you

- compose messages
- read messages
- view a list of messages, both sent and received, and filter your messages

Choose Messaging in the Navigation bar to access the *Messaging* window.

Reading a Message

The Read window displays the contents of a message.

From the History tab, you can read any message:

- double-click a message
- select a message and click the Read button
- select a message and click the Read tab

The Read tab provides all the Messaging functionality of the History tab through the **Forward**, **Reply**, and **Reply All** buttons.

In addition, you can click the **Previous** and **Next** buttons at the bottom left of the window to scroll through your messages.

By changing the message View in the History tab (by selecting a View from the *Inbox/Outbox* drop-down list), you can scroll through all your messages, all the messages you've received, or the entire message you've sent

Select a message and click the **Delete** button to remove it from the system.

Composing a Message

To compose a message:

1. Click the Compose tab at the left of the window to access the Compose window. The top window displays a list of everyone who's logged into the same TeleServer Message Switch.
2. Double-click Everyone to open a list of Agencies, and double-click an Agency to open a list of the available units for that Agency. Only units currently logged onto the TeleServer Message Switch display in this list.
3. Select your recipients. Click the box next to a unit, or select a unit and click the **Add** button, to send a message to that unit. Click the box next to an Agency, or select the Agency and click the **Add** button, to send the message to every unit logged in for that Agency. The *To:* field is automatically filled in, based on your selection(s). You can send a message to multiple recipients. Click the box again, or select a recipient and click the **Remove** button, to remove a unit from the To list.
4. Type a message heading in the Subject box.
5. Type your message in the Message Body box.
6. Click the **Send** button to send your message.







Other options:

- Click the **Refresh** button to refresh the list of units logged into the TeleServer Message Switch. The Agency list will close; double-click the Agency to reopen the list and view the active online units.
- Click the **Clear** button to delete your subject and message text and all the checkmarks next to the recipients you've selected.

Reviewing Messages

Once you've sent a message, and as soon as you've received a message, the message displays in the History tab of the Messaging utility window. Click the History tab to view all the messages you've sent and received.

Messages display in a list in descending chronological order, with the latest message displayed first. The first column in the History table indicates the status of the message.

	Message received but not read
	Priority message received but not read
	Message read
	Message read and replied to
	Message read and forwarded
	Message sent by dispatcher

The rest of the message History table contains additional information about each message.

From	Sender of the message
To	Recipient(s) of the message
Subject	Subject header of the message
Priority	Priority of the message

Filtering Your Messages

You can select which message type(s) displays in the list of messages in the History tab by using the Inbox/Outbox drop-down list to select a message View. You can view all your messages, all the messages you've received, or all the messages you've sent.

To filter your messages:

- Click the *Inbox/Outbox* down arrow and select the type of message you want to view in the History tab:
 - Inbox Only – messages you have received
 - Inbox/Outbox – messages you've both sent and received
 - Outbox Only – messages you've sent

Using the History Tab

The History tab gives you all the functionality of an email system in terms of replying, forwarding, and reading messages. The only difference is that you can only send messages to people who are currently logged onto the TeleServer Message Switch. The Messaging utility is a Messaging system rather than a true Email system.

To read/send messages from the History tab:

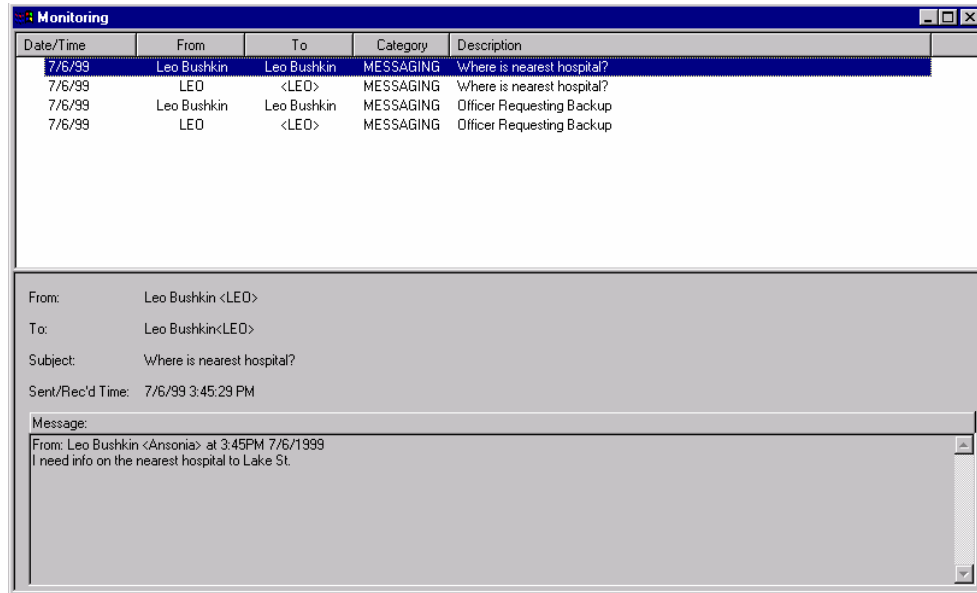
1. Double-click a message, select it and click the **Read** button, or select it and click the Read tab to read it. The Read tab opens with the contents of the message displayed.
2. Select a message and click **Reply** to send a message back to the sender. The Compose tab opens with the sender in the To box.
3. Select a message and click **Reply All** to send a message back to the sender as well as all the recipients of the selected message. The Compose tab opens with the sender in the To box and all the recipients in the CC: box.
4. Select a message and click the **Forward** button to forward the message to another unit. The Compose tab opens with the current message copied to the Message Body box.

Other options:

- Click the **Compose** button to open the Compose tab and create a new message.
- Select a message and click the **Delete** button to delete the selected message.

MONITORING

The Monitoring utility enables an agency to monitor the activity of users on the TeleServer Message Switch. In this release only Messaging is supported.



➔ To monitor messages:

In the navigation window on the left, click Monitoring.

The messages that have been sent display in a chronological list, with the most recent messages displayed first. The Monitor window displays the following information about each message:

Date/Time	Date/time the message was sent or received
From	Sender of the message
To	Recipient(s) of the message
Category	The type of event. In this release, the only category supported is Messaging
Description	A brief description of the event. For Messaging events, displays the subject header of the message

Select a message to read the contents of the message in the lower pane of the Monitoring window.

AGENCY ADMINISTRATION

The Agency Administration utility enables an Agency Administrator to manage users and groups on the TeleServer Message Switch (TMS). An Agency Administrator must have the appropriate security roles and privileges assigned to its user ID.

Note: To add an Agency Administrator, the System Administrator must define that user as an Agency Administrator using the System Administration utility.



Agency Administration utility options are:

- Manage the groups defined in the TeleServer Message Switch for the Agencies you are authorized to administer.
- Manage the users of the TeleServer Message Switch for the Agencies you are authorized to administer.
- Monitor the users who are actively using the TeleServer Message Switch for the Agencies you are authorized to administer.
- Manage external DataSources to the TeleServer Message Switch, such as an Agency's CAD and/or RMS systems.

Group Administration

The Group Administration utility lets you manage the user groups defined in the TeleServer Message Switch for those Agencies you're authorized to administer. If you are a System Administrator, you can administer the group list for all the Agencies defined in the TeleServer Message Switch.

The Group Administration utility lets you:

- view existing groups
- add a new group
- modify a group
- delete a group

Viewing Existing Groups

➔ **To view the groups defined for an Agency:**

1. In the navigation window on the left, click [Agency Administration](#), and then click [Group Admin](#).
2. Click the *Group Administration* down arrow and select the Agency whose groups you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. The groups defined for the selected Agency display in the table. For each group, PSA displays the group name and a description.

Adding a New Group

You can add groups to an Agency if you are authorized to administer that Agency. Once you have added a new group, you can modify the group to add users and set user privileges.

To add a group:

1. In the navigation window on the left, click [Agency Administration](#), and then click [Group Admin](#).
2. Click the *Group Administration* down arrow and select the Agency whose groups you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. Click the **Add** button on the *Group Administration* screen to open the *Add a New Group* screen.
4. Enter the name of the group you want to add to this Agency.
5. Enter a description of this group.
6. Enter the Agency code for this group.
7. Click **Submit** to add this group to this Agency.

Modifying a Group

You can modify the name of an existing group, specify the users that make up a group, and assign or remove privileges from a group. You can also delete a group from an Agency.

To modify a group:

1. In the navigation window on the left, click [Agency Administration](#), and then click [Group Admin](#).
2. Click the *Group Administration* down arrow and select the Agency whose groups you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. Click the name of the group you want to modify in the Group Name column. The *Modify Group* screen displays, where you can modify the name and/or description

of the group, modify the users in that group, and/or modify the user privileges of the users in that group.

4. In the first table, edit the name of the group in the Group Name box or edit the description in the Group Description box.
5. In the second table, specify which users belong to this group. All the users defined for the selected Agency display in the Available Users box on the right. The Current Users box on the left displays all the users currently assigned to this group. Select a user and click the <<<Assign or Remove>>> buttons in the middle of the screen to assign or remove users from this group.
6. In the third table, specify the user privileges you want to assign to the users in this group. All users in this group have the same set of privileges. All the system privileges defined display in the Available Privileges box on the right. The Current Privileges box on the left displays all the privileges currently assigned to the users in this group. Select a privilege and click the <<<Assign or Remove>>> buttons in the middle of the screen to assign or remove this privilege to/from the users in this group.
7. Click **Submit** to save all your changes and close the *Group Administration* screen, or click **Undo** in any of the tables to clear the modifications you made in that table. Click the **Cancel** button to clear all the modifications you made and close the *Group Administration* screen.

Deleting a Group

To delete a group from an Agency:

1. In the navigation window on the left, click Agency Administration, and then click Group Admin.
2. Click the *Group Administration* down arrow and select the Agency whose groups you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. The *Group Administration* screen displays. Select the checkbox next to the group you want to delete and click the **Delete** button. A confirmation message displays.
3. Click the **Yes** button in the message window to delete the selected group, or click **No** to abort the delete operation.

User Administration

The User Administration utility lets you manage the users of the TeleServer Message Switch for those Agencies you are authorized to administer. You can add, modify, and

delete users for each of your Agencies. When you add a user, you can assign security roles to that user.

The User Administration utility lets you:

- view existing users
- add new users
- modify existing users
- force off active users
- delete users

Viewing Existing Users

➔ **To view the users defined for an Agency:**

1. In the navigation window on the left, click [Agency Administration](#), and then click [User Admin](#).
2. Click the *User Administration* down arrow and select the Agency whose users you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)

The users for the selected Agency display in the table, which displays the User ID and the name of each user.

Adding a New User

You can add users to the TeleServer Message Switch by Agency. For each user, you must specify a User ID, a password, last name, first name, middle name, and title. You can also specify security roles, enable or disable the user, and specify that the user must change the password when he/she logs onto the TeleServer Message Switch.

➔ **To add a user to the TeleServer Message Switch:**

1. In the navigation window on the left, click [Agency Administration](#), and then click [User Admin](#).
2. Click the *User Administration* down arrow and select the Agency whose users you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. Click the **Add** button to open the *Add a New User* screen.
4. In the *UserID* field, enter the User ID you want to assign to this user.
Note: User IDs must be unique system-wide, not just within each Agency.
5. In the *Password* field, enter the password you want to assign to this user. The password displays as asterisks rather than letters for security purposes. Passwords are alphanumeric and must be between 1 and 13 characters long.

6. In the *Confirm Password* field, enter the password again, to confirm that you typed it correctly.
7. In the *Last Name*, *First Name*, and *Middle Name* fields, enter the full name of this user: last name, first name, and middle initial.
8. In the *Title* field, enter the appropriate title for this user.
9. By default, a user must change his/her password the first time he/she logs on to the TeleServer Message Switch. Deselect the *Password Change Required* checkbox if you don't want to make this user change the password the first time he/she logs onto the system.
10. The box on the right displays all the system security roles defined. (Security Roles are defined by a System Administrator.) Select the security roles you want to assign to this user.
11. Click the **Submit** button to add the user to the list of authorized users for the specified Agency.

Note: If you want to add either an Agency or System Administrator to the TeleServer Message Switch, you must first enter the user information using the Add a New User screen. Then use the System Administration utility to make the new user an administrator.

Modifying User Properties

You can change the properties of an existing user by clicking a User ID. You can change the name, the password, the title, and the security roles. You cannot change the Agency or User ID for a user. To change either of these items, you must delete the user record and create a new one.

To change a user's properties:

1. In the navigation window on the left, click Agency Administration, and then click User Admin.
2. Click the *User Administration* down arrow and select the Agency whose users you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. Click the User ID whose properties you want to change. The *Modify User* screen displays.
4. Make any necessary changes to the name of this user: last name, first name, and middle initial.
5. If necessary, type the new password you want to assign to this user. The password displays as asterisks for security purposes. Passwords are alphanumeric and must be between 1 and 13 characters long.
6. If you changed the password, retype the new password to confirm that you typed it correctly.
7. Make any necessary change to this user's title.

8. In the second table, make any necessary changes to the security roles assigned to this user. The Current Roles box on the left displays the roles currently assigned to this user, and the Available Roles box on the right displays all the security roles defined. Select a security role and click the <<<**Assign** or **Remove**>>> buttons in the middle of the screen to assign or remove this role to/from this user.
9. Click the **Submit** button to save your changes.

Deleting a User

You can delete users by selecting a user ID and clicking the Delete button.

To delete a user:

1. In the navigation window on the left, click Agency Administration, and then click User Admin.
2. Click the *User Administration* down arrow and select the Agency whose users you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. The *User Administration* screen displays. Select the checkbox next to the user you want to delete and click the **Delete** button. A confirmation message displays.
4. Click the **Yes** button in the message window to delete the selected user, or click **No** to abort the delete operation.

Monitor Users

The Monitor Users utility lets you monitor the users who are actively using the TeleServer Message Switch for the Agencies you are authorized to administer. If you are a System Administrator, you can monitor the user list for all of the Agencies defined in the TeleServer Message Switch.

To monitor the users for an Agency:

1. In the navigation window on the left, click Agency Administration, and then click Monitor Users.
2. Click the *Monitor Users* down arrow and select the Agency whose users you want to monitor from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. The *User Monitoring in Agency* screen displays. Click the **Refresh** button to refresh the user statistics.

PSA displays the following information for the active users for the selected Agency:

Column	Description
--------	-------------

Agency	The agency to which this user is assigned
User ID	The User ID assigned to this user
IP Address	The IP address of this user's computer
Inbound	The number of inbound requests received from this user
Outbound	The number of outbound responses sent to this user
In Queue	The number of requests from this user in the inbound queue
In Progress	The number of requests in progress for this user
Out Queue	The number of responses for this user in the outbound queue
Bytes IN User	The number of bytes received from this user
Bytes OUT User	The number of bytes sent to this user
Log ON Time	The length of time this user has been logged on to the TeleServer Message Switch
Last In Message	The time this user last sent a message
Last Out Message	The time this user last received a message
Failed In Message	The number of failed inbound messages from this user
Failed Out Message	The number of failed outbound messages sent to this user
CallBack Ports	The TCP/IP port at which the TeleServer Message switch can contact the client. For diagnostic purposes only.

Forcing Off an Active User

Occasionally a mobile user may drive a vehicle outside the range of the wireless modem, leaving the user account logged onto the TeleServer Message Switch but the user unable to access it. In this situation, the user cannot log in again until the first logon is ended.

The administrator can forcibly log off the user's account, thereby enabling that user to log in again.

To force off a user:

1. In the navigation window on the left, click [Agency Administration](#), and then click [User Admin](#).
2. Select an active user and click the **Force Off** button. A confirmation message displays; click the **Yes** button to continue the Force Off operation.

The user is immediately logged off the TeleServer Message Switch.

DataSources Administration

The DataSources Administration utility lets you define to the TeleServer Message Switch a backend application that serves your Agency, such as an RMS or CAD system. Each DataSource defined must have a unique Logon ID associated with the DataSource type (CAD/RMS).

When an Agency develops an interface between its CAD and/or RMS system and the TeleServer Message Switch, that interface communicates with the switch via the TCP/IP protocol, as described in Telepartner's TeleServer Switch CAD/RMS Interface Specification document.

When connecting to the switch, part of the protocol requires the interface to pass a logon ID and a password for verification purposes. Before the interface can connect to the switch, an Agency Administrator must add the Agency DataSource Logon ID to the switch, and assign it the DataSource types the interface has implemented. The two DataSource types defined to date are CAD (for Computer Aided Dispatch system) and RMS (for Records Management systems). A single interface program can implement either one or both of these interface types.

➔ **To add a DataSource for an Agency:**

1. In the navigation window on the left, click Agency Administration, and then click DataSource Admin.
2. Click the *Agency DataSource Administration* down arrow and select the Agency whose DataSources you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. The *DataSource Administration* screen displays. Click the top **Add** button to open the *Add a New DataSourceName to Agency* screen.
4. In the *DataSource Logon ID* field, enter the Logon ID you want to assign to the new DataSource.
5. In the *Password* field, enter the password you want to assign to the new DataSource.
6. In the *Confirm Password* field, enter the password again, to confirm that you typed it correctly.
7. In the *DataSource Type* field, enter the type for this DataSource (i.e., CAD or RMS).
8. The *Agency Code* field displays the appropriate Agency code.
9. Click the **Submit** button to add this DataSource logon ID to the list of authorized DataSource logon IDs for the specified

***Note:** When you add the Agency DataSource logon ID, you must specify a DataSource type at that time. If the DataSource is only implementing one of the interfaces types (CAD or RMS), then you are finished at this point. However, if the DataSource is implementing both CAD and RMS interfaces, you must add an additional DataSource type. When you add this additional DataSource type, be sure to select the same logon ID (it should be the only ID available to select).*

➔ **To assign an additional DataSource type to a DataSource logon ID for an Agency:**

1. In the navigation window on the left, click Agency Administration, and then click DataSource Admin.
2. Click the *Agency DataSource Administration* down arrow and select the Agency whose DataSources you want to administer from the drop-down list. This list displays only those Agencies you are authorized to administer. (If you are a System Administrator, the list contains all Agencies.)
3. The *DataSource Administration* screen displays. Click the bottom **Add** button to open the *Add DataSource Type for Agency* screen.
4. Click the *DataSource Logon ID* down arrow and select the DataSource Logon ID from the drop down list.
5. Enter the new DataSource type for this DataSource logon ID: RMS or CAD.
6. Click the **Submit** button to add the new DataSource type to this DataSource logon ID for the specified Agency.

➔ **To delete a DataSource logon ID:**

1. In the navigation window on the left, click Agency Administration, and then click DataSource Admin.
2. The *DataSource Administration* screen displays. Select the checkbox next to the DataSource logon ID to delete and click the **Delete** button.

InBasket Administration

CAPTAIN InBaskets are used to segregate reports that are pending approval in order to ensure that only designated Supervisors review and approve completed reports. All reports awaiting approval will be associated with one and only one InBasket. Supervisors will have the option of “watching” one or more InBaskets. When a supervisor “watches” an InBasket it means 2 things:

- During Supervisor Review only those reports that are associated with a supervisor’s watched InBaskets will be presented to the user.
- If the supervisor is logged on to the Teleserver Message switch when an officer submits a report for approval that is associated with the supervisor’s watched InBaskets the supervisor will be notified via a message that there is a new report ready for approval. The Supervisor will also be told of all reports available for review in that particular InBasket in each notification message.

All supervisors will be allowed to choose which InBaskets within their security group(s) they would like to watch via BlueLink. See BlueLink documentation for more information.

All users assigned to the Officers role will have a default InBasket for which newly created reports will be associated. When they submit a report for approval it will belong to their default InBasket unless they specify otherwise via BlueLink. Users can also change their default InBasket via BlueLink. See BlueLink documentation for more information.

An InBasket can be associated with a security group. A security group can be any group defined within the agency (see Group Administration section). If an InBasket is associated with a security group only supervisors who are members of that group can watch that InBasket. Officers do not have to be members of the group to specify that a report be placed in an InBasket that is associated with a security group.

All agencies must specify a default InBasket. This is to insure that all new users created in the agency will be assigned a default InBasket.

When a new agency is created (and when the InBasket functionality first comes on line) there will be a default InBasket created for the agency and all officers will have this InBasket as their default. All supervisors in the agency will watch the default InBasket and all unapproved reports will be associated with the default InBasket. This allows any agency not wishing to use the InBasket functionality to see the report writing interface the same as they always have.

The InBasket Administration utility lets you manage the InBaskets defined in your agency if you have the proper Manage InBasket privileges. If you are a System Administrator and have the proper Manage InBasket privileges, you can administer the InBaskets for all the Agencies defined in the TeleServer Message Switch.

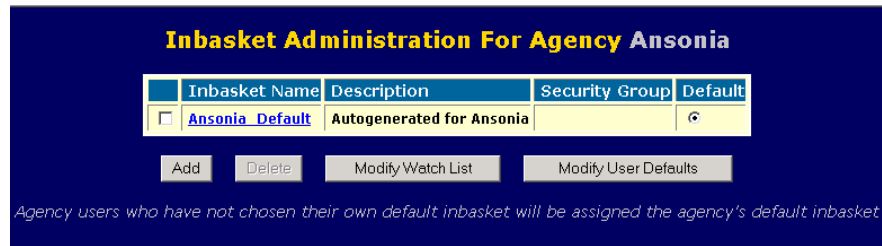
The InBasket Administration utility lets you:

- view existing InBaskets
- add a new InBasket
- modify an InBasket
- delete an InBasket
- change the default InBasket for an agency
- view and modify the list of InBaskets a supervisor is watching
- view and modify the default InBasket for the officers in the agency
- move reports from one InBasket to another

Viewing Existing InBaskets

➔ **To view the InBaskets defined for an Agency:**

1. In the navigation window on the left, click Agency Administration, and then click InBasket Admin.
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. For each InBasket, PSA displays the InBasket name, a description, the security group associated with the InBasket if any, and a default indicator. (If you are a System Administrator you must first select the agency you are interested in managing.)



Adding a New InBasket

You can add InBaskets to an Agency if you are a member of a group or role that has the ManageInBaskets privilege.

➔ To add a group:

1. In the navigation window on the left, click Agency Administration, and then click InBasket Admin.
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Click the **Add** button on the *InBasket Administration* screen to open the *Add a New InBasket* screen.
4. Enter the name of the InBasket you want to add to this Agency.
5. Enter a description of this InBasket.
6. Select a security group from the drop down list if you would like this InBasket to be associated with a security group.
7. Click **Submit** to add this InBasket to this Agency.

Modifying an InBasket

You can modify the name or description of an existing InBasket, change the security group associated with the InBasket, specify the supervisors that are watching the InBasket, specify users that have the InBasket as their default, and move reports from the InBasket to another InBasket. The privileges needed to perform these functions include: ManageInBaskets, ManageInBasketWatchList, ManageInBasketContents.

➔ To modify an InBasket:

1. In the navigation window on the left, click Agency Administration, and then click InBasket Admin.
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Click the name of the InBasket you want to modify in the InBasket Name column. The *Modify An InBasket* screen displays, where you can see and modify the list of supervisors watching the InBasket, the name, description or security group of the

InBasket, the users who have the InBasket as their default and the list of records currently associated with the InBasket.

Incident Number	Author	Status	Move
ITEST0029	RMSUser0029, Test User	PENDINGAPPROVAL	<input type="checkbox"/>
ITEST282	RMSUser0028, Test User	EDITINGCHECKOUT	<input type="checkbox"/>
I99-TEST123	RMSUser0021, Test User	PENDINGAPPROVAL	<input type="checkbox"/>
A99-TESTACCUPLD	RMSUser0022, Test User	INPROGRESS	<input type="checkbox"/>
A353	RMSUser0027, Test User	INPROGRESS	<input type="checkbox"/>
I99-USER25-INC1	RMSUser0025, Test User	INPROGRESS	<input type="checkbox"/>
A99-USER20-ACC1	RMSUser0020, Test User	INPROGRESS	<input type="checkbox"/>
A99-USERNEW-ACC1	RMSUser0028, Test User	INPROGRESS	<input type="checkbox"/>
A99-USER26-ACC1	RMSUser0026, Test User	INPROGRESS	<input type="checkbox"/>

4. To change the list of supervisors that are watching the InBasket click the **Modify** button under the *Supervisors Watching InBasket* list. The *Modify Supervisor Watch List for InBasket* screen displays. The Current Supervisors Assigned box on the left displays the current list of supervisors assigned to watch this InBasket. The Available Supervisors box on the right displays all supervisors currently eligible to watch this InBasket. Note that if a group secures the InBasket, only supervisors that are members of that group will be eligible to watch the InBasket. Select a user from either box and click the <<<Assign or Remove>>> buttons in the middle of the screen to add or remove supervisors from the watch list. When you are satisfied with your modifications click **Submit** to save your changes. You will be asked to confirm your changes and can cancel at this time. Click the **Cancel** button to clear all the modifications you made and close the *Modify Supervisor Watch List for InBasket* screen.
5. To change the InBasket name, description and/or security group for the InBasket make your changes in the text boxes under *Modify InBasket Details* and click the **Submit** button to save these changes. Click the **Cancel** button to clear all the modifications you made and close the *Modify An InBasket* screen.
6. To change the list of users who have this InBasket as their default click the **Modify** button under the *Users With InBasket as Default* list. See instructions for modifying user defaults in the section below.

7. To change the contents of the InBasket see the section on moving reports from one InBasket to another below.

Deleting an InBasket

You can delete InBaskets from an Agency if you are a member of a group or role that has the ManageInBaskets privilege. Conditions in which an InBasket may not be deleted are:

- The InBasket is the agency default.
- The InBasket has reports associated with it.
- The InBasket is the default InBasket for 1 or more users.

➔ To delete an InBasket from an Agency:

1. In the navigation window on the left, click Agency Administration, and then click InBasket Admin.
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Select the checkbox to the left of the InBasket you want to delete and click the **Delete** button. A confirmation message displays.
4. Click the **Ok** button in the message window to delete the selected InBasket, or click **Cancel** to abort the delete operation.

Changing the agency default InBasket

You can change the default InBasket of an Agency if you are a member of a group or role that has the ManageInBaskets privilege.

➔ To add a group:

1. In the navigation window on the left, click Agency Administration, and then click InBasket Admin.
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Select the radio button to the right of the InBasket you want to set as the agency default. A confirmation message displays.
4. Click the **Ok** button in the message window to set as the agency default the selected InBasket, or click **Cancel** to abort the operation.

Viewing and modifying the Supervisor Watch List

You can view and modify the supervisor watch lists in an Agency if you are a member of a group or role that has the ManageInBasketWatchList privilege.

➔ To view or modify the supervisor watch list:

1. In the navigation window on the left, click [Agency Administration](#), and then click [InBasket Admin](#).
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Click the **Modify Watch List** button on the *InBasket Administration* screen to open the *Supervisor Watch List Administration for Agency* screen.
4. A table containing a list of supervisors in the agency and the InBaskets they are currently watching is displayed. If a supervisor is watching more than one InBasket his or her name will appear more than once in the left column. If the supervisor is not currently watching an InBasket the word UNASSIGNED will appear in the InBasket Name column. The table can be sorted by clicking on the column headers. An up or down arrow appears indicating if the column is sorted in ascending or descending order.
5. Click on the name of the supervisor whose watch list you would like to modify. The *Modify Watch List for Supervisor* screen displays. The Currently Watched InBaskets box on the left displays the current list of InBaskets this supervisor is watching. The Available InBaskets box on the right displays all InBaskets that this supervisor is eligible to watch. Select an InBasket from either box and click the <<<**Assign** or **Remove**>>> buttons in the middle of the screen to add or remove InBaskets from the watch list. When you are satisfied with your modifications click **Submit** to save your changes. You will be asked to confirm your changes and can cancel at this time. Click the **Cancel** button to clear all the modifications you made and close the *Modify Watch List for Supervisor* screen.

Viewing and modifying the default InBasket for Officers

You can view and modify the default InBasket for the Officers in an Agency if you are a member of a group or role that has the ManageInBaskets privilege.

To view or modify the default InBasket for Officers:

1. In the navigation window on the left, click [Agency Administration](#), and then click [InBasket Admin](#).
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Click the **Modify User Defaults** button on the *InBasket Administration* screen to open the *User Default InBasket Administration for Agency* screen.
4. A table containing a list of officers in the agency and their corresponding default InBasket is displayed. The table can be sorted by clicking on the column headers. An up or down arrow appears indicating if the column is sorted in ascending or descending order.
5. To change the default InBasket of one or more Officers click on the check box in the rightmost column of table in the row containing their name. At the bottom of the screen select the new default InBasket you would like to assign to these users. Click on the **Change Default To InBasket** button. You will be asked to confirm

your changes and can cancel at this time. Click the **Cancel** button to clear all the modifications you made and close the *User Default InBasket Administration for Agency* screen.

Moving Reports from one InBasket to another

You can move reports from one InBasket to another if you are a member of a group or role that has the ManageInBasketContents privilege.

➔ To move reports from one InBasket to another:

1. In the navigation window on the left, click Agency Administration, and then click InBasket Admin.
2. If you are not a System Administrator the InBaskets defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)
3. Click the name of the InBasket from which you want to move the report in the InBasket Name column. The *Modify An InBasket* screen displays. At the bottom of the screen a table is displayed that contains each report's incident number, author name, and report status. The table can be sorted by clicking on the column headers. An up or down arrow appears indicating if the column is sorted in ascending or descending order.
4. To move one or more reports to another InBasket click on the check box in the rightmost column of table in the row containing the report. At the bottom of the screen select the new InBasket you would like to move the reports to. Click on the **Move To InBasket** button. You will be asked to confirm your changes and can cancel at this time. Click the **Cancel** button under the *Modify InBasket Details* table to clear all the modifications you made and close the *Modify An InBasket* screen.

Data Sharing Rules Administration

Data sharing rules govern how incident reports details are shared internally within an agency and externally among agencies. Each agency can tailor their own set of rules based on the System-wide roles that are common to all agencies. For each role a data sharing rules administrator can determine if the details of a report are available based on the NIBRS incident type for which that report has been categorized. Thus an Agency Administrator can limit access to report details among its users in one manner, and have a different and probably more restrictive manner for these incidents among external users. Note that Supplements and Accidents do not have a NIBRS incident type and are by default shared among all users.

The Data Sharing Rules Administration utility lets you:

- View and modify the data sharing rules for your agency

Viewing and Modifying Data Sharing Rules

➔ To view the Data Sharing Rules defined for an Agency:

1. In the navigation window on the left, click Agency Administration, and then click Data Sharing Rules Admin.
2. If you are not a System Administrator the data sharing rules defined for your Agency display in the table. (If you are a System Administrator you must first select the agency you are interested in managing.)

Data Sharing Rule Administration For Agency Rocky Hill

Incident Type	Officers	
	Internal	External
40B Assisting or Promoting Prostitution	<input checked="" type="checkbox"/>	<input type="checkbox"/>
90A Bad Checks	<input checked="" type="checkbox"/>	<input type="checkbox"/>
39A Betting/Wagering	<input checked="" type="checkbox"/>	<input type="checkbox"/>
510 Bribery	<input checked="" type="checkbox"/>	<input type="checkbox"/>
220 Burglary/Breaking and Entering	<input checked="" type="checkbox"/>	<input type="checkbox"/>
250 Counterfeiting/Forgery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26B Credit Card/Automatic Teller Machine Fraud	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
90B Curfew/Loitering/Vagrancy Violations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
290 Destruction/Damage/Vandalism of Property	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
90C Disorderly Conduct	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
90D Driving Under the Influence	<input checked="" type="checkbox"/>	<input type="checkbox"/>
35B Drug Equipment Violations	<input checked="" type="checkbox"/>	<input type="checkbox"/>
35A Drug/Narcotic Violations	<input checked="" type="checkbox"/>	<input type="checkbox"/>
90E Drunkenness	<input checked="" type="checkbox"/>	<input type="checkbox"/>
270 Embezzlement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
210 Extortion/Blackmail	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Submit Cancel

3. The *Data Sharing Rule Administration For Agency* screen contains a large table with the leftmost column listing all of the incident types. In the upper right corner of the table is a drop down list containing all the roles used for data sharing administration. Underneath this list are 2 check box columns internal and external. A checked box under the internal column indicates that the details of a report with the incident type specified in that row will be shared with users with that role who are members of the agency. A checked box under the external column indicates that the details of the report with the incident type specified in that row will be shared with users who are not members of the agency. Note that incident reports that have more than one incident type will only be shared if the user has permission to view all types of incidents based on these rules.
4. To make changes to the data sharing rules first select, using the drop down list, the role for which you want to make changes. The screen will refresh and display the rules for that role. Make all the changes you would like to make for that role by checking or unchecking the boxes. When you are satisfied with your modifications click **Submit** to save your changes. You will be asked to confirm your changes and can cancel at this time. Click the **Cancel** button to clear all the modifications you made and close the *Data Sharing Rule Administration For Agency* screen.

SYSTEM ADMINISTRATION

The System Administration utility enables a System Administrator to manage all agencies, security roles, privileges, external DataSources, and system alerts and to monitor events on the TeleServer Message Switch.

A System Administrator must have the appropriate security roles and privileges assigned to his/her user ID.



System Administration utility options are:

- manage administrative privileges, either System or Agency, for system users.
- manage the security roles defined for users of the TeleServer Message Switch.
- manage the Agencies defined in the TeleServer Message Switch.
- view the system-wide security privileges for users of the TeleServer Message Switch.
- monitor the activity and display statistics of the TeleServer Message Switch.
- manage external global DataSources to the TeleServer Message Switch, such as an agency's CAD and/or RMS systems.

Administrators

The Administrators utility displays a list of all administrators, both System and Agency Administrators. If you are a System Administrator, you can use the Administrators utility to add or delete administrative privileges, either System or Agency, for system users.

➔ **To view the administrators defined:**

- In the navigation window on the left, click [System Administration](#), and then click [Administrators](#).

All the administrators defined display in a table:

Column	Description
Admin Privilege	The Agency for which the administrator is authorized. System Administrators are listed as System Admin.
User ID	The User ID assigned to each administrator
Name	The full name of each administrator

Adding an Administrator

You can create new administrators by changing the privileges of existing system users. First you must select the Agency and the User ID of the user whose privileges you want to change. Then you must specify whether this user is an Agency or System Administrator.

Note: You must add a user to the system using the User Administration option before you can make a user an Administrator.

➔ To specify administrative privileges for defined users:

1. In the navigation window on the left, click System Administration, and then click Administrators.
2. Click the **Add** button to open the *Add Administrator* screen.
3. Click the *User from Agency* down arrow and select the Agency in which the user is defined.
4. Click the *User ID* down arrow and select the user you want to make an administrator.
5. Click a radio button to specify whether you want this user to be a System Administrator or an Agency Administrator.
6. Click the **Submit** button to create the new administrator.

Note: A user can be authorized as an administrator in more than one Agency. However, you must add each Agency authorization separately.

Deleting an Administrator

You delete administrators by removing the administrative privileges assigned to the user.

➔ To remove administrative privileges from a user:

1. In the navigation window on the left, click System Administration, and then click Administrators.
2. Select the checkbox next to an administrator's User ID and click the **Delete** button. A confirmation message displays.
3. Click the **Yes** button in the message window to delete the selected user's administrative privileges, or click **Cancel** to abort the delete operation.

Note: Deleting administrator privileges does not delete that user from the TeleServer Message Switch. If you want to delete the user, first remove

their administrative privileges and then delete the user using the User Administration utility.

Security Roles

The Security Roles utility displays the security roles defined for the system. Security roles are privileges that are meaningful to both the mobile client and the backend applications. For example, if a System Administrator defines the role of "Supervisor," Agency Administrators can then specify which officers should have the role of "Supervisor." This role information is made available to both the mobile client application and the backend applications. Certain system functions can be made available or unavailable at the client, depending upon what roles have been assigned to a user. Similarly, a backend application can require a user to be assigned a particular role in order to perform some specific function.

Depending on what client application or what backend applications are interfaced to the TeleServer Message Switch, the roles defined can vary.

You can add a new role, modify an existing role, delete a role, and view a list of users who have been assigned to a role.

Note: Only System Administrators can add, modify, or delete security roles.

To view a list of defined security roles:

- In the navigation window on the left, click [System Administration](#), and then click [Security Roles](#).

The Security Role Administration screen displays all the security roles defined.

Adding a Security Role

You can add a new security role to the list defined for the system.

To add a security role:

1. In the navigation window on the left, click [System Administration](#), and then click [Security Roles](#).
2. The *Security Role Administration* screen displays all the security roles defined. Click the **Add** button to access the *Add a Security Role Name* screen
3. Type the name of the role you want to add and click the **Submit** button.

Modifying a Security Role

You can modify the name of an existing security role or change the system privileges assigned to a security role.

To modify a security role:

1. In the navigation window on the left, click [System Administration](#), and then click [Security Roles](#).
2. The *Security Role Administration* screen displays all the security roles defined. Click the security role you want to modify.

3. The *Modify Security Role* screen has two tables. In the first table, make any changes to the name of the security role.
4. In the second table, you can modify the system privileges assigned to this security role. The Current Privileges box on the left displays the system privileges currently assigned to this security role, and the Available Privileges box on the right displays all the system privileges defined. Select a privilege and click the <<<**Assign** or **Remove**>>> buttons in the middle of the screen to assign or remove this privilege to/from this security role.
5. Click the **Submit** button to save your changes.

Deleting a Security Role

You can delete a security role from the system.

➔ To delete a security role:

1. In the navigation window on the left, click [System Administration](#), and then click [Security Roles](#).
2. Select the checkbox next to a security role name and click the **Delete** button. A confirmation message displays.
4. Click the **Yes** button in the message window to delete the selected role, or click **No** to abort the delete operation.

Agency Administration

If you are a System Administrator, the Agency Administration utility lets you manage the Agencies that use the TeleServer Message Switch. You can add, modify, or delete Agencies from the TeleServer Message Switch.

You must define an Agency in the Agency Administration page before you can add users to that Agency.

➔ To view the Agencies defined:

- In the navigation window on the left, click [System Administration](#), and then click [Agency Admin](#).

The *Agency Administration* screen displays a table with the following information:

- The name of the agency
- The agency type
- The code number assigned to this agency

Adding a New Agency

System Administrators can add a new Agency to the TeleServer Message Switch.

➔ To add an Agency:

1. In the navigation window on the left, click System Administration, and then click Agency Admin.
2. Click the **Add** button on the *Agency Administration* screen to open the *Add Agency* screen.
3. In the *Agency Name* field, enter the name of the new Agency.
4. Select the *Agency Type*: Police, Fire, or EMS.
5. In the *Agency Code* field, enter the code for this Agency. The codes are determined by the System Administrator of the TeleServer Message Switch. For example, the state of Connecticut uses town tax codes as Agency codes.
6. In the *ORI* field, enter the 9-digit code that identifies the Agency.
7. Click **Submit** to add this Agency to the system.

Modifying an Agency

You can modify the name of an Agency, the type of Agency, or the Agency code.

To modify an agency:

1. In the navigation window on the left, click System Administration, and then click Agency Admin.
2. Click an Agency Name in the *Agency Administration* screen to access the *Modify An Agency* screen.
3. As necessary, edit the name of the Agency, the Agency Type, or the Agency Code.
4. Click the **Submit** button to save your changes.

Deleting an Agency

You can delete an Agency.

To delete an agency:

1. In the navigation window on the left, click System Administration, and then click Agency Admin.
2. Select the checkbox next to an Agency name in the *Agency Administration* screen and click the **Delete** button. A confirmation message displays.
3. Click the **Yes** button in the message window to delete the selected agency, or click **No** to abort the delete operation.

Note: You cannot delete an Agency if there are users defined in that Agency.

View Privileges

The View Privileges utility lets you view the system-wide security privileges for users of the TeleServer Message Switch.

➔ **To view all system privileges:**

- In the navigation window on the left, click [System Administration](#), and then click [View Privileges](#).

The System Privileges screen displays the name and a description of all the system privileges currently defined.

Monitor Switch

The Monitor Switch utility lets you monitor the overall activity of the TeleServer Message Switch.

➔ **To view all switch activities:**

- In the navigation window on the left, click [System Administration](#), and then click [Monitor Switch](#).

PSA displays the current statistics for the TeleServer Message Switch. These statistics are not automatically updated. To continue to view the current statistics, you must click the Refresh button.

The *Monitor Switch* screen displays the following statistics about the TeleServer Message Switch:

Field	Description
<i>Inbound</i>	
Total Messages Since Switch Started	The total number of messages sent to the TeleServer Message Switch since it was last started.
Total Bytes Since Switch Started	The total number of kilobytes of inbound messages sent to the TeleServer Message Switch since it was last started.
Total Receive Failures	The total number of inbound messages the TeleServer Message Switch failed to receive.
Messages Enqueued	The number of messages currently in the inbound queue.
Messages in Progress	The number of messages currently being processed.
<i>Outbound</i>	
Total Messages Since Switch Started	The total number of messages sent by the TeleServer Message Switch since it was last started.
Total Bytes Since Switch Started	The total number of kilobytes of outbound messages sent by the TeleServer Message Switch since it was last started.

Total Send Failures	The total number of outbound messages the TeleServer Message Switch failed to send.
Messages Enqueued	The number of messages currently in the outbound queue.
<i>Time</i>	
Last Refresh	The time when statistics were last refreshed.
Current	The current time.
<i>Users</i>	
Logged on	The number of users currently logged on.
Total Sessions	The number of users who logged on since the TeleServer Message Switch was last started.

Global DataSource Administration

The Global DataSources Administration utility lets a System Administrator define to the TeleServer Message Switch backend applications that are implemented as system-wide resources. For example, COLLECT is a DataSource that is available to all agencies, as are the Regional RMS and Car-to-Car Messaging. Global DataSources should rarely change, but the Global DataSource Admin utility provides an interface to add additional DataSources or change existing ones. Each DataSource defined must have a unique logon ID associated with the DataSource type.

When connecting to the switch, part of the protocol requires the interface to pass a logon ID and a password for verification purposes. Before the interface can connect to the switch, a System Administrator must add the global DataSource logon ID to the switch, and assign it the DataSource type(s) the interface has implemented.

To add a global DataSource:

1. In the navigation window on the left, click System Administration, and then click Global DataSource Admin.
2. The *Global DataSource Administration* screen displays. Click the top **Add** button to open the *Add a New Global DataSourceName* screen.
3. In the *DataSource Logon ID* field, enter the Logon ID you want to assign to the new global DataSource.
4. In the *Password* field, enter the password you want to assign to the new global DataSource logon ID.
5. In the *Confirm Password* field, enter the password again, to confirm that you typed it correctly.
6. Click the **Submit** button to add this DataSource logon ID to the list of authorized global DataSources.

Note: When you add the *DataSource* logon ID, you must specify a *DataSource* type at that time. If the *DataSource* is only implementing one interface type, then you are finished at this point. However, if the *DataSource* is implementing more than one interface, you must add all additional *DataSource* type. When you add an additional *DataSource* type, be sure to select the same logon ID (it should be the only ID available to select).

Adding a DataSource Type to a Global DataSource Logon ID

Use the Global DataSource Admin utility to assign DataSource types to global DataSource logon IDs.

To add a DataSource type to a global DataSource logon ID:

1. In the navigation window on the left, click [System Administration](#), and then click [Global DataSource Admin](#).
2. The *Global DataSource Administration* screen displays. Scroll down to the DataSource Type table and click the **Add** button to open the *Add Global DataSource Type* screen.
3. Click the *DataSource Logon ID* down arrow and select the logon ID to which you want to add a DataSource type.
4. In the *Add a New Data Type* field, enter the new DataSource type name you want to add.
5. Click the **Submit** button to add this DataSource type to the selected Data Source logon ID.

Deleting a Global DataSource Logon ID or DataSource Type

To delete a global DataSource logon ID or DataSource type:

1. In the navigation window on the left, click [System Administration](#), and then click [Global DataSource Admin](#).
2. The *Global DataSource Administration* screen displays. Select the checkbox next to the DataSource logon ID (top frame) or DataSource type (bottom frame) to delete and click the **Delete** button.

MANAGEMENT REPORTS

The Management Reports utility lets you audit reports on agency activity such as Messaging, COLLECT, and incident reports; view the audit records for a report; view the current status of an incident, including the history of the actions that have been performed by each individual on each report; change the status of a report; and audit the activity log files for events. PSA also provides a set of common searches, to help you find the reports you need as quickly as possible.



The Management Report options are:

- search for reports by date, officer, status, and attributes.
- search criteria to find a set of reports by Officer.
- create a standard search for report sets.
- search for report events by officer and date.
- audit the activity log files for COLLECT queries.
- audit the activity log files for Messaging data.
- audit the activity log files for a specific Officer.

Once you've run a report search, you view the results of the search in the Query Results screen. When you select a specific report to view, the report details display on the Incident Details screen.

Report Search

The Report Search utility lets you search for reports by date, officer, status, and attributes. You can enter criteria in one, some, or all of these fields. If you leave a field blank, the search will not filter reports by that criteria. For example, if you leave the Report Status field empty (i.e., with a value of Any Status), the search retrieves reports regardless of their status.

➔ **To perform a report search:**

1. In the navigation window on the left, click Management Reports, and then click Report Search.

Reports Search

Enter search criteria

****Start Date/Time:** [02] / [25] / [2001] [16] : [32]

Date/Time format: MM/DD/YYYY hh:mm

****End Date/Time:** [02] / [26] / [2001] [16] : [32]

****Created By:** []

Report Status: [Any status ▼]

Report Attributes: Printed Created Today

[Search] [Reset]

2. In the *Reports Search* screen, enter the search criteria required to retrieve a report:
3. In the *Start Date/Time* field, enter the beginning date of the reports to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
4. In the *End Date/Time* field, enter the ending date of the reports to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
5. In the *Created By* field, enter the user name of the officer who created the report.
6. Enter any additional search criteria you want to use:
 - Click the *Report Status* down arrow and select a status from the drop-down list: *Approved*, *In Progress*, or *Checked Out*. Leave the status as *Any status* if you don't want to filter the reports by status.
 - Select any *Report Attributes* you want to use: *Printed* (only those reports that have already been printed) and/or *Created Today* (only those reports that were created today). Leave these checkboxes unselected if you don't want to filter the reports by either attribute.
7. Click the **Search** button to run your search.

PSA executes your search and displays the results in the *Query Results* screen.

Reading a Report

Report Search Query Results

Once you've entered your search criteria on the *Report Search* screen and clicked the **Search** button, PSA executes your search and returns the results of your search in the Query Results screen.

The Query Results screen presents the following information about the reports that match your search criteria:

Records found – the number of reports that match your search criteria.

Search criteria statement – search criteria used to retrieve these records.

Incident number – the number of the incident described in the report. Click the incident number to view details about this incident on the Incident Details page.

Status – the status of each report:

- *In Progress* – report has been created but is not yet approved. It is not currently checked out to anyone
- *Checked out for editing* – the report is checked out for editing by the owning officer
- *Checked out for review* – report is checked out for review by a supervisor
- *Pending approval* – report has been submitted for review
- *Approved* – report has been completed and approved by a supervisor. No more changes are allowed.

Created on – date and time the report was first created.

Last modified – the date and time the report was last changed, if it has been modified.

Print status – the date and time the report was last printed, if it has been printed.

Owner – the officer who currently is in charge of (i.e., the owner of) this report.

View Incident Summary

When you click an incident number on a *Query Results* screen, you access the *Incident Summary* screen for that report.

The *Incident Summary* screen presents the following information about a report:

Report # – number assigned to this report

Record Owner – the user ID of the report owner

Date Created – date and time the report was first created

Checked Out To – the user ID of the officer to whom the report is currently checked out, if any

Date Modified – date and time the report was last modified, if any

Record Approver – the user ID of the supervisor who has approved the report, if any

Date Approved – the date and time the report was approved, if any

Revision – number of times the report has been revised. An unrevised report has a revision number of 1

Date Transferred – the date and time the report was transferred to the agency's internal Report Management System, if any

Current Status – the current status of the report:

- *In Progress* – the report has been created but is not yet approved. It is not currently checked out to anyone
- *Checked out for editing* – the report is checked out for editing by the owning officer
- *Checked out for review* – the report is checked out for review by a supervisor
- *Pending approval* – the report has been submitted for review
- *Approved* – the report has been completed and approved by a supervisor. No more changes are allowed.

Date Printed – the date and time the report was printed, if any. If the report has already been printed, you can click the Reset button to reset the Print status to Not Printed so that the report can be printed from again.

➔ **To change the owner of a report:**

1. Click the *Record Owner* down arrow and select a different owner from the list of user IDs.
2. PSA displays a confirmation message regarding the owner change; click the **Yes** button.

➔ **To change the status of a report:**

1. Click the *Current Status* down arrow and select a different status: *In Progress*, *Checked out for editing*, *Checked out for review*, *Pending approval*, *Approved*.
2. PSA displays a confirmation message regarding the status change; click the **Yes** button.

➔ **To view the events about a report:**

- Click the [View events for this record](#) hyperlink to open the *Incident Events* screen for this incident.

Reports Search Incident Details

When you click the [View Incident Details](#) hyperlink on an *Incident Details* screen, you access a screen that provides detailed information about the incident.

Incident Number – incident number assigned to case

Incident ID information– Incident Type Code, report status, date/time the incident was reported, clearance code, and officer name

Location information – street intersection names, type of location, type of premise, town name, state, and zip code.

Persons involved information – name, gender, race, date of birth, age (minimum and maximum), height & weight, status, and charge, if any.

Vehicle property involved information – registration number, VIN number, and year.

Non-vehicle property involved information – item, quantity, serial number

Narrative – from report filed

Report Search Events For This Record

When you click the [View events for this record](#) hyperlink on an *Incident Details* screen, you access the *Incident Events* screen for that report.

The *Incident Events* screen presents a list of all the events that have occurred for the current report, and the user ID of the officer who performed each event. Each event listing includes:

- **Incident #** – the number of the incident
- **Date** – the date and time the event occurred
- **Description** – a brief description of the event
- **Details** – some events also include additional information about the event. For example, a status change event includes the new status in the Details field
- **By Whom** – the user ID of officer/supervisor who performed or was involved in the event

List of Report Events

The report event types included in the PSA application include:

Record List Retrieved – user retrieved a list of records from within the mobile client

Record Created – user created a new record in the RMS system

Record Checked Out for Editing – the user checked out the record to make changes

Record Checked Out for Review – the supervisor checked out the record to review it

Record Checked In With Editing Changed – the user checked a record in that s/he has modified

Record Checked In Without Editing Changes – the user canceled the checkout of a record and discarded any changes

Record Submitted For Supervisor Review – user submitted the record for review and potential approval by a supervisor

Record Approved By Supervisor – the supervisor reviewed and approved the record

Record Rejected By Supervisor – the supervisor reviewed the record but did not approve it. The record may require modification

Record Retrieved for Read-Only Viewing – the user retrieved a record for the purpose of reading it

Record Security Changed – security flags of the specified record were altered

Record Printing Started – the user began the process of printing a record

Record Printing Finished – the user completed the printing of a record

Submit Review Comment – the supervisor created a review comment for a record submitted to him/her.

Reset Printed Date – the supervisor reset the date on which a record was printed, to enable the record to be printed again

Record Deleted By Owner – the owner of the record deleted it

Record Status Changed – the status of a record was manually changed by an administrator

Record Creatorship Reassigned – the creator/owner of a record was reassigned by an administrator

Report by Officer

The Reports by Officer report utility presents a list of reports by officer, where you can select the officer whose In Progress reports you want to view.

***Note:** The Reports by Officer Search executes a search for reports with a status of In Progress and Checked Out For Editing only. To view all reports owned by an officer, use the Reports Search utility instead.*

➔ **To perform a Reports by Officer search:**

1. In the navigation window on the left, click Management Reports, and then click Report by Officer. The *Reports By Officer* screen opens.

Reports By Officer			
Select an officer to view reports in progress:			
Officer List	Report Counts		
	Checked Out	In Progress	Total
● TECHSUPPORT (Telepartner Technical Support)	0	0	0
● JTM5528 (McMahon, Jack)	0	0	1
● PWN4168 (Nielsen, Phil)	0	4	5
● ESHERBACOW (Sherbacow, Eric)	0	14	15
● MUZ (Mu, Zongliang)	0	0	0
● CRENNA (Carol Renna)	0	1	1
● ROVER (Rovanelli, Don)	0	0	0

2. In the *Report by Officer* screen, click the user ID of the officer whose reports you want to view.

PSA displays the reports found by the search in the *Query Results* screen.

The *Report By Officer* screen contains the following information:

Officer List – of officers and supervisors, by user ID

Report Counts

- Number of reports checked out by each officer
- Number of reports with an In Progress status for each officer
- Total number of reports owned by each officer

Report by Officer Search Query Results

Once you've clicked an officer's user name on the *Reports By Officer* screen, PSA executes your search and returns summaries about all the *In Progress* and *Checked Out For Editing* reports owned by the selected officer.

The *Query Results* screen presents the following information about the Officer reports that match your search criteria:

Records found – number of reports that match your search criteria.

Search criteria statement – search criteria used to retrieve these reports.

Incident number – the number of the incident described in the report. Click the incident number to view details about this incident on the *Incident Details* screen.

Status – the status of each report:

- *In Progress* – report has been created but is not yet approved. It is not currently checked out to anyone

- *Checked out for editing* – report is checked out for editing by the owning officer
- *Checked out for review* – report is checked out for review by a supervisor
- *Pending approval* – report has been submitted for review
- *Approved* – the report has been completed and approved by a supervisor. No more changes are allowed.

Created on – date and time the report was first created.

Last modified – date and time the report was last changed, if it has been modified.

Print status – date and time the report was last printed, if it has been printed.

Owner – officer who currently is in charge of (i.e., the owner of) this report.

Report by Officer Search Incident Details

When you click an incident number on a *Query Results* screen, you access the *Incident Details* screen for that report.

The *Incident Details* screen presents the following information about a report:

Report # – number assigned to this report

Record Owner – user ID of the report owner

Date Created – date and time the report was first created

Checked Out To – user ID of the officer to whom the report is currently checked out, if any

Date Modified – date and time the report was last modified, if any

Record Approver – user ID of the supervisor who has approved the report, if any

Date Approved – date and time the report was approved, if any

Revision – number of times the report has been revised. An unrevised report has a revision number of 1

Date Transferred – the date and time the report was transferred to the agency's internal Report Management System, if any

Current Status – current status of the report:

- *In Progress* – the report has been created but is not yet approved. It is not currently checked out to anyone
- *Checked out for editing* – report is checked out for editing by the owning officer
- *Checked out for review* – report is checked out for review by a supervisor
- *Pending approval* – report has been submitted for review
- *Approved* – report has been completed and approved by a supervisor. No more changes are allowed.

Date Printed – the date and time the report was printed, if any. If the report has already been printed, you can click the **Reset** button to reset the Print status to *Not Printed* so that the report can be printed again.

➔ To change the owner of a report:

1. Click the *Record Owner* down arrow and select a different owner from the list of user IDs.
2. PSA displays a confirmation message regarding the owner change; click the **Yes** button.

➔ To change the status of a report:

1. Click the *Current Status* down arrow and select a different status: *In Progress*, *Checked out for editing*, *Checked out for review*, *Pending approval*, *Approved*.
2. PSA displays a confirmation message regarding the status change; click the **Yes** button.

➔ To view the events about a report:

- Click the [View events for this record](#) hyperlink to open the *Incident Events* screen for this incident.

Report by Officer Search Incident Details

When you click the [View Incident Details](#) hyperlink on an *Incident Details* screen, you access a screen that provides detailed information about the incident.

Incident Number – incident number assigned to case

Incident ID information– Incident Type Code, report status, date/time the incident was reported, clearance code, and officer name

Location information – street intersection names, type of location, type of premise, town name, state, and zip code.

Persons involved information – name, gender, race, date of birth, age (minimum and maximum), height & weight, status, and charge, if any.

Vehicle property involved information – registration number, VIN number, and year.

Non-vehicle property involved information – item, quantity, and serial number

Narrative – from report filed

Report by Officer Search Record Events

When you click the [View events for this record](#) hyperlink on an *Incident Details* screen, you access the *Events* screen for that report.

The *Events* screen presents a list of all the events that have occurred for the current report, and the user ID of the officer who performed each event. Each event listing includes:

Incident # – incident number assigned to case

Date – the date and time the event occurred

Description – brief description of the event. See the “List of Report Events” section for a list of all possible report events.

Details – events also include additional information about the event. For example, a status change event includes the new status in the *Details* field

By Whom – user ID of officer/supervisor who performed or was involved in the event

Common Searches

The Common Searches report utility presents a list of the most commonly-executed searches performed on the Regional RMS database.

➔ **To execute a common search:**

1. In the navigation window on the left, click Management Reports, then click Common Searches. The *Reports Quick Searches* screen opens.

Reports Quick Searches

Use ONE of the following queries to quickly search:

Reports whose incident number is	<input style="width: 150px;" type="text"/>	<input type="button" value="Search"/>
Reports in progress more than	<input style="width: 40px;" type="text" value="24"/> hours.	<input type="button" value="Search"/>
Reports rejected at least	<input style="width: 40px;" type="text" value="5"/> times.	<input type="button" value="Search"/>
Reports that were created	<input style="width: 80px;" type="text" value="Today"/> ▾	<input type="button" value="Search"/>
Reports that have NOT yet been approved.		<input type="button" value="Search"/>
Reports that have NOT yet been printed.		<input type="button" value="Search"/>

2. You can execute any one of the six common searches. Enter any required search criteria and click one of the six **Search** buttons to execute a search.
 - **Incident Number** – enter an incident number and click **Search** to find all the reports that pertain to that incident
 - **In Progress Reports** – enter a number and click **Search** to find all the reports that have had an In Progress status for more than the specified number of hours
 - **Rejected Reports** – enter a number and click **Search** to find all the reports that have been rejected at least that number of times
 - **Time Period** – click the down arrow, select a time frame, and click **Search** to find all the reports that were created at that time
 - **Reports Not Approved** – click **Search** to find all the reports that have not yet been approved

- **Reports Not Printed** – click **Search** to find all the reports that have not yet been printed

PSA displays the results of the search in a *Query Results* screen.

Common Search Query Results

Once you have clicked a **Search** button on the *Reports Quick Searches* screen, PSA executes your search and returns details on all the reports that match the search criteria in the *Query Results* screen.

The *Query Results* screen presents the following information about the reports that match your search criteria:

Records found – the number of reports that match your search criteria.

Search criteria statement – the search criteria used to retrieve these records.

Incident number – the number of the incident described in the report. Click the incident number to view details about this incident on the Incident Details screen.

Status – the status of each report:

- *In Progress* – report has been created but is not yet approved. It is not currently checked out to anyone
- *Checked out for editing* – report is checked out for editing by the owning officer
- *Checked out for review* – report is checked out for review by a supervisor
- *Pending approval* – the report has been submitted for review
- *Approved* – report has been completed and approved by a supervisor. No more changes are allowed.

Created on – date and time the report was first created.

Last modified – the date and time the report was last changed.

Print status – date and time the report was last printed, if it has been printed.

Owner – officer who currently is in charge of this report.

Common Search Incident Details

When you click an incident number on a *Query Results* screen, you access the *Incident Details* screen for that report.

The *Incident Details* screen presents the following information about a report:

Report # – number assigned to this report

Record Owner – user ID of the report owner

Date Created – date and time the report was first created

Checked Out To – user ID of the officer to whom the report is currently checked out, if any

Date Modified – date and time the report was last modified, if any

Record Approver – user ID of the supervisor who has approved the report, if any

Date Approved – date and time the report was approved, if any

Revision – number of times the report has been revised. An unrevised report has a revision number of 1

Date Transferred – date and time the report was transferred to the agency's internal Report Management System, if any

Current Status – current status of the report:

- *In Progress* – report has been created but is not yet approved. It is not currently checked out to anyone
- *Checked out for editing* – report is checked out for editing by the owning officer
- *Checked out for review* – report is checked out for review by a supervisor
- *Pending approval* – report has been submitted for review
- *Approved* – report has been completed and approved by a supervisor. No more changes are allowed.

Date Printed – the date and time the report was printed, if any. If the report has already been printed, you can click the **Reset** button to reset the Print status to *Not Printed* so that the report can be printed again.

➔ **To change the owner of a report:**

1. Click the *Record Owner* down arrow and select a different owner from the list of user IDs.
2. PSA displays a confirmation message regarding the owner change; click the **Yes** button.

➔ **To change the status of a report:**

1. Click the *Current Status* down arrow and select a different status: *In Progress*, *Checked out for editing*, *Checked out for review*, *Pending approval*, *Approved*.

2. PSA displays a confirmation message regarding the status change; click the **Yes** button.

➡ **To view the events about a report:**

- Click the [View events for this record](#) hyperlink to open the *Incident Events* screen for this incident.

Common Search Incident Details

When you click the [View Incident Details](#) hyperlink on an *Incident Details* screen, you access a screen that provides detailed information about the incident.

Incident Number

Incident ID information– Incident Type Code, report status, date/time the incident was reported, clearance code, and officer name

Location information – street intersection names, type of location, type of premise, town name, state, and zip code.

Persons involved information – name, gender, race, date of birth, age (minimum and maximum), height & weight, status, and charge, if any.

Vehicle property involved information – registration number, VIN number, and year.

Non-vehicle property involved information – item, quantity, serial number

Narrative – from report filed Common Search Report Events

When you click the [View events for this record](#) hyperlink on an *Incident Details* screen, you access the *Incident Events* screen for that report.

The Incident Events screen presents a list of all the events that have occurred for the current report, and the user ID of the officer who performed each event. Each event listing includes:

- **Incident #** – the number of the incident
- **Date** – date and time the event occurred
- **Description** – brief description of the event. See the “List of Report Events” section for a list of all possible report events.
- **Details** – some events also include additional information about the event. For example, a status change event includes the new status in the Details field
- **By Whom** – user ID of officer/supervisor who performed or was involved in the event

Officer Events

The Officer Events report utility lets you search for report events by officer and date.

➔ **To execute an officer event search:**

1. In the navigation window on the left, click Management Reports, and then click Officer Events.

Officer Event Search

Enter search criteria

**Start Date/Time: 03 / 14 / 2001 15 : 24

Date/Time format: MM/DD/YYYY hh:mm

**End Date/Time: 03 / 15 / 2001 15 : 24

**Officer ID:

2. In the *Officer Event Search* screen, enter the search criteria required to retrieve a report:
3. In the *Start Date/Time* field, enter the beginning date for the report, in MM/DD/YYYY format and the time in HH:MM format.
4. In the *End Date/Time* field, enter the ending date for the report, in MM/DD/YYYY format and the time in HH:MM format.
5. In the *Officer ID* field, enter the user ID of the officer whose report events you want to view.
6. Click the **Search** button to run your search.

PSA searches for the report events that match the search criteria you've entered, and displays the results in the *Officer Events* screen.

Officer Events Query Results

Once you have entered your officer event search criteria and clicked the **Search** button on the *Officer Event Search* screen, PSA executes your search and returns the events found by your search in the *Officer Events* screen.

The *Officer Events* screen presents the following information about the report events found:

- **Search criteria statement** – the search criteria used to retrieve these events: the user ID and/or date range.
- **Date and time** – the date and time of the event.
- **Description** – description of the event. See the “List of Report Events” section for a list of all possible report events.
- **Incident number** – the number of the incident described in the report event, if applicable. Click the incident number to view details about this incident on the *Incident Details* screen.

Officer Event Incident Details

When you click an incident number on an *Officer Events* screen, you access the *Incident Details* screen for that report.

The *Incident Details* screen presents the following information about a report:

Report # – number assigned to this report

Record Owner – user ID of the report owner

Date Created – date and time the report was first created

Checked Out To – the user ID of the officer to whom the report is currently checked out, if any

Date Modified – date and time the report was last modified, if any

Record Approver – user ID of the supervisor who has approved the report, if any

Date Approved – date and time the report was approved, if any

Revision – number of times the report has been revised. An unrevised report has a revision number of 1

Date Transferred – date and time the report was transferred to the agency's internal Report Management System, if any

Current Status – current status of the report:

- *In Progress* – the report has been created but is not yet approved. It is not currently checked out to anyone
- *Checked out for editing* – report is checked out for editing by the owning officer
- *Checked out for review* – report is checked out for review by a supervisor
- *Pending approval* – report has been submitted for review
- *Approved* – report has been completed and approved by a supervisor. No more changes are allowed.

Date Printed – date and time the report was printed, if any. If the report has already been printed, you can click the Reset button to reset the Print status to Not Printed so that the report can be printed again.

➔ To change the owner of a report:

1. Click the *Record Owner* down arrow and select a different owner from the list of user IDs.
2. PSA displays a confirmation message regarding the owner change; click the **Yes** button.

➔ To change the status of a report:

1. Click the *Current Status* down arrow and select a different status: *In Progress*, *Checked out for editing*, *Checked out for review*, *Pending approval*, *Approved*.
2. PSA displays a confirmation message regarding the status change; click the **Yes** button.

➔ To view the events about a report:

- Click the [View events for this record](#) hyperlink to open the *Incident Events* screen for this incident.

Officer Event Incident Events

When you click the [View Incident Details](#) hyperlink on an *Incident Details* screen, you access a screen that provides detailed information about the incident.

Incident Number

Incident ID information– Incident Type Code, report status, date/time the incident was reported, clearance code, and officer name

Location information – street intersection names, type of location, type of premise, town name, state, and zip code.

Persons involved information – name, gender, race, date of birth, age (minimum and maximum), height & weight, status, and charge, if any.

Vehicle property involved information – registration number, VIN number, and year.

Non-vehicle property involved information – item, quantity, serial number

Narrative – from report filed

Officer Event Report Events

When you click the [View events for this record](#) hyperlink on an *Incident Details* screen, you access the *Incident Events* screen for that report.

The *Incident Events* screen presents a list of all the events that have occurred for the current report, and the user ID of the officer who performed each event. Each event listing includes:

Incident # – the number of the incident.

Date – the date and time the event occurred.

Description – a brief description of the event. See the “List of Report Events” section for a list of all possible report events.

Details – some events also include additional information about the event. For example, a status change event includes the new status in the *Details* field.

By Whom – user ID of officer/supervisor who performed or was involved in the event.

Officer Activity Summary

The Officer Activity Summary report utility lets you enter search criteria to generate a summary of activities by officer.

➔ **To perform an Officer Activity Summary search:**

1. In the navigation window on the left, click Management Reports, and then click Officer Activity Summary.

Officer Activity Summary

Enter search criteria

**Start Date/Time: 03 / 14 / 2001 15 : 24

Date/Time format: MM/DD/YYYY hh:mm

**End Date/Time: 03 / 15 / 2001 15 : 24

Search Reset

2. In the *Officer Activity Summary Search* screen, enter the search criteria required to retrieve a report:
3. In the *Start Date/Time* field, enter the beginning date of the officer activities to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
4. In the *End Date/Time* field, enter the ending date of the officer activities to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
5. Click the **Search** button to run your search.

PSA generates a summary of all the officer activities during the specified time period, and displays the results in the *Query Results* screen.

Officer Activity Summary Query Results

Once you have entered your search criteria in the *Officer Activity Summary Search* screen and clicked the **Search** button, PSA executes your search and displays the results of your search in the *Query Results* screen.

The *Query Results* screen presents the following information about the officer activity summary:

- **Search criteria statement** – the date range
- For each officer:
 - the user ID of the officer
 - a description of the activity and the number of times performed
 - the total number of activities performed

Audit COLLECT

The Audit COLLECT report utility lets you enter search criteria to generate a list of officers who ran a specific license plate, or the license plate numbers run by a specific officer, within a specified time period.

➔ **To perform an Audit COLLECT search:**

1. In the navigation window on the left, click [Management Reports](#), and then click [Audit COLLECT](#).

Collect Transaction Auditing

Enter search criteria

****Start Date/Time:** 01 / 14 / 2001 15 : 31

Date/Time format: MM/DD/YYYY hh:mm

****End Date/Time:** 03 / 15 / 2001 15 : 31

****Plate/Name:** 856MMG

2. In the *COLLECT Transaction Auditing* screen, enter the search criteria required to retrieve a report:
3. In the *Start Date/Time* field, enter the beginning date for the report, in MM/DD/YYYY format and the time in HH:MM format.
4. In the *End Date/Time* field, enter the ending date for the report, in MM/DD/YYYY format and the time in HH:MM format.

5. In the *Plate/Name/OLN/Vin* field, enter the license plate number or the name of the officer for which you want to view license plates run.
6. Click the **Search** button to run your search.

PSA generates a list of all the officers who ran the specified plate during the specified time period, or a list of all the license plates run by the specified officer during the specified time period, and displays the results in the *Query Results* screen.

Audit COLLECT Query Results

Once you have entered your search criteria in the *COLLECT Transaction Auditing* screen and clicked the **Search** button, PSA executes your search and displays the results of your search in the *Query Results* screen

The *Query Results* screen presents the following information about the COLLECT audit: **Search criteria statement** – the license plate number and date range.

For each instance the plate was run:

- the date and time the plate was run
- the town and agency of the officer who ran the plate
- the user ID of the officer who ran the plate

If you click the license plate number on the *Query Results* screen, you access a detailed report about vehicle registration checks made on the license plate number: COLLECT person/vehicle information, Motor Vehicle information, and NCIC Response information.

Audit Messaging

The Audit Messaging report utility lets you enter search criteria to generate a list of persons who sent a message within a specified time period, containing a specified piece of text.

To perform an audit messaging search:

1. In the navigation window on the left, click Management Reports, and then click Audit Messaging.

2. In the *Message Transaction Auditing* screen, enter the search criteria required to retrieve a report:
3. In the *Start Date/Time* field, enter the beginning date for the report, in MM/DD/YYYY format and the time in HH:MM format.
4. In the *End Date/Time* field, enter the ending date for the report, in MM/DD/YYYY format and the time in HH:MM format.
5. In the *Message Contents* field, enter the text string for which you want to search. If you want to search for all messages within the specified time frame, enter "a."
6. Click the **Search** button to run your search.

PSA generates a list of all the persons who sent a message that contains the specified text string during the specified time period, and displays the results in the *Query Results* screen.

Audit Messaging Query Results

Once you have entered your search criteria in the *Message Transaction Auditing* screen and clicked the **Search** button, PSA executes your search and returns information found by your search in the *Query Results* screen.

The *Query Results* screen presents the following information about the message audit:

Search criteria statement – the text search string and the date range.

For each message:

- the date and time the message was sent
- the town and agency of the person who sent the message
- the user ID of the person who sent the message

Click the user ID of a specific message in the *Query Results* screen to access the *Detailed Message Report* screen, which contains the following data about the selected message:

- End date/time – the date and time the message was sent
- From – the user ID of the sender of the message
- Subject – the message header
- Text – the body of the message
- Recipient – the user ID of the recipient of the message

Audit Officer Activity

The Audit Officer Activity report utility lets you enter search criteria to generate a list of activities performed by a specific officer during a specified time period.

➔ To perform an audit officer activity search:

1. In the navigation window on the left, click [Management Reports](#), and then click [Audit Officer Activity](#).

Activity By Officer

Enter search criteria

Officer ID	DDK				
**Start Date/Time:	03	/	14	/	2001 15 : 38
**End Date/Time:	03	/	15	/	2001 15 : 38

COLLECT
 CHAT
 Incident Reporting
 RMS Enquiry

2. In the *Activity By Officer* screen, enter the search criteria required to retrieve a report:
3. In the *Officer ID* field, enter the ID of the officer whose activity you want to view.
4. In the *Start Date/Time* field, enter the beginning date for the report, in MM/DD/YYYY format and the time in HH:MM format.
5. In the *End Date/Time* field, enter the ending date for the report, in MM/DD/YYYY format and the time in HH:MM format.
6. Select the type of activity to view: COLLECT, Messaging, Incident Reporting, or RMS Enquiry.

- Click the **Search** button to run your search.

PSA generates a list of activities performed by the specified officer for the specified utility.

Audit Officer Activity Query Results

Once you have entered your search criteria in the *Activity By Officer* screen and clicked the **Search** button, PSA executes your search and returns information found by your search in the *Query Results* screen.

The *Query Results* screen presents the following information about the officer activity audit:

- **Search criteria statement** – the officer's user ID, the utility, and the date range
- For each activity performed by the officer:
 - the date and time the activity was performed
 - the Backend / CAPTAIN Switch application
 - the Message / activity that was performed

Agency Activity Summary

The Audit Agency Activity report utility lets you enter search criteria to generate a list of activities performed in specific Agencies during a specified time period.

➔ **To perform an audit Agency activity search:**

- In the navigation window on the left, click [Management Reports](#), and then click [Audit Agency Activity](#).

Agency Activity

Enter search criteria

** Start Date/Time: / / :

Date/Time format: MM/DD/YYYY hh:mm

** End Date/Time: / / :

- In the *Activity By Agency* screen, enter the search criteria required to retrieve a report:

3. In the *Start Date/Time* field, enter the beginning date of the Agency activity to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
4. In the *End Date/Time* field, enter the ending date of the Agency activity to retrieve, in MM/DD/YYYY format and the time in HH:MM format.
5. Click the **Search** button to run your search.

PSA generates a list of the activities performed, by Agency, for the specified time period.

Audit Agency Activity Query Results

Once you have entered your search criteria in the *Activity By Agency* screen and clicked the **Search** button, PSA executes your search and returns information found by your search in the *Query Results* screen.

The *Query Results* screen presents the following information about the Agency activity audit:

Search criteria statement – the date range

For each activity:

- Transaction / the type of activity performed
- Messages Sent / number of times the activity was performed
- Total / total for all activities for the agency where the activity was performed

PSA MESSAGES

PSA error messages indicate that a backend application is not working correctly, or that a user has performed an illegal operation, entered incomplete data, entered an illegal parameter, or specified an incorrect system configuration.

Msg No.	Error Message	Description	Action
MWS00001	User does not have the privilege required to update the Agency.	A user must be a System Administrator to update Agency fields.	Change the privilege assigned to the user role or group.
MWS00002	Could not update Agency. Another Agency with code <code> already exists.	You cannot have duplicate Agency codes in the switch. The system requires that Agency codes be unique.	Change the Agency code and try again.
MWS00003	User does not have the privilege required to get the list of users in the Agency.	A user must have the appropriate privilege to request the user list.	Change the privilege assigned to the user role or group.
MWS00004	A required value is missing. The following values cannot be empty: User ID, Password, or Last Name.	You cannot add a user with any required fields empty.	Fill in all required fields.
MWS00005	User creation failed. Another user currently exists with the same User ID ('<userid>').	You cannot use duplicate User IDs. The system requires that User IDs be unique.	Create a unique User ID.
MWS00006	User does not have the privilege required to add a user.	A user must have the appropriate privilege to create a user.	Change the privilege assigned to the user role or group.
MWS00007	Add User ('<userid>') Failed. Failed adding to the User Catalog.	The switch could not create the user in NT, or add the user to the database, or add the user to the internal catalogs.	Most likely there is an NT user with this ID that is not a user of the system. Either delete the NT user with NT User Manager, or use a different user ID.
MWS00008	Invalid Agency.	ASP code has an error. You will never get this error unless the ASP code attempts to access an un-initialized object.	Contact your System Administrator.

Msg No.	Error Message	Description	Action
MWS00009	A required value is missing. The following values cannot be empty: Agency Name, Agency Code, Town Name, Town Code, or Agency Type.	You cannot update an Agency with any required fields empty.	Fill in all required fields.
MWS00010	Update Agency failed.	Internal failure. The system could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00011	User does not have the privilege required to delete a user.	A user must have the appropriate privilege to delete a user.	Change the privilege assigned to the user role or group.
MWS00012	Delete User Failed. Failed deleting from the User Catalog.	The switch could not delete the user from NT, or modify the database, or modify the internal catalogs.	Contact your System Administrator.
MWS00013	A required value is missing. The following value cannot be empty: Group Name.	You cannot update or create a group with this required field empty.	Fill in all required fields.
MWS00014	User does not have the privilege required to add a group to the Agency.	A user must have the appropriate privilege to add a group.	Change the privilege assigned to the user role or group.
MWS00015	Group creation failed. Another Group with name <group name> already exists	You cannot have duplicate group names within an Agency.	Define a unique group name within the Agency.
MWS00016	Failed to add a group to the Agency. Failed adding to group catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00017	User does not have the privilege required to delete a group from the Agency.	A user must have the appropriate privilege to delete a group.	Change the privilege assigned to the user role or group.
MWS00018	Could not delete group.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00019	User does not have the privilege required to add a DataSource to the Agency.	A user must have the appropriate privilege to add a DataSource.	Change the privilege assigned to the user role or group.
MWS00020	A required value is missing. The following values cannot be empty: DataSource Logon ID Key, DataSource Type.	You cannot update or create a DataSource with any required fields empty.	Fill in all required fields.

Msg No.	Error Message	Description	Action
MWS00021	DataSource creation failed. Invalid authorized user - not a DataSource user.	You cannot create a DataSource without creating a logon ID first.	Create a DataSource logon ID.
MWS00022	DataSource creation failed. Could not add to DataSource catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00023	User does not have the privilege required to get the list of groups in the Agency.	A user must have the appropriate privilege to get the list of groups.	Change the privilege assigned to the user role or group.
MWS00024	User does not have the privilege required to add a DataSource user to the Agency.	A user must have the appropriate privilege to add a DataSource logon ID.	Change the privilege assigned to the user role or group.
MWS00025	A required value is missing. The following values cannot be empty: Logon ID, Password, and DataSource Type.	You cannot update or create a DataSource logon ID with any required fields empty.	Fill in all required fields.
MWS00026	DataSource user creation failed. Another DataSource user currently exists with the same Logon ID.	You cannot have duplicate logon IDs.	Define a unique logon ID for the DataSource.
MWS00027	DataSource user creation failed. Unable to create an authorized user for the DataSource.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00028	Could not add DataSource user to DataSource Group. Please contact your system administrator.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00029	DataSource user creation failed. Failed adding to DataSource catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00030	DataSource creation failed. Invalid authorized user.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00031	User does not have the privilege required to get a list of DataSources in the Agency.	A user must have the appropriate privilege to get the list of DataSources.	Change the privilege assigned to the user role or group.
MWS00032	User does not have the privilege required to get a list of DataSource Logon IDs in the Agency.	A user must have the appropriate privilege to get the list of DataSource logon IDs.	Change the privilege assigned to the user role or group.

Msg No.	Error Message	Description	Action
MWS00033	User does not have the privilege required to delete a DataSource in the Agency.	A user must have the appropriate privilege to delete a DataSource.	Change the privilege assigned to the user role or group.
MWS00034	DataSource was not deleted.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00035	User does not have the privilege required to delete a DataSource Logon ID in the Agency.	A user must have the appropriate privilege to delete a DataSource logon ID.	Change the privilege assigned to the user role or group.
MWS00036	DataSource Logon ID was not deleted.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00037	Invalid DataSource.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00038	Invalid User.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00039	A required value is missing. The following values cannot be empty: Last Name, First Name.	You cannot update a user with any required fields empty.	Fill in all required fields.
MWS00040	User does not have the privilege required to update the user.	A user must have the appropriate privilege to update a user.	Change the privilege assigned to the user role or group.
MWS00041	Could not update user.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00042	User does not have the privilege required to request the list of roles assigned to a user.	A user must have the appropriate privilege to get a list of security roles.	Change the privilege assigned to the user role or group.
MWS00043	GetAgencyName failed. Invalid Agency associated with user.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00044	User does not have the privilege required to reset a user's password.	A user must have the appropriate privilege to change a password.	Change the privilege assigned to the user role or group.
MWS00045	The password cannot be blank.	You cannot create a blank password.	Fill in the password.

Msg No.	Error Message	Description	Action
MWS00046	Password change failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00047	Invalid Group.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00048	User does not have the privilege required to modify a group.	A user must have the appropriate privilege to modify a group.	Change the privilege assigned to the user role or group.
MWS00049	Grant Privilege failed. Privilege not found in catalog.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00050	Group already has privilege.	You cannot add a privilege to a group if the group already has that privilege.	Verify the privilege assignment.
MWS00051	Grant Privilege failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00052	User does not have the privilege required to get the list of privileges.	A user must have the appropriate privilege to get the list of privileges.	Change the privilege assigned to the user role or group.
MWS00053	Remove Privilege failed. Privilege not found in catalog.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00054	Group has not been granted privilege.	You cannot remove a privilege if it has not been granted to the group.	Verify the privilege assignment.
MWS00055	Remove Privilege failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00056	Add user to group failed. User not found in catalog.	Client program error - trying to access an invalid object.	Contact your System Administrator
MWS00057	Add user to group failed. User already a member of group.	You cannot add a user to a group if s/he is already a member of that group.	Verify user group assignment.
MWS00058	Add user to group failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00059	Remove user from group failed. User not found in catalog.	Client program error - trying to access an invalid object.	Contact your System Administrator.

Msg No.	Error Message	Description	Action
MWS00060	Remove user from group failed. User not a member of group.	You cannot remove a user from a group if s/he is not a member of that group.	Verify user group assignment.
MWS00061	Remove user from group failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00062	A required value is missing. The following value cannot be empty: Name.	You cannot update a group with this required field empty.	Fill in all required fields.
MWS00063	Update group failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00064	Invalid privilege.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00065	A required value is missing. The following values cannot be empty: Name, Code.	You cannot update or create a privilege with any required fields empty.	Fill in all required fields.
MWS00066	User does not have the privilege required to update the privilege.	A user must have the appropriate privilege to update privileges.	Change the privilege assigned to the user role or group.
MWS00067	Update privilege failed.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00068	Invalid Session.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00069	GetAgencyName failed. Invalid agency associated with session.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00070	User does not have the privilege required to force off a user.	A user must have the appropriate privilege to force of users.	Change the privilege assigned to the user role or group.
MWS00071	Cannot force off a non-client session.	You cannot force off backend applications.	Select to force off a user ID only.
MWS00072	You must logon before attempting this function.	Client program error - trying to access an object before authenticating the user.	Contact your System Administrator.
MWS00073	User does not have the privilege required to request an Agency list.	A user must have the appropriate privilege to request an Agency list.	Change the privilege assigned to the user role or group.

Msg No.	Error Message	Description	Action
MWS00074	Authentication failed for user. User ID field is empty.	You cannot authenticate without a valid User ID.	Fill in the User ID.
MWS00075	Authentication failed. Bad user ID or password.	You cannot authenticate without a valid User ID or password.	Re-enter the User ID or password. If this fails, contact the System or Agency Administrator.
MWS00076	User does not have the privilege required to logon as an administrator.	A user must have the appropriate privilege to logon as an administrator.	Change the privilege assigned to the user role or group.
MWS00077	A required value is missing. The following values cannot be empty: Agency Name, Agency Code, Agency Type, Town Name, Town Code.	You cannot create or update an Agency with any required fields empty.	Fill in all required fields.
MWS00078	User does not have the privilege required to add an Agency.	A user must have the appropriate privilege to add an Agency.	Change the privilege assigned to the user role or group.
MWS00079	Agency creation failed. Agency code <'code'> already exists.	You cannot have duplicate Agency codes.	Change the Agency code.
MWS00080	Agency creation failed. Could not add Agency to catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00081	Security Role creation failed. Role name cannot be blank.	You cannot leave a role name blank.	Define a unique security role name.
MWS00082	User does not have privilege required to add a security role.	A user must have the appropriate privilege to add a security role.	Change the privilege assigned to the user role or group.
MWS00083	Security Role creation failed. Security Role already exists.	You cannot have duplicate security roles.	Define a unique security role name.
MWS00084	Security Role creation failed. Could not add role to catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00085	User does not have privilege required to delete a security role.	A user must have the appropriate privilege to delete a security role.	Change the privilege assigned to the user role or group.

Msg No.	Error Message	Description	Action
MWS00086	Could not delete security role.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00087	User does not have the privilege required to deactivate the Agency.	A user must have the appropriate privilege to deactivate an Agency.	Change the privilege assigned to the user role or group.
MWS00088	Agency could not be deactivated.	Agency must not have any users or groups defined in order to deactivate.	Verify that all users and groups have been removed from the Agency prior to deactivating.
MWS00089	User does not have the privilege required to add a global DataSource user.	A user must have the appropriate privilege to add a global DataSource user.	Change the privilege assigned to the user role or group.
MWS00090	Global DataSource user creation failed. DataSource group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00091	Global DataSource user creation failed. Another DataSource user currently exists with the same Logon ID.	You cannot have duplicate DataSource Logon IDs.	Define a unique DataSource Logon ID.
MWS00092	Global DataSource user creation failed. Unable to create an authorized user for the DataSource.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00093	Global DataSource user creation failed. Could not add user to DataSource group.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00094	Global DataSource user creation failed. Could not add to DataSource catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00095	User does not have the privilege required to get a list of global DataSources.	A user must have the appropriate privilege to get a global DataSource list.	Change the privilege assigned to the user role or group.
MWS00096	User does not have the privilege required to delete a global DataSource.	A user must have the appropriate privilege to delete a global DataSource.	Change the privilege assigned to the user role or group.
MWS00097	Global DataSource was not deleted.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.

Msg No.	Error Message	Description	Action
MWS00098	User does not have the privilege required to add a privilege.	A user must have the appropriate privilege to add a privilege.	Change the privilege assigned to the user role or group.
MWS00099	Privilege creation failed. Could not add to privilege catalog.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00100	User does not have the privilege required to get the list of privileges.	A user must have the appropriate privilege to get a list of privileges.	Change the privilege assigned to the user role or group.
MWS00101	User does not have the privilege required to get the list of privileges in a restricted category.	A user must have the appropriate privilege to get a list of privileges in a restricted category.	Change the privilege assigned to the user role or group.
MWS00102	User does not have the privilege required to delete a privilege.	User must have the appropriate privilege to delete a privilege.	Change the privilege of the user role or group.
MWS00103	Could not delete privilege.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00104	User does not have the privilege required to enable a System Administrator.	A user must have the appropriate privilege to enable a System Administrator.	Change the privilege of the user role or group.
MWS00105	Enable System Administrator failed. Invalid user.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00106	Enable System Administrator failed. System Administrator group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00107	User already a System Administrator.	You cannot define user as a System Administrator if the user already has that privilege.	Verify administrative privileges.
MWS00108	Enable System Administrator failed. Agency Administrator group not found. Cannot check if user is Agency Administrator.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.

Msg No.	Error Message	Description	Action
MWS00109	User is currently an Agency Administrator. Disable the user as an Agency Administrator before attempting to make them a System Administrator.	You cannot define user as a System Administrator if the user already has Agency Administrative privileges.	Verify administrative privileges.
MWS00110	Enable System Administrator failed. Could not add user to System Administrator group.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00111	User does not have the privilege required to enable an Agency Administrator.	A user must have the appropriate privilege to enable an Agency Administrator.	Change the privilege assigned to the user role or group.
MWS00112	Enable Agency Administrator failed. Invalid user.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00113	Enable Agency Administrator failed. Agency Administrator group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00114	User already an Agency Administrator.	You cannot define a user as an Agency Administrator if the user already has that privilege.	Verify administrative privileges.
MWS00115	Enable Agency Administrator failed. System Administrator group not found. Cannot check if user is System Administrator.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00116	User is currently a System Administrator. Disable the user as a System Administrator before attempting to make the user an Agency Administrator.	You cannot define a user as a System Administrator if the user already has Agency Administrator privileges.	Verify administrative privileges.
MWS00117	Enable Agency Administrator failed. Could not add user to Agency Administrator group.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00118	User does not have the privilege required to disable a System Administrator.	A user must have the appropriate privilege to disable a System Administrator.	Change the privilege assigned to the user role or group.

Msg No.	Error Message	Description	Action
MWS00119	Disable System Administrator failed. Invalid user.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00120	Disable System Administrator failed. System Administrator group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00121	Disable System Administrator failed.	You cannot disable a user as a System Administrator if the user does not have that privilege.	Verify administrative privileges.
MWS00122	Disable System Administrator failed. Could not remove user from System Administrator group.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00123	User does not have the privilege required to disable an Agency Administrator.	A user must have the appropriate privilege to disable an Agency Administrator.	Verify administrative privileges.
MWS00124	Disable Agency Administrator failed. Invalid user.	Client program error - trying to access an invalid object.	Contact your System Administrator.
MWS00125	Disable Agency Administrator failed. Agency Administrator group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00126	Disable Agency Administrator failed.	You cannot disable a user as an Agency Administrator if the user does not have that privilege assigned	Verify administrative privileges.
MWS00127	Disable Agency Administrator failed. Could not remove user from Agency Administrator group.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00128	User does not have the privilege required to request the list of System Administrators.	A user must have the appropriate privilege to get the list of System Administrators.	Change the privilege assigned to the user role or group.
MWS00129	Get System Administrators failed. System Administrator group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.

Msg No.	Error Message	Description	Action
MWS00130	User does not have the privilege required to request the list of Agency Administrators.	A user must have the appropriate privilege to get the list of Agency Administrators.	Change the privilege assigned to the user role or group.
MWS00131	Get Agency Administrators failed. Agency Administrator group not found.	Internal failure. The switch could not update the database or its internal catalogs.	Contact your System Administrator.
MWS00132	User does not have the privilege required to add a global DataSource.	A user must have the appropriate privilege to add a global DataSource.	Change the privilege assigned to the user role or group.
MWS00133	User does not have the privilege required to get a list of global DataSources.	A user must have the appropriate privilege to get the list of global DataSources.	Change the privilege assigned to the user role or group.
MWS00134	User does not have the privilege required to delete a global DataSource logon ID.	A user must have the appropriate privilege to delete a global DataSource logon ID.	Change the privilege assigned to the user role or group.
AIBE00001	ERROR: Request operation is not supported in this version.	The request sent in is attempting to use an unimplemented feature. Currently, the only way this occurs is if the user attempts to use the "MoreItemsRequestKey" parameter. This can only be done if the person writes the HTML pages that submit the query.	Contact your System Administrator.
AIBE00002	ERROR: Unable to unserialize message sent to Inquiry Backend. Transaction Code: %1!d! Tracking Number: %2 Message ID: %3!d!"	The message sent in was corrupted or otherwise unable to be parsed by the Inquiry Backend.	Contact your System Administrator.
AIBE00010	ERROR: SQL Log Database is currently unavailable. Please try your query again later.	The database server is unreachable or improperly configured within the Inquiry Backend setup.	Contact your System Administrator.
AIBE00011	ERROR: Unable to obtain a connection to the SQL Log database. Please try your query again later.	The Inquiry Backend was unable to establish a connection with the database server. The server is probably down or mis-configured.	Contact your System Administrator.

Msg No.	Error Message	Description	Action
AIBE00012	ERROR: Unable to access the inquiry sets table.	The database supplied in the Inquiry Backend configuration is not set up for use by the Inquiry Backend. More specifically, the database is missing the "InquirySets" table.	Contact your System Administrator.
AIBE00013	ERROR: Failure accessing SQL database table.	Inquiry Backend was unable to read a table's contents. More information, such as the table name, is supplied in the Inquiry Backend's trace log. This message primarily relates to an inability to read the InquirySets table.	Contact your System Administrator.
AIBE00014	ERROR: Failure obtaining SQL result set.	A result set was unreadable. This occurs in three situations: 1) The InquirySets table provided is not in the correct format; 2) The Stored Procedure executed for the query failed; or 3) The arguments provided to the Stored Procedure were incorrect. This can occur if the HTML submission form contains typos in the argument names.	Contact your System Administrator.
AIBE00015	ERROR: Unable to access stored database stored procedure.	The InquirySets table is configured to run a non-existent Stored Procedure.	Contact your System Administrator.
AIBE00016	ERROR: User unrecognized (no 1004 sent for session?)	The Inquiry Backend received a request from an unknown user. The users are recognized if and only if the Inquiry Backend has received a Notification of Logon message from the switch, but has not yet received a Notification of Logoff message for that user.	Contact your System Administrator.
AIBE00017	ERROR: Unable to find entry for DataSource/Subset.	The Inquiry Backend has not been configured to support the subset (i.e., the database) supplied in the request.	Contact your System Administrator.
AIBE00018	ERROR: Insufficient privilege for request.	This is the only message that users should receive. This means the user is not a member of a role or group that contains the necessary privileges to run this query. Privileges are specified in the InquirySets table within each database.	Contact your System Administrator.