PremierOne™ Provisioning

User Guide

Version 3.3

Motorola Solutions Confidential

September 2013

© 2013 Motorola Solutions, Inc. All rights reserved.

BN 0601-90153

Copyrights

The Motorola products described in this document may include copyrighted Motorola computer programs stored in semiconductor memories or other media.

Laws in the United States and other countries preserve for Motorola certain exclusive rights for copyright computer programs, including the exclusive right to copy or reproduce in any form the copyright computer program. Accordingly, any copyright Motorola computer programs contained in the Motorola products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola. Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola, except for the rights that arise by operation of law in the sale of a product.

Confidentiality

You acknowledge and agree that the Software, including its structure, organization, design, and Documentation, contains and constitutes proprietary trade secrets and confidential information of Motorola Solutions (the “Confidential Information”). You agree to take all steps reasonably necessary to maintain and protect the Confidential Information in the strictest confidence for the benefit of Motorola Solutions, including by instruction to or agreement with all persons authorized to have access to the Documentation under this Agreement.

Restrictions

The software described in this document is the property of Motorola. It is furnished under a license agreement and may be used and/or disclosed only in accordance with the terms of the agreement. Software and documentation are copyright materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Motorola.

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Motorola assumes no liability resulting from any inaccuracies or omissions in this document, or from the use of the information obtained herein. Motorola reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Motorola does not assume any liability arising out of the application or use of any product or circuit described herein; neither does it convey license under its patent rights of others.

Trademarks

Motorola, Moto, Motorola Solutions, PremierOne, and the stylized M logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

Microsoft, Windows, Windows XP, Windows Vista, Windows 7, and Windows Server are registered trademarks of Microsoft Corporation. All other product or service names are the property of their respective owners.

Build date: September 3, 2013

Contents

List of Tables

Chapter 1: Introduction

What Is In This Book. . . . 1-1
Related Documents . . . 1-3
About the Conventions Used in This Guide . . . 1-4
- Keyboard Conventions . . . 1-4
- Typographic Conventions . . . 1-5
- Notes and Cautions . . . 1-5
- Contacting Technical Support. . . . 1-5

Using Motorola Online . . . 1-6

Chapter 2: Getting Started With Provisioning

Logging in to Provisioning . . . 2-1
Overview of the Provisioning Window . . . 2-4
Overview of the Work Area . . . 2-5
Using Filters . . . 2-7
Searching for Records . . . 2-9
Working With Configuration Items. . . . 2-9
- Adding Configuration Items by Cloning . . . 2-10
- Modifying Configuration Items . . . 2-11
- Deleting Configuration Items . . . 2-11
- Exporting Configuration Items . . . 2-12
- Importing Configuration Items . . . 2-13

Logging Out of Provisioning. . . . 2-15

Chapter 3: Provisioning CAD and Mobile

Provisioning CAD . . . 3-1
Provisioning Mobile . . . 3-3
Levels of Provisioning. . . . 3-5
Tables of Field Interdependencies. . . . 3-11
Diagrams of Field Interdependencies . . . 3-23
- Incident Management Field Interdependencies . . . 3-24
- Resource Management Field Interdependencies. . . . 3-26
- Recommendations Field Interdependencies . . . 3-27
- Interfaces Field Interdependencies . . . 3-28

Chapter 4: Configuring Agencies and Agency Types

Configuring Agency Types . . . 4-2
- Adding Agency Types . . . 4-2

Configuring Agencies 4-3
Adding Agencies 4-4
Adding Agencies by Cloning 4-6

Chapter 5: Configuring Trusted Agencies

Commands Exempt from Trusted Agency Provisioning 5-2
Understanding Permission Sets 5-2
Configuring Trusted Agencies 5-3
Adding Permission Sets 5-3
Setting Permissions Within a Permission Set 5-5
Setting CAD Command Access for Trusted Agencies 5-6
Setting Provisioning Access for Trusted Agencies 5-7
Granting Role Permissions by Owning Agencies 5-9
Setting CAD Command Access for Roles 5-10
Setting Provisioning Access for Roles 5-11

Chapter 6: Configuring Lists and Codes

Understanding Global Codes 6-1
Configuring Standard Lists 6-2
Configuring New Lists and List Items 6-6
Adding Lists and Codes 6-6
Adding General List Information 6-6
Adding Codes to Lists 6-7
Previewing Code Lists 6-8
Configuring Active Directory for Authentication 6-9
Prerequisites 6-10
Configuring AD Authentication 6-10

Chapter 7: Configuring Plans

Overview of Plans 7-1
Configuring Plans 7-2
Adding Plans 7-2
Modifying a Plan 7-4
Setting the Active Plan 7-5
Viewing the Current Plan 7-6

Chapter 8: Configuring Role Permissions

Configuring Roles 8-2
Adding Roles 8-2
Adding Role General Information 8-2
Adding Role Permissions 8-5
Adding Role Permissions for Mobile Users 8-11
Viewing a Role Preview 8-13
Adding Resources to Roles 8-13
Adding Reporting Permissions 8-16

Chapter 9: Configuring Authentication

Configuring Agency Authentication Settings 9-2

Configuring General Agency Authentication Settings 9-2
Configuring Passwords for Your Agency 9-6
Enabling the Emergency Mode 9-8
Configuring System Notifications 9-9
Forcing Password Changes 9-11

Chapter 10: Configuring Unit Management

Configuring Units 10-2
Adding Unit IDs 10-2
Configuring Unit Preassignments 10-4
Adding New Unit Preassignments 10-4
Adding Unit General Preassignments 10-4
Adding Personnel and Unit Vehicle Information 10-6
Adding Unit Equipment Information 10-7
Adding Unit Capabilities Information 10-8
Adding Capability Settings 10-9
Configuring Unit Status Codes 10-11
Adding Unit Status Codes 10-11
Adding Unit Status Code Properties Information 10-11
Adding Unit Status Code Timeout Information 10-13
Adding Mobile/Handheld Status Codes 10-15
Configuring Handheld Status Code Sequences 10-17
Configuring Cross Staffing Groups 10-19
Understanding Cross Staffing and Unit Status 10-19
Adding Cross Staffing Groups 10-20
Configuring Unit Management Settings 10-21
Configuring Command Line Numbers 10-22
Configuring Shift ID Code Information 10-23
Configuring Unit Status Transaction 10-24
Configuring Activity Codes 10-29
Adding Activity Codes 10-29
Configuring Duty Types 10-30
Adding Duty Types 10-31
Configuring Move Ups 10-32

Chapter 11: Configuring Resources

Configuring Capability Groups 11-2
Adding Capability Groups 11-3
Configuring Capabilities/Skills 11-4
Capabilities Overview 11-4
Provisioning Capabilities 11-5
Adding Capabilities/Skills 11-6
Configuring Personnel 11-7
Adding Personnel Records 11-8
Adding Personnel Detail Information 11-8
Adding Personnel Contact Information 11-11
Adding Personnel Roles Information 11-13
Adding Personnel Authorization Information 11-14
Adding Personnel Resource Assignment Information 11-16

Adding Personnel Preassignments 11-18
Configuring Vehicles 11-20
Configuring Device Profiles 11-22
Configuring Device Profiles General Information 11-22
Configuring Device Profiles BOLO Content 11-24
Configuring Device Profiles Emergency Content 11-26
Configuring Device Profile Incident Content 11-27
Configuring Device Profile Message Content 11-28
Configuring Device Profile Hot Hit Notification Content 11-30
Configuring Device Profile Query Content 11-31
Configuring System Address Message Type Indicators 11-33
Configuring Device Types 11-34
Modifying Device Types 11-34
Adding Device Type General Information 11-35
Adding Device Type Login Information 11-36
Adding Device Type Printers 11-38
Adding Device Type Permissions 11-39
Adding Equipment 11-41
Configuring Devices 11-43
Configuring Workstation/MDT/Handheld Devices 11-43
Adding Workstation/MDT/Handheld General Information 11-44
Adding Login Settings Information 11-46
Adding Permissions Information 11-50
Adding Interface Settings 11-52
Configuring Radios 11-55
Adding Radios 11-55
Configuring Two-Tone Radio Groups 11-57
Configuring Pagers 11-58
Adding Pagers 11-59
Configuring Pager Groups 11-60
Adding Pager Groups 11-60
Configuring Printer Devices 11-61
Configuring a Tear and Run Printer in a High Availability (HA) Environment 11-63
Configuring GPS Devices 11-64
GPS Through PremierOne Mobile 11-65
Direct GPS 11-65
Adding GPS Devices 11-65
Configuring Systems 11-67
Adding Systems 11-67

Chapter 12: Call Control

Configuring General Call Control Settings 12-2
Configuring the Debounce Factor 12-3
Configuring Incoming Line Types and Lines 12-4
Configuring Incoming Line Types 12-5
Configuring Incoming Lines 12-6
Managing Incorrect ALI Records 12-7
Configuring Intelligent Transfer Settings 12-9
Configuring Intelligent Transfer Service Provider Types 12-9

Configuring Intelligent Transfer Service Providers 12-11
Configuring Intelligent Transfer ESN Recommendations 12-16
Configuring Intelligent Transfer Line Recommendations 12-17
Understanding the Recommended Service Provider Display 12-18
Configuring Preprogrammed Messages 12-19
Configuring the Call Control Window 12-22
Configuring General Settings for the Call Control Center Window 12-22
Configuring Queue Buttons for the Call Control Center Window 12-24
Configuring Permissions for the Call Control Window 12-25

Chapter 13: Configuring Incident Management

Configuring Coverage Groups 13-2
Adding Coverage Groups 13-2
Configuring Incident Type Codes 13-4
Adding Incident Type Codes 13-4
Adding Incident Type Aliases 13-6
Configuring Modifying Circumstance Codes 13-8
Adding Modifying Circumstances Codes 13-8
Configuring Service Settings 13-10
Service Settings 13-10
Configuring Service Defaults 13-10
Configuring Initiation Defaults 13-15
Rules for Traffic Stop and Field-Initiated Incidents 13-21
Configuring Search Defaults 13-23
Configuring Priorities 13-25
Configuring Incident Timeouts 13-26
Configuring Priority Updates 13-28
Configuring Priority Updates – Mobile 13-30
Configuring Mobile/Handheld Incident Settings 13-32
Configuring Mobile/Handheld Priority Alert Settings 13-33
Configuring Mobile/Handheld Priority Alert Settings for Incident Dispatch 13-33
Configuring Mobile Priority Alert Settings for Incident Updates 13-35
Configuring Incident Response Factors 13-37
Adding IRF General Information 13-37
Adding IRF Attributes 13-39
Configuring Dispositions 13-43
Adding Disposition Codes 13-43
Configuring Response Messages 13-45
Adding Response Message Subject and Text Settings 13-46
Adding Response Message Area, Sector, and Beat Settings 13-47
Adding Response Message Locations Settings 13-48
Adding Response Message Incident Types Settings 13-49
Configuring Incident Source Codes 13-50
Adding Incident Source Codes 13-50
Setting the Default Source Codes 13-52
Configuring Premise/Hazard Types and Records 13-53
Configuring Premise/Hazard Types and Proximities 13-53
Configuring Premise/Hazard Settings 13-56
Configuring Premise Hazard Records 13-58

Adding Premise/Hazard Records 13-58

Chapter 14: Configuring Unit Recommendations

Configuring Response Cards 14-2
Adding Incident Response Factors to Response Cards 14-2
Adding Response Cards for IRFs or Response IDs – General Subtab 14-3
Adding Response Cards for IRFs or Response IDs – Response Subtab 14-6
Copying Response Cards 14-10
Configuring Response Modes 14-11
Adding Response Modes 14-11
Configuring Response Classes 14-13
Adding Response Classes 14-13
Configuring Response IDs 14-15
Adding Response IDs 14-15
Configuring Response Descriptors 14-17
Adding Response Descriptors 14-17
Configuring Run Cards 14-19
Searching for Run Cards 14-19
Adding Run Cards 14-20
Adding Run Card Order Information 14-20
Adding Run Card Response ID Information 14-23
Adding Run Card IRF Information 14-24
Copying Run Cards 14-26
Breaking Ties on a Run Card 14-27
Configuring Unit Recommendations Settings 14-27
Logging Unit Recommendations 14-28
Holding Units for Dispatch 14-29
Setting the Sort Order for Capabilities 14-31
Setting the Sort Order for Duty Types 14-32
Setting the Maximum Speed for ARL Recommendations for a Vehicle Type 14-34
Configuring Response Categories 14-36
Adding Response Categories 14-36

Chapter 15: Configuring Contractor Rotation

Configuring General Contractor Information 15-2
Adding Contractor Types 15-2
Adding Contractor Capabilities 15-4
Modifying Contractor Action Codes 15-6
Provisioning Auto Club Affiliations and Payment Methods 15-8
Configuring Individual Contractors Information 15-8
Adding New Contractors 15-9
Adding General Contractor Contact Information 15-9
Adding Contractor Address Information 15-13
Setting Contractor Type and Availability 15-15
Configuring Contractor Rotations 15-16
Adding New Rotations 15-16
Creating Default Rotations 15-20

Chapter 16: Customizing the User Interface

Configuring the Mobile Interface 16-2
Configuring the Mobile Services Areas 16-4
Configuring the Mobile Action Bar 16-5
Configuring Mobile Option Buttons 16-7
Configuring the Mobile Navigation Bar 16-10
Configuring the Mobile Status Bar 16-13
Configuring the Mobile Address Book and Login Icons 16-14
Configuring the Mobile Command Line 16-17
Configuring Mobile Text-to-Speech 16-18
Enabling Text-To-Speech 16-19
Selecting the Speaking Voice 16-20
Adding Voices 16-21
Selecting Query Fields 16-22
Selecting Incident Management Fields 16-22
Selecting Messaging Fields 16-24
Selecting BOLO Fields 16-25
Selecting Chat Text-To-Speech Fields 16-26
Configuring Function Keys for CAD and Mobile 16-28
Configuring Function Keys for CAD 16-28
Configuring the Soft Function Keys for Mobile 16-30
Configuring Motorola MW810 Programmable Buttons 16-32
Configuring Data Elements 16-34

Chapter 17: Configuring CAD Display Settings

Configuring CAD WAA Settings 17-1

Chapter 18: Configuring Address Books and Groups

Configuring Address Books 18-1
Adding Address Books 18-2
Adding Address Book General Information 18-2
Adding Existing Entries to Address Books 18-5
Adding New Entries to Address Books 18-8
Viewing Contacts in the Address Books 18-11
Configuring Groups 18-12
Adding Groups 18-12
Adding Group General Information 18-12
Adding Existing Entries to a Group 18-15
Adding New Entries to a Group 18-17

Chapter 19: Configuring Alarms

Configuring Alarm Companies 19-1
Adding Alarm Companies 19-1
Configuring Alarm Records 19-3
Adding Alarm Records 19-3
Adding Alarm Records General Information 19-4
Adding Alarm Records Incident Information 19-6
Configuring Chronic Alarm Settings 19-9

Viewing False Alarms 19-10

Chapter 20: Configuring Chat Rooms

Configuring Chat Permissions 20-1
Setting Agency-Level Chat Permissions 20-2
Setting Agency Type Permissions 20-4
Configuring Chat Settings 20-5
Configuring Chat Settings 20-5
Configuring Chat Status Settings 20-5
Configuring General Chat Settings 20-7
Configuring Chat Rooms 20-9
Adding Chat Rooms 20-9
Adding General Chat Room Settings 20-9
Adding Chat Room Member Properties 20-11
Adding Members to Chat Rooms 20-12

Chapter 21: Configuring the Command Line

Configuring Commands 21-1
Configuring Identifiers 21-7
Configuring Separators 21-8
Configuring Command Line Behaviors 21-10

Chapter 22: Configuring Interfaces

Configuring the Alerting Interface 22-1
Configuring Alerting Settings 22-3
Configuring an Agency Alerting Scheme 22-7
Configuring and Enabling Existing Toning Systems at the Agency Level 22-8
Configuring Alerts for In-Station 22-10
Configuring Alerts for Out-of-Station 22-12
Configuring Unit-Based Alerting Records That Override the Default Scheme 22-14
Configuring Common Response Parameters For All Toning Statuses 22-16
Alerting Example 22-18
Customizing the Alerting Interface 22-20
Configuring the External System Interface 22-21
Configuring System Identification for External Interfaces 22-23
Configuring Local Agency Settings 22-24
Using the External System Interface as a Call for Service Interface 22-27
Call for Service Features 22-27
Call for Service Definitions 22-27
Provisioning the Call for Service Interface 22-28
Overview of Provisioning the Local Agency 22-28
Overview of Provisioning the Foreign Agency 22-29
Provisioning Foreign CAD Systems 22-29
Provisioning Local Agencies 22-31
Provisioning Foreign Agencies 22-33
Provisioning the Default Incident Source Code 22-36
Provisioning Default Incident Status 22-37
Configuring Infotrak 22-37

Configuring the QA Interface 22-39
Configuring ProQA 22-39
Configuring ProQA Paramount 22-41
ProQA Paramount Keyboard Shortcuts and Function Keys 22-44
Configuring the Radios Interface 22-45
Configuring System Configuration Settings 22-45
Configuring Radio System Settings 22-47
Configuring General Radio Settings 22-48
Configuring Two-Tone Alerting 22-50
Configuring Talkgroups 22-53
Configuring Channel Groups 22-54
Configuring the Records Interface 22-56
Configuring Names and Descriptions of Reporting Data Warehouses 22-57

Chapter 23: Configuring Jurisdictions

Setting the Default Location for Areas, Beats, and Sectors 23-1
Assigning the Default Locations and Response Classes 23-2
Defining Response Classes for Locations 23-4
Adding and Modifying Response Classes for Locations 23-4
Setting the Information for Stations 23-6
Adding Station General Information 23-6
Adding Station Preferred Recommendation Order 23-8

Chapter 24: Configuring Notifications

Configuring the Emergency Notification Message 24-1
Configuring Manual Notifications 24-3

Chapter 25: Configuring Mapping

Setting the Active GIS Database 25-1
Revalidating Provisioned Addresses 25-2
Exporting the Geodatabase Revalidation Error Report 25-4
Configuring Location Verifications 25-6
Configuring Additional Verification Settings 25-10
Configuring the MUD Setting 25-12
Configuring Route Solving 25-13
Modifying Route Solving By Vehicle Type 25-15
Configuring Incident and Unit Icons 25-16
Adding and Modifying Incident Icons 25-16
Adding and Modifying Call Location Icons 25-19
Adding and Modifying Unit Icons 25-20
Adding and Modifying Camera Icons 25-21
Configuring GPS Cadence 25-22
Configuring Mapping Agency Settings 25-24
Adding and Modifying General Settings – CAD 25-25
Adding and Modifying General Settings – Mobile/Handheld 25-27
Setting CAD Map Zoom Behavior 25-28
Setting the Mouse Hover Display 25-30
Configuring Non-GPS Equipped Units Display 25-32

Configuring Person Location 25-33
Setting When Person Location Icons Display 25-34
Setting the Person Icon Display Information 25-35
Setting the Mouse Hover Display Information 25-37
Setting Person Location Cadence 25-38
Configuring ARL History Playback Defaults 25-40
Configuring Railroad and Bridge Gate Status 25-41

Chapter 26: Configuring Messaging

Configuring Agency Messaging Settings 26-1
Configuring General Agency Messaging Settings 26-2
Configuring Mobile Agency Messaging Settings 26-4
Configuring CAD Agency Messaging Settings 26-5
Configuring Smart Client Agency Messaging Settings 26-6
Configuring Handheld Agency Messaging Settings 26-7
Configuring Message Types 26-8
Configuring General Message Types 26-9
Configuring Mobile Message Types 26-10
Configuring CAD Message Types 26-12
Configuring Smart Client Message Types 26-14
Configuring Handheld Message Types 26-16
Configuring Message Folder Settings 26-17
Configuring Mobile Message Folders 26-17
Configuring CAD Message Folders 26-19
Configuring Smart Client Message Folders 26-21
Configuring Handheld Message Folders 26-22
Configuring Alternative Routing for Messages 26-24

Chapter 27: Configuring Mobile Browsers

Configuring Agency Settings for Mobile Browsers 27-1

Chapter 28: Configuring Peripherals

Viewing Printers 28-1
Configuring GPS Settings 28-2
Configuring Magnetic Stripe Readers 28-5

Chapter 29: Configuring External Adapters

Configuring System Information for External Adapters 29-1
Configuring External Agencies for External Adapters 29-3
Configuring Entity Mapping for External Adapters 29-4

Chapter 30: Configuring Purge Operations

Viewing Scheduled Purges 30-1
Configuring Online Purge Options 30-3
Configuring Reporting Data Warehouse Purge Options 30-5

Chapter 31: Configuring Queries

Queries Overview 31-1
Importing Metadata 31-2
Updating Metadata 31-5
Metadata Import Errors 31-5
Confirming the State Interface Setup 31-6
Configuring PremierOne Records Queries 31-6
Configuring Queries at the Suite Level 31-7
Configuring Interfaces for Queries at the Suite Level 31-8
Configuring Query Response Settings 31-10
Configuring Agency Default Query Settings 31-10
Configuring Mobile Query Response Settings 31-12
Configuring CAD/Smart Client Query Response Settings 31-13
Configuring Query Types 31-15
Adding Query Type Settings 31-16
Adding Interfaces for Query Types 31-18
Adding Interface Fields for Query Types 31-19
Adding Form Fields for Query Types 31-20
Adding Response Fields for Query Types 31-24
Setting Up Duplicate Fields for Query Types 31-27
Adding Hot Hits for Query Types 31-28
Adding Cascading Queries for Query Types 31-30
Adding Drill Down Information for Query Types 31-33
Configuring Query Types Mapping 31-34
Mapping Query Types by Agency 31-35
Mapping Query Types by Query Type 31-36
Configuring Watch Lists 31-37
Adding Watch Lists 31-38
Adding Watch List Settings 31-38
Adding Frequency Settings for Watch Lists 31-40
Adding Watch List Exclude Settings 31-41
Configuring Response Formats 31-43
Configuring a Reply Using the Designer Tool 31-45
Configuring a Reply Using XSLT 31-48
Configuring Response Format Mapping 31-49
Mapping Response Formats by Agency 31-50
Mapping Response Formats by Response Format 31-51
Configuring Response Fields Mapping 31-52
Configuring ALPR Automatic Queries 31-54
Configuring Query Two-Factor Authentication 31-56
Configuring Queries at the Agency Level 31-57
Configuring Interfaces for Queries at the Agency Level 31-57
Configuring Interface Mnemonic Settings at the Agency Level 31-57
Configuring the Interface ORI Settings at the Agency Level 31-59
Configuring Interface Hot Hit Settings at the Agency Level 31-61
Configuring Incident Management Query Settings at the Agency Level 31-64

Chapter 32: Configuring Status Monitors

Fixed and Varying Areas in Status Monitors 32-1

Configuring Agency Defaults for Status Monitors 32-2
Configuring General Status Monitor Settings– Agency Defaults 32-3
Configuring CAD Status Monitor Icons 32-3
Configuring Right-Click Menu Options 32-9
Configuring CAD Status Monitor Settings – Agency Defaults 32-13
Configuring CAD Unit Status Colors 32-13
Configuring CAD Incident Status Colors 32-15
Configuring Call Control Colors 32-17
Configuring Status Monitor Fonts for the Default CAD Display 32-18
Configuring the Monitor Background Color 32-19
Configuring Mobile/Handheld Status Monitor Settings – Agency Defaults 32-20
Configuring Mobile/Handheld Unit Status Colors 32-21
Configuring Mobile/Handheld Incident Status Colors 32-22
Configuring Mobile/Handheld Status Monitor Fonts 32-24
Configuring Closed Incidents for Mobile/Handheld Status Monitors 32-25
Adding Status Monitor Displays 32-26
Adding CAD Status Monitor Displays 32-26
Adding CAD Status Monitor General Information 32-26
Adding CAD Status Monitor Window Information 32-28
Adding Windows General Information 32-28
Adding Windows Fields 32-36
Adding Windows Sorting Information 32-39
Adding Windows Filtering Information 32-40
Adding Windows Grouping Information 32-42
Adding Windows Position Information 32-43
Adding Windows Alerts Information 32-44
Adding Windows Right-Click Menu Options 32-47
Adding Windows Status Color Options 32-49
Configuring Status Monitor Fonts for Display Sets 32-53
Configuring Status Monitor Fonts for Individual CAD Monitors 32-54
Configuring Mobile Status Monitor Displays 32-55
Configuring Incident Type Display Options for Mobile 32-55
Configuring Display Fields for Mobile 32-57

Chapter 33: Configuring Trigger Point Systems

Configuring Triggers 33-1
Configuring Trigger Groups 33-4
Configuring External Systems 33-6
Configuring Batch Transmission Information 33-8

Chapter 34: Internationalization

Configuring Phone Number Format 34-1

Appendix A: Recommendation References

Run Cards A-1
Alerting: Toning, Paging, and Tear and Run A-3
Creating and Sending Alerts A-3
Building the Unit Alerting List A-6

Building the Final Alerting List A-10
Summary A-13
Alerting by Toning A-14
Unit Recommendations A-16
Jurisdictional Recommendation Methods A-16
Recommendations Based on Fixed Unit Responses A-16
Recommendations Based on a Unit’s Jurisdictional Assignments A-17
Recommendations Based on Run Card Assignments A-17
Location (ARL) Based Recommendation Methods A-18
Alternate Recommendation Methods A-18
Advanced Recommendation Methods A-19
Personnel Skill Recommendation Methods A-19
Specific Unit Recommendation Methods A-20
Recommendation Logging A-20
Log Every Time a Recommendation Occurs A-21
Log Only When a Recommendation Occurs Resulting in a Dispatch A-21
Do Not Log A-21

Index

List of Tables

Table 1-1: Keyboard Conventions 1-4
Table 1-2: Typographic Conventions 1-5
Table 2-1: Six Main Areas of the Provisioning Window 2-4
Table 2-2: Common Buttons in the Provisioning Work Area 2-7
Table 3-1: Levels of Provisioning for Provisioning Pages 3-5
Table 3-2: Provisioning Field Interdependencies – Sorted by Field Name 3-11
Table 3-3: Provisioning Field Interdependencies – Sorted by Where Defined 3-18
Table 8-1: Permissions Required For Mobile Users – Incident Initiation and Incident Update 8-12
Table 8-2: Permissions Required For Mobile Users – Incident Dispatch and Unit Status 8-12
Table 10-1: Cross-Staffing and Status 10-19
Table 13-1: VOICE CALL: ANI/ALI & Incident Initiation Form 13-17
Table 14-1: Sample Response Requirement 14-9
Table 22-1: ProQA Paramount Keyboard Shortcuts and Function Keys 22-44
Table 25-1: Gate Status Icons 25-41
Table 32-1: Right-Click Options Voice Call Control 32-12
Table 34-1: Filter Operation Symbols 34-3

CHAPTER 1

Introduction

This guide explains how to configure all of the aspects of PremierOne for CAD and Mobile, including agencies, the command line, mapping, messaging, queries, units, and many others.

This document is intended for use by personnel who are responsible for the configuration of PremierOne. Provisioning requires an understanding of both current operations procedures and how PremierOne functions. For more information, see the *PremierOne CAD User Guide* and the *PremierOne Mobile User Guide*.

What Is In This Book

This Provisioning Guide has the following chapters:

Chapter 1: "Introduction." Describes the contents of the Provisioning Guide and explains the conventions used in the guide, how to determine the version number of the software, and how to report a problem with the software.

Chapter 2: "Getting Started With Provisioning." Describes how to log in and log out of Provisioning and gives an overview of the Provisioning window and the Provisioning work area.

Chapter 3: "Provisioning CAD and Mobile." Provides an overview of how to provision the CAD and Mobile applications.

Chapter 4: "Configuring Agencies." Describes how to configure new agencies and agency types and how to reconfigure existing agencies and agency types.

Chapter 5: "Configuring Trusted Agencies." Describes how to configure security for trusted agencies.

Chapter 6: "Configuring Lists and Codes." Describes how to configure code tables.

Chapter 7: "Configuring Plans." Describes how to configure plan assignments and how to set the active plan.

Chapter 8: "Configuring Role Permissions." Describes how to configure roles and set permissions.

Chapter 9: "Configuring Authentication." Describes how to configure general agency settings, configure passwords for your agency, enable the emergency mode, configure system notifications, and how to force password changes.

Chapter 10: "Configuring Unit Management." Describes how to configure unit IDs, general unit preassignments, unit status code properties, unit status code timeouts, cross staffing groups, unit settings for the command line, unit settings for shift ID codes, unit settings for transactions, capabilities, capability groups, activity codes, and duty types.

Chapter 11: "Configuring Resources." Describes how to configure personnel, vehicles, general device types, devices, E911 systems, and TDD systems.

Chapter 12: "Call Control." Describe how to configure PremierOne to integrate with Intrado's NG911 customer premise equipment.

Chapter 13: "Configuring Incident Management." Describes how to configure coverage groups, incident types, modifying circumstances, service settings, mobile settings, incident response factors, dispositions, response messages, incident source codes, and premise and hazard information.

Chapter 14: "Configuring Unit Recommendations." Describes how to configure response modes, response classes, response IDs, and run cards.

Chapter 15: "Configuring Contractor Rotation." Describes how to configure contractor types, capabilities, and rotations for assigning contractors to incidents.

Chapter 16: "Customizing the User Interface." Describes how to configure the CAD and Mobile interfaces for primary and secondary services, the Actions bar, command lines, options, and other user interface items.

Chapter 17: "Configuring CAD Display Settings."Describes how to configure the manner in which comments and response messages are displayed on the Comments tab, and dispatch information, comments, and response messages are displayed on the Dispatch tab of the Incident Management screen.

Chapter 18: "Configuring Address Books and Groups." Describes how to configure general address book information, how to add address book entries, and how to configure groups for address books.

Chapter 19: "Configuring Alarms." Describes how to configure alarm companies, alarm records, chronic alarm settings, and false alarms.

Chapter 20: "Configuring Chat Rooms." Describes how to configure chat status settings, general settings, and chat rooms; how to create new chat rooms; how to reconfigure existing chat rooms; how to work with existing chat room members; and how to add new chat room members.

Chapter 21: "Configuring the Command Line." Describes how to configure commands, separators, and behaviors for the command line. It also describes how to view identifiers and where identifiers are used.

Chapter 22: "Configuring Interfaces." Describes how to configure incident data for Infotrak.

Chapter 23: "Configuring Jurisdictions." Describes how to assign a default geoverified location to areas, beats, locations, and sectors.

Chapter 24: "Configuring Notifications." Describes how to configure manual notifications.

Chapter 25: "Configuring Mapping." Describes how to set the active geodatabase, and how to configure location information, multi-unit settings, route solving settings, incident icons, call location icons, unit icons, and cadence.

Chapter 26: "Configuring Messaging." Describes how to configure your agency settings, general message types, MDT message types, CAD message types, message folders for MDT, message folders for CAD, and alternative routing for messages.

Chapter 27: "Configuring Mobile Browsers." Describes how to configure agency settings for mobile browsers.

Chapter 28: "Configuring Peripherals." Describes how to view your peripherals, including your printers and GPS devices.

Chapter 30: "Configuring Purge Operations." Describes how to configure purge operations for online databases and data warehouse operations.

Chapter 31: "Configuring Queries." Describes how to configure state interface queries, query types, watch lists, and incident management query settings.

Chapter 32: "Configuring Status Monitors." Describes how to set agency defaults for unit status colors, incident status colors, icons, and for right-click menu options. Also describes how to configure status monitor displays.

Chapter 33: "Configuring Trigger Point Systems." Describes how to configure triggers, trigger groups, external systems, and batch transmissions.

Appendix A: "Recommendation References." contains detailed explanations of run cards, unit recommendations, and alerting (toning, paging, and tear and run).

Related Documents

PremierOne CAD User Guide

PremierOne CAD Quick Reference Guide

PremierOne Mobile User Guide

PremierOne Mobile Quick Reference Guide

PremierOne Provisioning Guide

PremierOne System Administrator Guide

About the Conventions Used in This Guide

There are several conventions used in this guide:

- "Keyboard Conventions" on page 1-4
- "Typographic Conventions" on page 1-5
- "Notes and Cautions" on page 1-5

Keyboard Conventions

Using the keyboard to carry out commands often involves pressing keys at the same time or in sequence.

Table 1-1 Keyboard Conventions

Convention	Description
Shift+F1	(Or any two keys joined by a plus sign) Press the **Shift** key while pressing the **F1** key. **Example**: Press `Shift+F1` to open online help.

Typographic Conventions

These typographic conventions are used throughout this guide.

Table 1-2 Typographic Conventions

Convention	Description
Courier New Font	Information that the user needs to enter is in Courier New font. **Example:** Enter `BO90001` in the text box. Information that the system displays is in Courier New font. **Example:** The `Undefined Field` error message appears.
Bold	Labeled buttons, menu commands, and menu options are in bold. **Example:** Click **OK** to close the dialog box.
<variable>	Information the user must substitute appears in italics surrounded by angled brackets. Example: <agency ID> means the user must supply the appropriate agency identification. **Example:** *<agency ID>* means the user must supply the appropriate agency identification.

Notes and Cautions

Throughout this guide, notes and cautions are used to highlight text. Notes indicate information that is of high importance. Cautions contain information that must be observed or damage to the system could result.

NOTE
Information listed in notes is of high importance.

CAUTION
Cautions contain information that must be observed or loss of data could result.

Contacting Technical Support

You can obtain support by phone from Technical Support at **1-800-323-9949**. International customers, call **1-847-576-7300**. After you are connected, use the following information to obtain product-specific support:

- For PremierOne CAD, press `2-6-1`
- For PremierOne Mobile, press `2-6-3`

- For NetRMS, NetCAD, and Evalis, press `2-6-2`
- For Offendertrak, press `2-6-4`
- For Infotrak, press `2-6-5`
- For CSR 311, press `2-6-6`
- For all other products, press `2-6-0`

During regular business hours, your call is routed directly to available technical support personnel. After regular business hours, a 24/7 support engineer is contacted and will immediately return your call. Have the following information ready:

- Product name and version number
- Description of the problem
- What you were doing when the problem occurred
- Steps you took to try to solve the problem
- Hardware description
- Exact wording of any messages appearing on your screen

Using Motorola Online

The Motorola Online Web site, http://BusinessOnline.MotorolaSolutions.com, contains the documentation for Public Safety products, including user guides, system configuration guides, System Administrator guides, and training course details. You can download any of these documents.

You can also open new service cases, and view and update existing cases. Case history reports are available to view and download.

You need a user ID and password to enter the site, both of which you can request from the initial page.

CHAPTER 2

Getting Started With Provisioning

Provisioning is the tool where you, the administrator, set up and maintain the data, resources, and the business rules for your agencies. This includes details such as agency types, chronic alarm settings, message folders, and query types. This chapter describes how to log into and log out of Provisioning, and what you need to know to get started using Provisioning to configure settings for your agency.

Logging in to Provisioning

The Provisioning tool is one of several tools in the System Management Portal, a Web browser-based tool.

To log in to Provisioning:

1. From your Web browser, access the address of your PremierOne server. If you have multiple servers, access your data server.

   The Console Login dialog box appears.

Figure 2-1 PremierOne Console Login Dialog Box

2. In the User ID field, type your Provisioning user ID.
3. In the Password field, type your Provisioning password.
4. From the Agency list, select the agency that maintains your user ID.

5. From the Role list, select your role.

   Your role determines the areas in Provisioning to which you have permission to make changes.

6. Click **Login**.

   If you have access to multiple areas of system management, the System Management Tool Portal appears.

   If you only have access to Provisioning, or if you used the Provisioning-only URL, the Provisioning window appears.

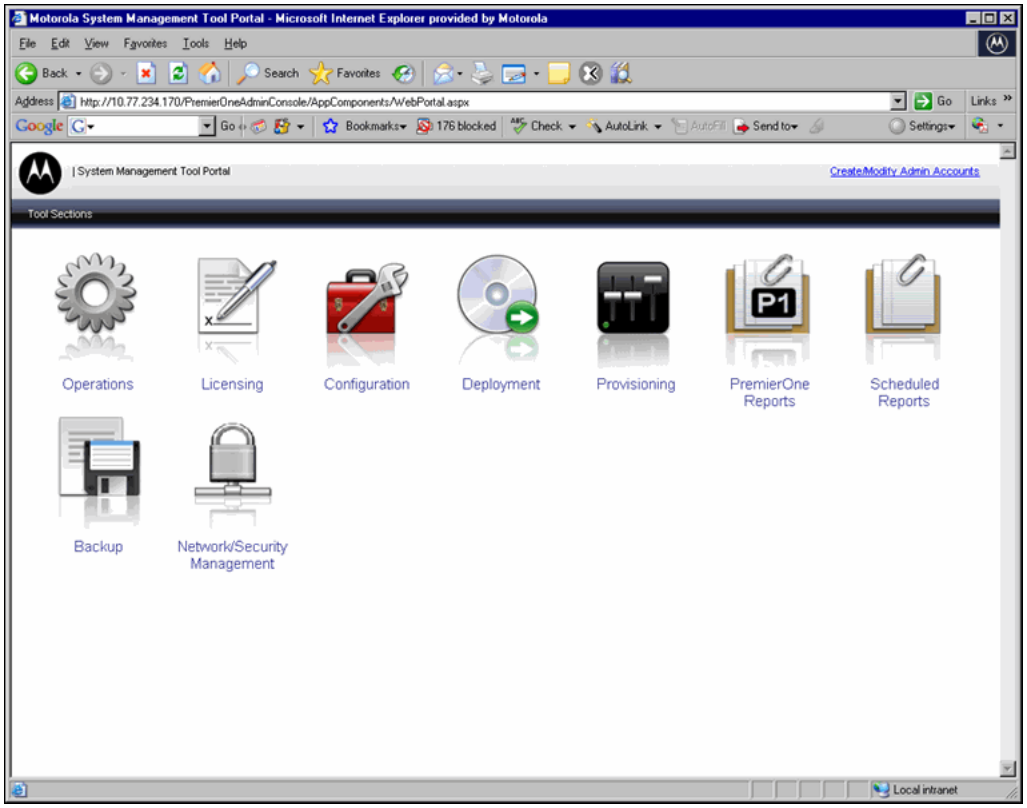


Figure 2-2 System Management Tool Portal

7. Click **Provisioning**.

The Provisioning window opens showing the Provisioning dashboard. The dashboard contains links to the various configuration items in PremierOne Provisioning.

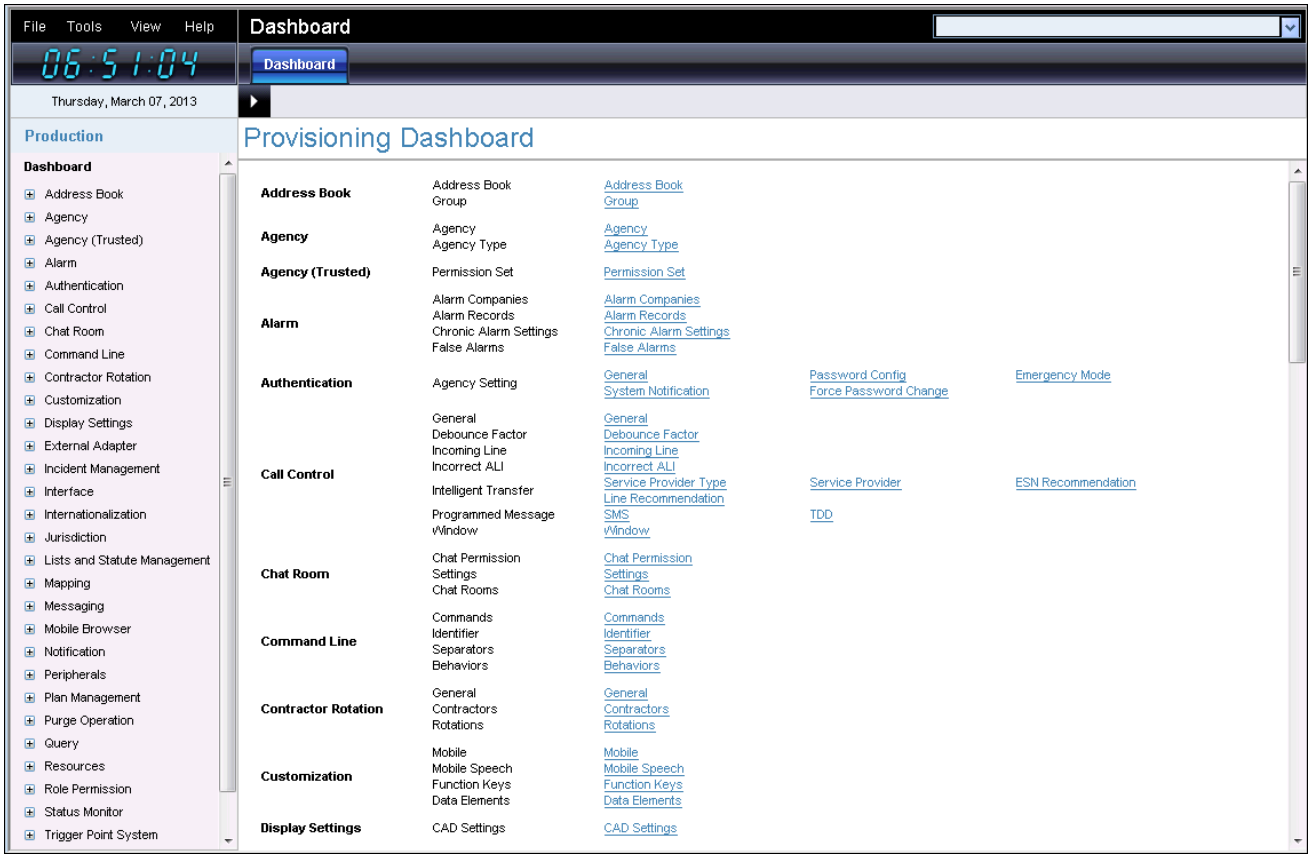


Figure 2-3 Provisioning Window Showing Dashboard

Overview of the Provisioning Window

The Provisioning window has six main areas. These are described in the following table.

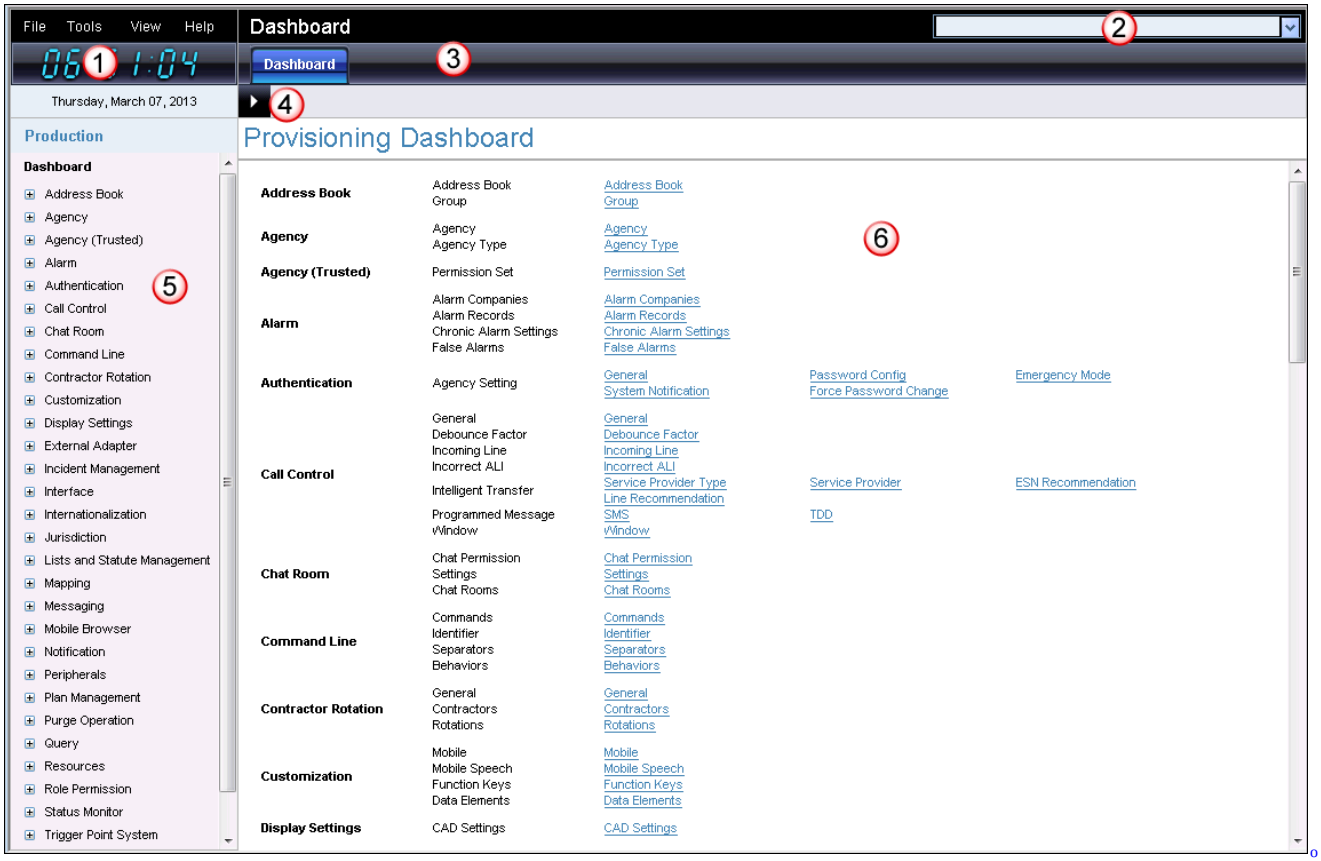
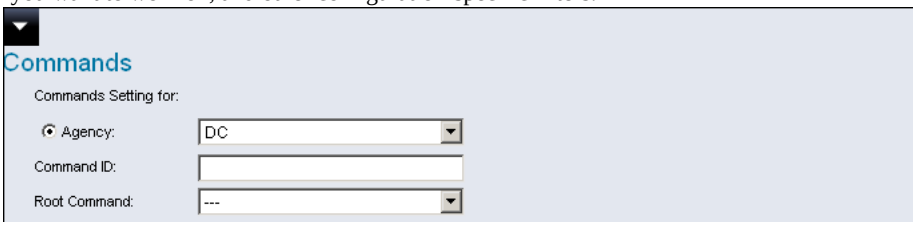


Figure 2-4 Main Areas Of Provisioning Window

Table 2-1 Six Main Areas of the Provisioning Window

1	Menu Bar – Displays the four menus available in Provisioning: File, Tools, View, and Help. File – Contains commands to logout of Provisioning but stay in the System Management Tools Portal and to logout of Provisioning and exit the Portal. Tools – Export PR Data – Exports the provisioning data as a `.dat` (data) file. You use the `.dat` file when configuring the CAD or Mobile client. View – Closes Provisioning and returns you to the System Management Tools Portal. Help – Opens the online help for Provisioning.
2	Message Area – Displays success and error messages related to your actions.

Table 2-1 Six Main Areas of the Provisioning Window

3	Tabs – Provides access to different information specific to the type of configuration you are working on.
4	Filter Button – Opens the filter area. The filter area is where you select whether you are adding a new configuration, working on an existing configuration, the agency or agency type you want to work on, and other configuration-specific filters. 
5	Navigation Pane – Displays all the configuration items. Click the Expand button to show additional configuration items. To show only the main item headings, click the Collapse button.
6	Work Area – Displays the configuration forms, except when you are in the Dashboard.

Overview of the Work Area

The work area is where the configuration forms appear after you select the configuration item you want from the navigation pane. For details, see “Overview of the Provisioning Window” on page 2-4.

When you first open Provisioning, the Dashboard appears in the work area. The Dashboard is an expanded version of the navigation pane. It shows and provides links to all of the Provisioning configuration items. You can display the Dashboard at any time by clicking Dashboard, the first item, from the navigation pane. You need to scroll up and down to see all of the items in the Dashboard.

After you select a configuration item, such as Agency or Messaging, the work area nearly always displays several common buttons at the bottom of the window and often displays a list of configurable items next to the navigation pane at the left of the work area.

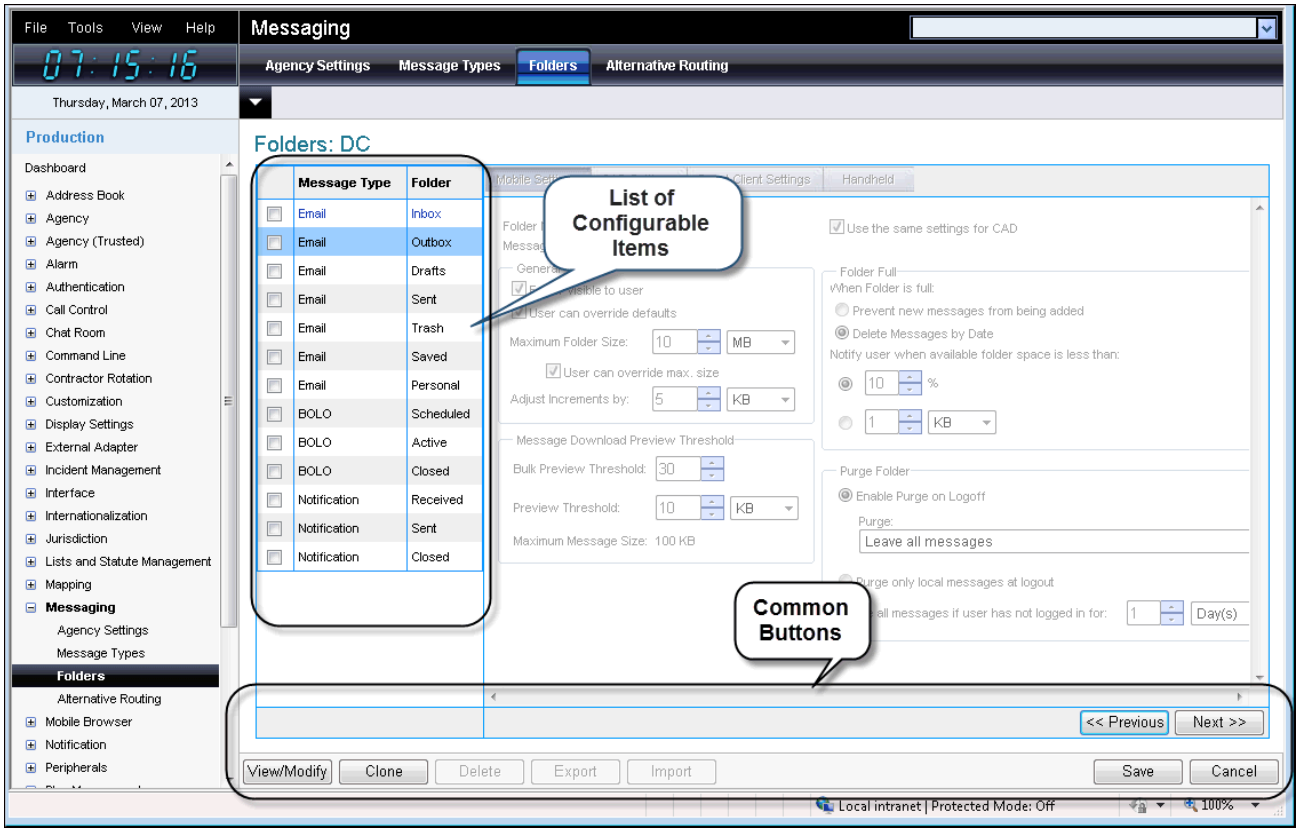


Figure 2-5 Common Features in Work Area

Table 2-2 Common Buttons in the Provisioning Work Area

Button	Description
Previous	Display the previous item from the list of configurable items.
Next	Display the next item from the list of configurable items.
View/Modify	View or modify the information shown in the form in the work area.
Clone	Clone (copy) the information shown in the form in the work area to quickly create another folder, vehicle, person, or whatever item you are copying.
Delete	Delete the item selected in the list of configurable items. When you click Delete, PremierOne draws a red line through the information in the list. Click **Save**.
Export	Export information to an Excel 97 (2003) spreadsheet.
Import	Import information from an Excel spreadsheet.
Save	Save the item you are configuring or confirm your deletion.
Cancel	Cancel any changes you made to the form in the work area.
New (Only on some forms)	Create a new item of the type shown in the list of configurable items.

NOTE
Depending on what activity you are performing, some buttons are inactive.

Using Filters

The first time you access a configuration item after logging on, a filter for the configuration item displays at the top of the work area. Use the filter to do the following:

- For new records, select the agency type or agency for the record.

- For existing records, use the search fields to limit the records that are retrieved.

NOTE
You can re-display the filter area by clicking the Filter button (down arrow).

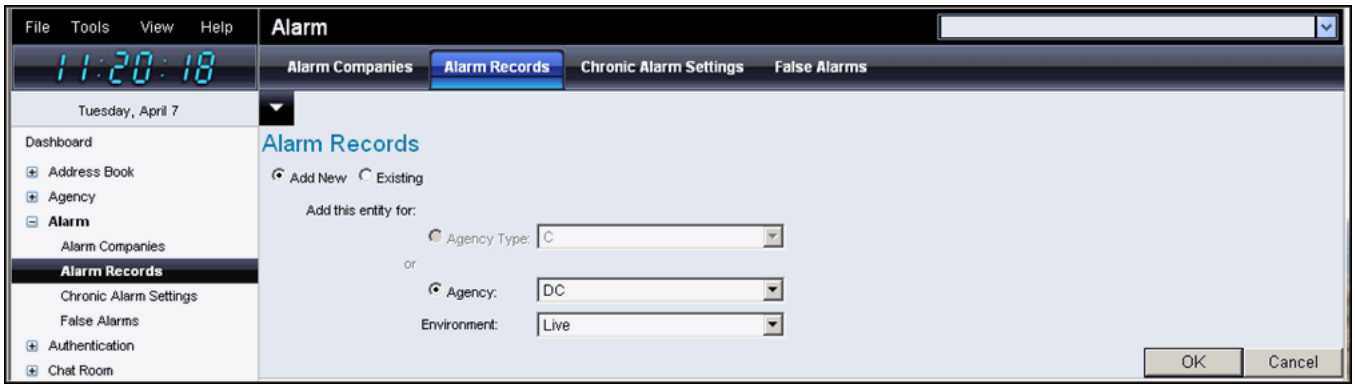


Figure 2-6 Alarm Records Filter – New

To create a new record:

1. Display the filter area for the configuration item.
2. Select **Add New**.
3. Select the agency type or agency.
4. Click **OK**.

   The form displays for the configuration item. A list of all existing records displays on the left side of the form.

To modify an existing record:

1. Display the filter area for the configuration item.
2. Select **Existing**.
3. Select the agency type or agency.
4. To narrow your search, enter more search criteria in the fields that are available.

   Criteria include fields such as Address Book name, Device Type, Plan ID, Role, Unit ID, Unit Status code, and so on.

5. Click **OK**.

   The form displays for the configuration item with a list of all matching records.

Searching for Records

You can search for individual records in many of the configuration items using the configuration item filter. Fields may be present to the right of the Agency fields where you can enter the record you want to retrieve.

For example, if you want to search for a response mode, select the agency and then type the response mode in the Response Mode field. Then click **OK**. When the form appears, the response mode you specified is the only one that appears on the form.

The percent sign (%) can be used as a wildcard in any of the search fields in the Filter area and represents match zero-or-more characters. For example T% would retrieve THEFT and TRSTO.

Partial entries are also assumed to have a % at the end of them. For example, AREA is the same as AREA%. An entry of AREA would return AREA1, AREA2, and so on.

NOTE
Values are not case-sensitive; for example, unit is the same as Unit.

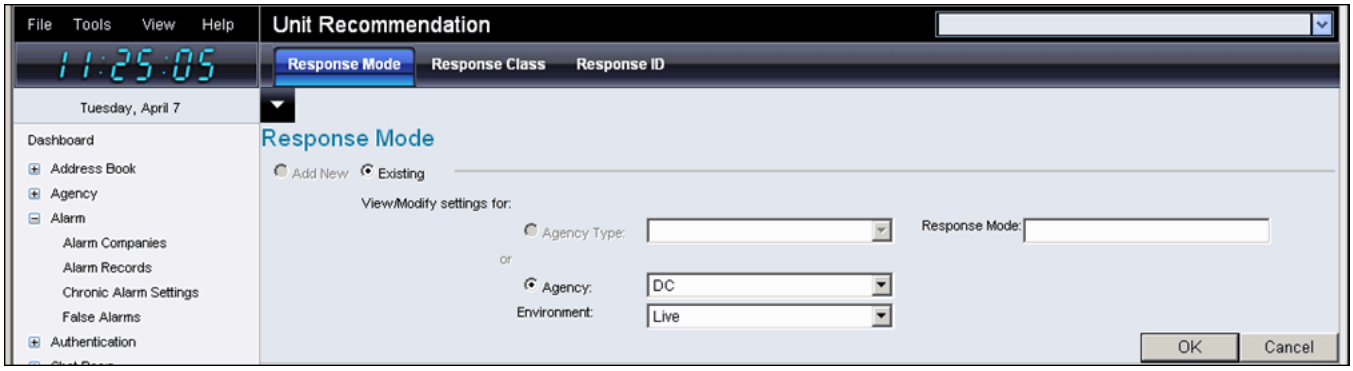


Figure 2-7 Response Mode Filter

Working With Configuration Items

In Provisioning, configuration items are the agency data that are made available in other Provisioning, CAD, and mobile windows, such as incident types, dispositions, modifying circumstances, plans, and unit statuses. For many of the items, you can clone, delete, import, and export. Because these procedures are generally the same for each configuration item, they are described once in this section. When the procedure differs significantly from the general one, the details are provided in the section for the configuration item.

Adding Configuration Items by Cloning

In many of the configurations, you can add configuration items by cloning an existing configuration item. Cloning is useful when you have an existing configuration item that closely matches the new item you need to add.

To add a configuration item by cloning:

1. Display the form for the configuration item.
2. From the item list on the left side of the form, select the check box for the item that most closely matches the new configuration item you need to create.
3. Click **Clone**.

   The Clone dialog box appears.

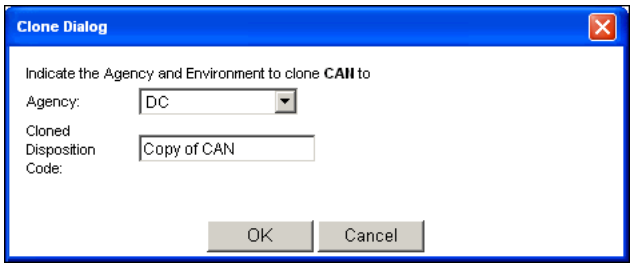


Figure 2-8 Clone Disposition Item Dialog Box

4. From the Agency list, select the agency.
5. In the new name field, type the name of the new configuration.
6. Enter any other information.

   Depending on the configuration item, different fields may display.

7. Click **OK**.

The configuration item is added to the list on the left side of the window.

8. Click **Save**.
9. To modify the cloned record, click **View/Modify**.

Modifying Configuration Items

You can modify configuration items to change the properties. In most cases you cannot change the name of the item, such as agency type or name. If you want to change the name of the item, you must delete and re-add the record.

To modify a configuration item:

1. Access the form for the configuration item.

   The appears in the work area. A list of existing items usually displays on the left side of the form.

2. From the list of items on the left side of the work area, select the item that you want to modify. Selecting the check box does not select the item.
3. Click **View/Modify**.

   You can now modify the properties.

4. Click **Save**.

Deleting Configuration Items

You can delete configuration items when they are no longer used.

To delete a configuration item:

1. Display the form for the configuration item.
2. From the list of items on the left side of the form, select the item you want to delete by selecting the check box to the left of the item.

   You can select more than one item. Select all items by selecting the check box at the top of the column.

   NOTE
   You must select the check box. Highlighting the row does not select the item for deletion.

3. Click **Delete**.

A confirmation message appears.

4. Click **Yes**.

   In the list, a red line appears through the items you deleted.

5. Click **Save**.

   The configuration item you deleted no longer appears in the list.

Exporting Configuration Items

You can export many configuration items to a folder on your computer or network. This feature allows you to export your configuration items, work on them in Excel, and the import them back into Provisioning. If you have a lot of codes or configuration items, this feature can save you significant time.

NOTE
You must save as `.xls`, not `.xlsx`; as an Excel 97 (2003) spreadsheet.

To export a configuration item:

1. Display the Provisioning form for the configuration item.
2. Select the check box adjacent to the configuration item you want to export.
3. Click **Export**.

   A dialog box may appear asking if you want to export only the selected item(s), or if you want to export all items.

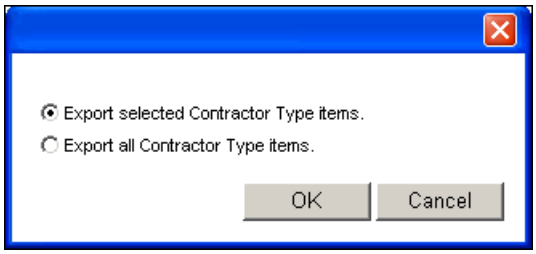


Figure 2-9 Export Dialog Box

4. Make your selection and then click **OK**.

   A File Download dialog box appears, asking if you want to open or save the file.

5. Click **Save**.

   A Save As dialog box appears, with a default name for the file in the File Name field.

6. Rename the file if you would like.

7. Navigate to the folder where you want to save the file and click **Save**.

   The configuration items are saved as a Microsoft Excel Comma Separated Values (CSV) file or Excel (XLS) files.

Importing Configuration Items

You can import configuration items from a file on your computer or network into the PremierOne Provisioning application. This feature allows you to create and work on your configuration items in Excel and the import them into Provisioning. If you have a lot of codes or configuration items, this feature can save you significant time.

To import codes:

1. Display the Provisioning form for the configuration item.

2. Export the file for the Provisioning element.

   The ensures you have an Excel file with all of the appropriate data headings.

3. Add your new information below the existing data on each tab. (Some spreadsheets have only one tab.)

   For help, you can open the comments by clicking the red triangle in the headings of many of the spreadsheets.

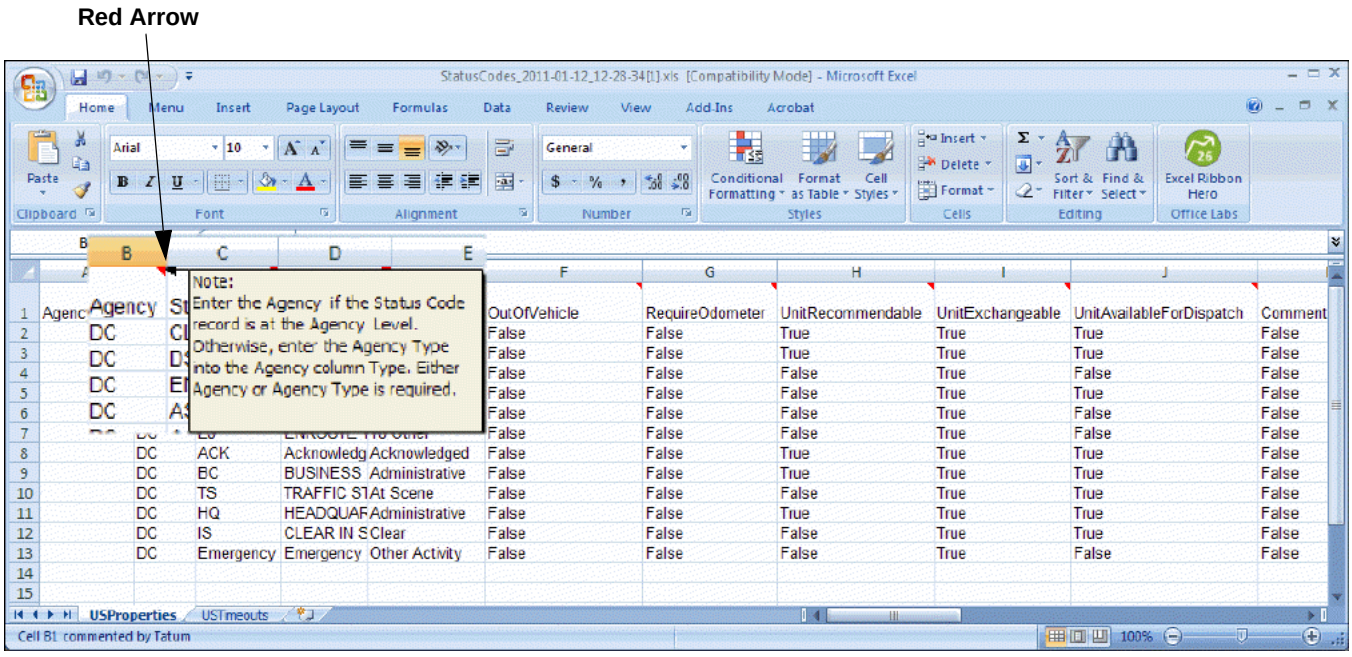


Figure 2-10 Help For Agency Column Showing After User Clicked Red Arrow in Agency Heading

In addition, when you click in some columns, a down arrow appears to the right of the value. When you click the arrow, a list of the acceptable values appears.

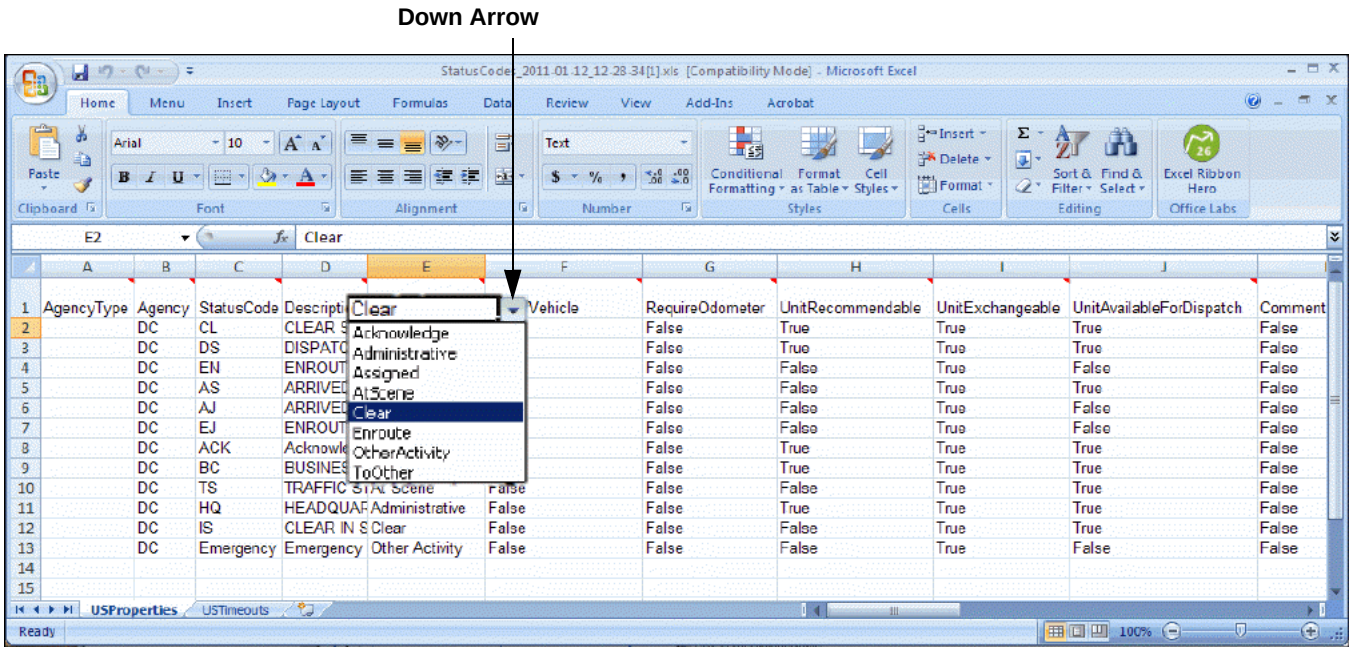


Figure 2-11 List of Acceptable Values Showing After User Clicked Down Arrow Next to Clear Value

> **NOTE**
> Because Unit Status Codes can be imported at the Agency and at the Agency Type level, the spreadsheet contains columns for both Agency and AgencyType. If you are importing at the Agency level, use the Agency column and leave the AgencyType column blank. If you are importing at the Agency Type level, use the AgencyType column and leave the Agency column blank.

For fields that can have multiple entries, such as Role in Personnel, you need to enter the Agency Type, Agency, and any other associated information again for each different role to which a person is assigned.

4. Delete everything except your new information and the column headings.

5. Save the spreadsheet.

   This procedure works with both `.xls` and `.csv` files.

> **NOTE**
> When saving to Excel, you must save as `.xls`, not `.xlsx`; as an Excel 97 (2003) spreadsheet.

6. Display the Provisioning form for the configuration item again.

7. Click **Import**.

   The File Browser window appears.

8. Navigate to the file that you want to import and click **Open**.

   An Import dialog box may appear. Select the appropriate agency and click **OK**.

   The imported configuration items appear in the list on the left side of the window, such as the Contractor Type Code list or the Run Card list, and a success message displays in the Status Message area. If errors occurred, they appear, one at a time, in the Status Message area.

Logging Out of Provisioning

Log out of Provisioning when you finish your configuration tasks and when you leave your workstation for an extended period of time, such as for breaks, meetings, or lunch. Logging out ensures that no one else enters or changes information.

To log out of Provisioning:

Do one of the following from the Provisioning **File** menu:

- To log out and open the PremierOne Console Login dialog box, select **Logout**.
- To log out and close the System Management Portal, select **Exit**.

CHAPTER 3

Provisioning CAD and Mobile

When you provision PremierOne the first time, you need to configure settings in a specific order. Depending on the specific configuration item, provisioning occurs at one of the following different levels: global (all agency types and agencies), by agency type (such as fire, medical, and law), and by agency. Some configuration items such as incident types can also be configured for an agency type, and then for a specific agency.

NOTE

You must load the GIS data before provisioning; without the GIS data the beats do not exist.

Provisioning CAD

To provision CAD:

1. Create lists and list items (codes), such as cities, counties, vehicle types, personnel skills, and so on. These items display in drop-down lists.

   Global entries are available to all agencies. Codes entered at the agency level display in addition to the global values.

   NOTE

   This configuration should be done first globally and then will apply to all agencies. If the configuration is not done before adding individual agencies, then each agency must be also individually configured. Additionally, anything provisioned at the agency level will override the global setting.

   For details, see Chapter 6: “Configuring Lists and Codes.”

2. Create the agencies and agency types.

   For details, see Chapter 4: “Configuring Agencies and Agency Types.”

Make sure the agency is identified in GIS before provisioning an agency.

3. Configure trusted agencies (optional).

   For details, see Chapter 5: “Configuring Trusted Agencies.”

4. Create the plans and set the active plan.

   For details, see Chapter 7: “Configuring Plans.”

5. Create the roles and set the permissions for the roles. Add the roles before you add resources.

   For details, see Chapter 8: “Configuring Role Permissions.”

6. Create the authentication settings, such as password restrictions.

   For details, see Chapter 9: “Configuring Authentication.”

7. Create the resources and capabilities.

   a. Add capabilities (skills for personnel).

   b. Create the personnel records (personnel records require authentication, list items, and skills).

   c. Create the vehicle records.

   d. Create the device types.

   e. Create the devices.

   For details, see Chapter 11: “Configuring Resources.”

8. Create the units, unit status codes, and capabilities.

   a. Create the unit status codes.

   b. Create the capabilities.

   For details, see Chapter 10: “Configuring Unit Management.”

9. Create the incident information.

   a. Create the incident types.

   b. Create the modifying circumstances.

   c. Create the dispositions.

   d. Create the service settings and priorities.

   e. Create the incident response factors (IRF).

f. Create the Mobile settings.

g. Create the response messages.

h. Create the premise/hazard codes and proximity settings.

For details, see Chapter 13: “Configuring Incident Management.”

Configure other areas of PremierOne, such as Status Monitors, Queries, Recommendations, and other items as needed. You do not need to configure the rest of the items in any specific order.

Provisioning Mobile

When you provision Mobile for the first time, you need complete the following configuration settings:

1. Create the roles and set the permissions for the roles.

   When setting up roles, select the MDT check box on the General tab to make a role available for Mobile.

   For details, see “Adding Roles” on page 8-2.

2. Create the address books.

   For details, see “Configuring Address Books” on page 18-1.

3. Configure messaging setting, such as MDT synchronization, size limits, types, and locations.

   For details, see “Configuring Agency Messaging Settings” on page 26-1.

4. Create the Manual Notifications for any mobile group.

   For details, see “Configuring Manual Notifications” on page 24-3.

5. Configure mapping settings, such as icons, cadence, and mouse hover notes, the incident fields that display, the unit fields that display, and the number of digits in the incident number to display on the mobile map.

   For details, see the following:

   - “Adding and Modifying Unit Icons” on page 25-20
   - “Adding and Modifying General Settings – Mobile/Handheld” on page 25-27

- “Setting the Mouse Hover Display” on page 25-30

6. Configure Incident Management settings such as enabling self dispatch, mobile alert settings, and priority updates.

   For details, see “Configuring Mobile/Handheld Priority Alert Settings” on page 13-33.

7. Configure Mobile browser settings, identifying the Web sites that Mobile users can view.

   For details, see “Configuring Agency Settings for Mobile Browsers” on page 27-1.

8. Configure Mobile status monitor settings, such as unit status colors, incident status colors, status monitor fonts, and closed incident display.

   For details, see:

   - “Configuring Mobile/Handheld Status Monitor Settings – Agency Defaults” on page 32-20
   - “Configuring Mobile Status Monitor Displays” on page 32-55

9. Make Mobile interface customizations, setting the primary and secondary services that display, and controlling the mobile options, navigation bar, status bar, login icon, address book log, command line, and function keys.

   For details, see “Configuring the Mobile Interface” on page 16-2

10. Set Text to speech options, such as enabling text-to-speech and selecting fields for speech.

    For details, see “Configuring Mobile Text-to-Speech” on page 16-18

11. Configure magnetic stripe readers, devices that allow the mobile user to swipe a driver’s license and submit the information to the mobile application.

    For details, see “Configuring Magnetic Stripe Readers” on page 28-5.

Levels of Provisioning

Most of the configuration items in Provisioning are defined at the agency level. Some items, however are defined at the Global level (all agencies and agency types), and others can be defined at the agency or agency type level. For those that can be defined at the agency or agency type level, the settings at the agency level override those at the agency type level.

The following table lists the provisioning pages and the level at which the configuration is performed.

Table 3-1 Levels of Provisioning for Provisioning Pages

Provisioning Page	Level
AGENCY	
Agency Type	Global
Agency	Global
AGENCY (TRUSTED)	
Permission Set	Agency
ADDRESS BOOK	
Address Book	Agency
Group	Agency
ALARM	
Alarm Companies	Agency
Alarm Records	Agency
Chronic Alarm Settings	Agency
False Alarms	Agency
AUTHENTICATION	
Agency Setting	
General	Agency
Password Config	Agency
Emergency Mode	Agency
System Notification	Agency
Force Password Change	Agency
CHAT ROOM	
Chat Permission	Agency Type and Agency
Settings	Agency
Chat Rooms	Agency
CALL CONTROL	
General	Agency
Debounce Factor	Agency

Table 3-1 Levels of Provisioning for Provisioning Pages (Cont.)

Provisioning Page	Level
Incoming Line	Agency
Incorrect ALI	Agency
Intelligence Transfer	Agency
Service Provider Type	Agency
Service Provider	Agency
ESN Recommendation	Agency
Line Recommendation	Agency
Programed Message	Agency
SMS	Agency
TDD	Agency
Window	Agency
COMMAND LINE	
Commands	Agency
Identifier	Agency
Separators	Agency
Behaviors	Agency
CONTRACTOR ROTATION	
General	Agency
Contractors	Agency
Rotations	Agency
CUSTOMIZATION	
Mobile	Agency Type and Agency
Mobile Speech	Agency
Function Keys	Agency
Data Elements	Agency
DISPLAY SETTINGS	
CAD Settings	Agency
EXTERNAL ADAPTER	
System Definition	Global
External Agency	Global
Entity Mapping	Agency
INCIDENT MANAGEMENT	
Coverage Groups	Agency
Incident Type	
Incident Type	Agency Type

Table 3-1 Levels of Provisioning for Provisioning Pages (Cont.)

Provisioning Page	Level
Incident Type Alias	Agency Type
Modifying Circumstance	Agency Type
Service Settings	Agency
General Settings	Agency
Priority Settings	Agency
Incident Response Factors	Agency Type and Agency
Dispositions	Agency
Response Message	Agency
Incident Source Code	Agency Type
Premise Hazard	
Premise Hazard	Agency Type and Agency
Premise Hazard Record	Agency
INTERFACE	
Alerting	
Alerting Scheme	Agency
Toning System	Agency
In-Station Record	Agency
Out-of-Station Record	Agency
Override Record	Agency
Response Parameters	Agency
External System	
System Identification	Global
Foreign Agency Settings	Agency
Local Agency Settings	Agency
Infotrak	Agency
Q/A	
ProQA	Agency
Radio	
System Configuration	Global
Radio System Settings	Agency
Talkgroups Configuration	Global
Channel Groups Configuration	Global
Records	
Records	Agency
Reporting	

Table 3-1 Levels of Provisioning for Provisioning Pages (Cont.)

Provisioning Page	Level
Reporting	Global
JURISDICTION	
Area	Agency
Beat	Agency
Location	Agency
Sector	Agency
Station	Agency
LISTS AND STATUTE MANAGEMENT	
LSM	Global and Agency
MANUAL NOTIFICATION	
Emergency Notification	Agency
Manual Notification	Agency
MAPPING	
GIS Data	Agency
Location Verification	Agency
MUD Setting	Agency
Route Solving	Agency Type
Icons	Agency
Cadence	Agency
Agency Setting	
General Settings	Agency
CAD Map Zoom Behavior	Agency
Mouse Hover Display	Agency
MESSAGING	
Agency Settings	Agency
Message Types	Agency
Folders	Agency
Alternative Routing	Agency
MOBILE BROWSER	
Agency Settings	Agency
PERIPHERALS	
Printer	Agency
GPS	Agency
PURGE OPERATION	
Scheduled Purges	Global

Table 3-1 Levels of Provisioning for Provisioning Pages (Cont.)

Provisioning Page	Level
Online Scheduling	Global
RDW Scheduling	Global
QUERY	
Suite Level Setting	Global
Interfaces	Global
Query Settings	Global
Query Types Mapping	Global
Watch Lists	Global
Response Format Designer	Global
Response Format Mapping	Global
Response Fields Mapping	Global
ALPR	Global
Query 2-Factor Authentication	Global
Agency Level Setting	
Agency Interfaces	Agency
Im Query Settings	Agency
State Interfaces	Agency
Query Types	Agency
Watch Lists	Agency
IM Query Settings	Agency
RESOURCES	
Capability Group	Agency
Capability/Skill	Agency
Personnel	Agency
Vehicle	Agency
Device Profile	Agency
General	Agency
BOLO Content	Agency
Emergency Content	Agency
Incident Content	Agency
Message Content	Agency
Notification Content	Agency
Query Content	Agency
Device Types	Agency

Table 3-1 Levels of Provisioning for Provisioning Pages (Cont.)

Provisioning Page	Level
Devices	
Workstation/MDT	Agency
Radio	Agency
Pager	Agency
Pager Groups	Agency
Printer	Agency
GPS	Agency
Systems	Agency
ROLE PERMISSION	
Roles	Agency
PLAN MANAGEMENT	
Plans	Agency
Active Plan	Agency
STATUS MONITOR	
Agency Defaults	
General Settings	Agency
CAD	Agency
MDT	Agency
Displays	
CAD	Agency
MDT	Agency
TRIGGER POINT SYSTEM	
Triggers	Global
Trigger Groups	Global
External Systems	Global
Batch Transmission	Global
UNIT MANAGEMENT	
Unit	
Unit ID	Agency
Unit Preassignments	Agency
Unit Status Codes	
Unit Status Codes	Agency Type and Agency
MDT Setting	Agency
Cross Staffing Group	Agency
Settings	

Table 3-1 Levels of Provisioning for Provisioning Pages (Cont.)

Provisioning Page	Level
Command Line	Agency Type and Agency
Shift ID Codes	Agency Type and Agency
Transactions	Agency Type and Agency
Activity Code	Agency
Duty Type	Agency
UNIT RECOMMENDATION	
Response Card	
Incident Response Factor	Agency
Response ID	Agency
Response Mode	Agency
Response Class	Agency
Response IDs	Agency Type
Response Descriptor	Agency
Run Card	Agency
Settings	Agency
Response Category	Agency

Tables of Field Interdependencies

The following table shows the field interdependencies in Provisioning sorted by Field name.

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name

Field Name	Configuration Item Where Used	Tab	Where Defined
Active Plan ID	Plans	Active Plan ID	Plan Management - Plans
Agency Type	Agency	Agency	Agency - Agency Type
Alarm	Alarm	Alarm Records - Alarm Company	Alarms - Alarm Companies
Area	Incident Management	Coverage Groups	Plan Management - Plans
Area	Mapping	MUD Setting	Plan Management - Plans
Area	Resources	Personnel - Preassignments	Plan Management - Plans
Area	Unit Management	Unit Preassignments - General	Plan Management - Plans

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name (Cont.)

Field Name	Configuration Item Where Used	Tab	Where Defined
Areas	Incident Management	Response Messages - Areas/Sect/ Beat	Plan Management - Plans
Auto club	Contractor Rotation	Contractors - General	Lists and Statute Management - LSM - Auto Club
Beat	Interface	Infotrak	Plan Management - Plans
Beat	Mapping	MUD Setting	Plan Management - Plans
Beat	Resources	Personnel - Preassignments	Plan Management - Plans
Beat	Interface	Records	Plan Management - Plans
Beat	Unit Management	Unit Preassignments - General	Plan Management - Plans
Beats	Incident Management	Response Messages - Areas/Sect/ Beat	Plan Management - Plans
Book	Chat Room	Chat Rooms - Add Member	Address Book - Address Book
Book	Address Book	Group - Entries	Address Book - Address Book
Capabilities	Unit Management	Unit Preassignments - Unit Capabilities	Resources - Capability/Skill
Capability	Contractor Rotation	Contractors - General	Resources - Capability/Skill
Capability	Unit Recommendation	Run Card - Resp ID	Resources - Capability/Skill
Capability	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Capability/Skill
Capability	Resources	Vehicle	Resources - Capability/Skill
Capability	Resources	Capability Group	Resources - Capability/Skill
Capability Group Code	Unit Management	Unit Preassignments - Unit Capabilities	Resources - Capability Groups
Capability Settings	Unit Management	Unit Preassignments - Capability Settings	display only
Channels	Interface	Radio - Channel Groups Configuration	Interface - Radio - Talkgroups
Contacts	Notification	Manual Notification	Resources - Personnel - Details
Contractor type	Contractor Rotation	Contractors - Contractor Types	Coded in GIS database
Contractors	Contractor Rotation	Rotations	Contractor Rotation - Contractors
Coverage Group	Resources	Devices - Workstation MDT - Login Settings subtab - General subtab	Incident Management - Coverage Groups
Default Unit Status	Unit Management	Settings - Transactions	Unit Management - Unit Status Codes - Unit Status Codes - Properties subtab
Device (this is Device ID)	Resources	Personnel - Authorization	Resources - Devices - Workstation/MDT

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name (Cont.)

Field Name	Configuration Item Where Used	Tab	Where Defined
Device Profile	Devices	Radio	Resources - Device Profile - General
Device Type	Resources	Devices - Workstation MDT - General subtab	Resources - Device Types; Workstation and MDT hardcoded
Device Type category	Resources	Device Types - General	Read only; workstation and MDT
Disposition	Incident Management	Incident Response Factors - General	Incident Management - Disposition
Disposition	Interface	Infotrak	Incident Management - Disposition
Disposition	Interface	Records	Incident Management - Disposition
Disposition	Incident Management	Service Settings - Initiation Defaults - Create an incident when moving up a unit section	Incident Management - Disposition
Disposition	Incident Management	Service Settings - Initiation Defaults - Move Up incident section	Incident Management - Disposition
Disposition for closed status	Alarm	Chronic Alarm Settings	Incident Management - Disposition
Duty Type	Interface	Alerting - In Station Record	Unit Management - Duty Type
Duty Type	Interface	Alerting - Out of station Record	Unit Management - Duty Type
Duty Type	Unit Management	Unit Preassignments - General	Unit Management - Duty Type
Equip ID	Resources	Personnel - Resource Assignments	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment ID	Unit Management	Unit Preassignments - Personnel & Vehicles	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Resources	Personnel - Resource Assignments	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Unit Management	Unit Preassignments - Personnel & Vehicles	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Unit Management	Unit Preassignments - Unit Equipment	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Resources	Vehicle	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Group	Chat Room	Chat Rooms - Add Member	Address Book - Group
Incident Type	Alarm	Alarm Records - Incident - Time/ Day Specific Setting & Chronic alarm sections	Incident Management - Incident Type
Incident Type	Interface	Alerting - In Station Record	Incident Management - Incident Type
Incident Type	Interface	Alerting - Out of station Record	Incident Management - Incident Type

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name (Cont.)

Field Name	Configuration Item Where Used	Tab	Where Defined
Incident Type	Mapping	Icons	Incident Management - Incident Type
Incident Type	Incident Management	Incident Response Factors - General	Incident Management - Incident Type
Incident Type	Incident Management	Incident Response Factors - IRF Attributes	Incident Management - Incident Type
Incident Type	Interface	Infotrak	Incident Management - Incident Type
Incident Type	Interface	Records	Incident Management - Incident Type
Incident Type	Unit Recommendation	Response Card - Incident Response Factor - General	Incident Management - Incident Type
Incident Type	Incident Management	Response Messages - Incident Types	Incident Management - Incident Type
Incident Type	Unit Recommendation	Run Card - IRF	Incident Management - Incident Type
Incident Type	Incident Management	Service Settings - Initiation Defaults - Move up incidents section	Incident Management - Incident Type
Incident Type	Incident Management	Service Settings - Initiation Defaults - Traffic Stops section	Incident Management - Incident Type
Incident type for New or Pending Status	Alarm	Chronic Alarm Settings	Incident Management - Incident Type
Jurisdictional units	Contractor Rotation	Rotations	Plan Management - Plans
Manual Notification	Incident Management	Incident Response Factors - IRF Attributes	Notification - Manual Notification
Member of Groups	Address Book	Address Book - New Entries - Groups subtab	Address Book - Group
Message to be Sent	Alarm	Alarm Records - Incident	Incident Management - Response Messages
Modifying Circumstance	Alarm	Alarm Records - Incident - Time/ Day Specific Setting & Chronic alarm sections	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Incident Response Factors - General	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Incident Response Factors - IRF Attributes	Incident Management - Modifying Circumstance
Modifying Circumstance	Unit Recommendation	Response Card - Incident Response Factor - General	Incident Management - Modifying Circumstance
Modifying Circumstance	Unit Recommendation	Run Card - IRF	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Service Settings - Initiation Defaults - Create an incident when moving up a unit section	Incident Management - Modifying Circumstance

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name (Cont.)

Field Name	Configuration Item Where Used	Tab	Where Defined
Modifying Circumstance	Incident Management	Service Settings - Initiation Defaults - Traffic Stops section	Incident Management - Modifying Circumstance
Disposition	Incident Management	Service Settings - Initiation Defaults - Move Up incidents section	Incident Management - Modifying Circumstance
Modifying Circumstance (M.C.)	Alarm	Chronic Alarm Settings	Incident Management - Modifying Circumstance
Owned by	Chat Room	Chat Rooms - General	Resources - Personnel - Details
Payment Method	Contractor Rotation	Contractors - General	Lists and Statute Management - LSM - Payment Method
Plan ID	Plans	Active Plan	Plan Management - Plans
Priority	Incident Management	Incident Response Factors - IRF Attributes	Incident Management - Service Settings - Priorities
Radio System	Interface	Radio - Radio System Settings	Interface Radio - System Configuration
Radio System	Interface	Radio - Talkgroups	Interface Radio - System Configuration
Recipients	Authentication	Agency Setting - System Notification	Resources - Personnel - Details
Recipients	Resources	Device Types - Login	Resources - Personnel - Details
Recipients	Notification	Emergency Notification	Resources - Personnel - Details
Recipients	Notification	Manual Notification	Resources - Personnel - Details
Response Category Code	Resources	Capability/Skill	Unit Recommendation - Response Category
Response Class	Jurisdiction	Area	Unit Recommendation - Response Class
Response Class	Jurisdiction	Beat	Unit Recommendation - Response Class
Response Class	Jurisdiction	Location	Unit Recommendation - Response Class
Response Class	Unit Recommendation	Run Card - Resp ID	Unit Recommendation - Response Class
Response Class	Jurisdiction	Sector	Unit Recommendation - Response Class
Response ID	Incident Management	Incident Response Factors - IRF Attributes	Unit Recommendation - Response IDs
Response ID	Unit Recommendation	Run Card - Resp ID	Unit Recommendation - Response IDs
Response message sent for No incident status	Alarm	Chronic Alarm Settings	Incident Management - Response Messages
Response Message to be sent	Alarm	Alarm Records - Incident	Incident Management - Response Messages
Response Mode	Unit Recommendation	Run Card - Resp ID	Unit Recommendation - Response Mode

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name (Cont.)

Field Name	Configuration Item Where Used	Tab	Where Defined
Role	Address Book	Address Book - Add Existing Entries	Role Permission - Roles
Role	Address Book	Address Book - New Entries - General subtab	Role Permission - Roles
Role	Chat Room	Chat Rooms - Add Member	Role Permission - Roles
Role	Resources	Devices - Workstation MDT - Login Settings - General	Role Permission - Roles
Role	Address Book	Group - Entries	Role Permission - Roles
Role	Resources	Personnel - Roles	Role Permission - Roles
Sectors	Mapping	MUD Setting	Plan Management - Plans
Sectors	Resources	Personnel - Preassignments	Plan Management - Plans
Sectors	Incident Management	Response Messages - Areas/Sect/Beat	Plan Management - Plans
Sectors	Unit Management	Unit Preassignments - General	Plan Management - Plans
Skill	Resources	Personnel - Details	Resources - Capability/Skill
Skill	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Capability/Skill
Station ID	Interface	Alerting - In Station record	Jurisdiction - Station
Station ID	Interface	Alerting - Out of Station record	Jurisdiction - Station
Stations	Unit Management	Unit Preassignments - General	Jurisdiction - Station
System ID	Interface	Radio - Talkgroups configuration	Interface - Radio - System Configuration (hard coded 0-9)
System to configure channel groups	Interface	Radio - Channel Groups Configuration tab	Interface - Radio - System Configuration
System to Configure Radios	Interface	Radio - Radio System Settings	Interface - Radio - System Configuration
Toning System Name	Interface	Alerting - Toning System	Resources - Systems - Toning
Unit status	Status Monitor	Agency Defaults - MDT - Unit Status Colors subtab - Day mode, night mode	Unit Management - Unit Status Codes - Unit Status Codes - Properties subtab
Unit Status	Mapping	Cadence	Unit Management - Unit Status Codes - Unit Status Codes - Properties subtab
User	Role Permission	Roles - Resources	Resources - Personnel - Details
User ID	Address Book	Address Book - New Entries - General subtab	Resources - Personnel - Details
User ID	Interface	Infotrak	Resources - Personnel - Details

Table 3-2 Provisioning Field Interdependencies – Sorted by Field Name (Cont.)

Field Name	Configuration Item Where Used	Tab	Where Defined
User ID	Interface	Records	Resources - Personnel - Details
User ID	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Personnel - Details
Users	Authentication	Agency Setting - Force Password Change	Resources - Personnel - Details
vehicle capabilities	Mapping	Icons - Unit	Resources - Capability/Skill
Vehicle ID	Resources	Personnel - Resource Assignments	Resources - Vehicle
Vehicle ID	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Vehicle
Vehicle Type	Resources	Vehicle	Lists and Statute Management - Vehicle Types
Vehicle Type Max Speed	Unit Recommendation	Settings - Vehicle Type	Resources - Vehicle

The following table shows the field interdependencies in Provisioning sorted by where the field is defined.

Table 3-3 Provisioning Field Interdependencies – Sorted by Where Defined

Field	Configuration Item Where Used	Tab	Where Defined
Book	Address Book	Group - Entries	Address Book - Address Book
Book	Chat Room	Chat Rooms - Add Member	Address Book - Address Book
Group	Chat Room	Chat Rooms - Add Member	Address Book - Group
Member of Groups	Address Book	Address Book - New Entries - In Groups subtab	Address Book - Group
Agency Type	Agency	Agency	Agency - Agency Type
Alarm	Alarm	Alarm Records - Alarm Company	Alarms - Alarm Companies
Contractor type	Contractor Rotation	Contractors - Contractor Types	Coded in GIS database
Contractors	Contractor Rotation	Rotations	Contractor Rotation - Contractors
Capability Settings	Unit Management	Unit Preassignments - Capability Settings	display only
Equip ID	Resources	Personnel - Resource Assignments	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Resources	Personnel - Resource Assignments	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Resources	Vehicle	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment ID	Unit Management	Unit Preassignments - Personnel & Vehicles	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Unit Management	Unit Preassignments - Personnel & Vehicles	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Equipment Type (devices + equip)	Unit Management	Unit Preassignments - Unit Equipment	for MDT, Devices - Workstation/MDT; for Radio, Devices - Radio
Coverage Group	Resources	Devices - Workstation MDT - Login Settings subtab - General subtab	Incident Management - Coverage Groups
Disposition for closed status	Alarm	Chronic Alarm Settings	Incident Management - Disposition
Disposition	Incident Management	Incident Response Factors - General	Incident Management - Disposition
Disposition	Incident Management	Service Settings - Initiation Defaults - Move Up incidents section	Incident Management - Disposition
Disposition	Interface	Infotrak	Incident Management - Disposition
Disposition	Interface	Records	Incident Management - Disposition
Incident Type	Alarm	Alarm Records - Incident - Time/ Day Specific Setting & Chronic alarm sections	Incident Management - Incident Type

Table 3-3 Provisioning Field Interdependencies – Sorted by Where Defined (Cont.)

Field	Configuration Item Where Used	Tab	Where Defined
Incident type for New or Pending Status	Alarm	Chronic Alarm Settings	Incident Management - Incident Type
Incident Type	Incident Management	Response Messages - Incident Types	Incident Management - Incident Type
Incident Type	Incident Management	Incident Response Factors - General	Incident Management - Incident Type
Incident Type	Incident Management	Incident Response Factors - IRF Attributes	Incident Management - Incident Type
Incident Type	Incident Management	Service Settings - Initiation Defaults - Move up incidents section	Incident Management - Incident Type
Incident Type	Incident Management	Service Settings - Initiation Defaults - Traffic Stops section	Incident Management - Incident Type
Incident Type	Interface	Alerting - In Station Record	Incident Management - Incident Type
Incident Type	Interface	Alerting - Out of station Record	Incident Management - Incident Type
Incident Type	Interface	Infotrak	Incident Management - Incident Type
Incident Type	Interface	Records	Incident Management - Incident Type
Incident Type	Mapping	Icons	Incident Management - Incident Type
Incident Type	Unit Recommendation	Response Card - Incident Response Factor - General	Incident Management - Incident Type
Incident Type	Unit Recommendation	Run Card - IRF	Incident Management - Incident Type
Modifying Circumstance	Alarm	Alarm Records - Incident - Time/ Day Specific Setting & Chronic alarm sections	Incident Management - Modifying Circumstance
Modifying Circumstance (M.C.)	Alarm	Chronic Alarm Settings	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Incident Response Factors - General	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Incident Response Factors - IRF Attributes	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Service Settings - Initiation Defaults - Move Up incidents section	Incident Management - Modifying Circumstance
Modifying Circumstance	Incident Management	Service Settings - Initiation Defaults - Traffic Stops section	Incident Management - Modifying Circumstance
Modifying Circumstance	Unit Recommendation	Response Card - Incident Response Factor - General	Incident Management - Modifying Circumstance
Modifying Circumstance	Unit Recommendation	Run Card - IRF	Incident Management - Modifying Circumstance
Message to be Sent	Alarm	Alarm Records - Incident	Incident Management - Response Messages

Table 3-3 Provisioning Field Interdependencies – Sorted by Where Defined (Cont.)

Field	Configuration Item Where Used	Tab	Where Defined
Response message sent for No incident status	Alarm	Chronic Alarm Settings	Incident Management - Response Messages
Response Message to be sent	Alarm	Alarm Records - Incident	Incident Management - Response Messages
Priority	Incident Management	Incident Response Factors - IRF Attributes	Incident Management - Service Settings - Priorities
System to configure channel groups	Interface	Radio - Channel Groups Configuration	Interface - Radio - System Configuration
System to Configure Radios	Interface	Radio - Radio System Settings	Interface - Radio - System Configuration
System ID	Interface	Radio - Talkgroups configuration	Interface - Radio - System Configuration (hard coded 0-9)
Channels	Interface	Radio - Channel Groups Configuration	Interface - Radio - Talkgroups
Radio System	Interface	Radio - Radio System Settings	Interface Radio - System Configuration
Radio System	Interface	Radio - Talkgroups	Interface Radio - System Configuration
Station ID	Interface	Alerting - In Station record	Jurisdiction - Station
Station ID	Interface	Alerting - Out of Station record	Jurisdiction - Station
Stations	Unit Management	Unit Preassignments - General	Jurisdiction - Station
Auto club	Contractor Rotation	Contractors - General	Lists and Statute Management - LSM - Auto Club
Payment Method	Contractor Rotation	Contractors - General	Lists and Statute Management - LSM - Payment Method
Vehicle Type	Resources	Vehicle	Lists and Statute Management - Vehicle Types
Manual Notification	Incident Management	Incident Response Factors - IRF Attributes	Notification - Manual Notification
Jurisdictional units	Contractor Rotation	Rotations	Plan Management - Plans
Areas	Incident Management	Response Messages -Areas/Sect/ Beat	Plan Management - Plans
Beats	Incident Management	Response Messages - Areas/Sect/ Beat	Plan Management - Plans
Sectors	Incident Management	Response Messages - Areas/Sect/ Beat	Plan Management - Plans
Area	Incident Management	Coverage Groups	Plan Management - Plans
Beat	Interface	Infotrak	Plan Management - Plans
Beat	Interface	Records	Plan Management - Plans
Area	Mapping	MUD Setting	Plan Management - Plans
Beat	Mapping	MUD Setting	Plan Management - Plans

Table 3-3 Provisioning Field Interdependencies – Sorted by Where Defined (Cont.)

Field	Configuration Item Where Used	Tab	Where Defined
Sectors	Mapping	MUD Setting	Plan Management - Plans
Active Plan ID	Plans	Active Plan ID	Plan Management - Plans
Plan ID	Plans	Active Plan	Plan Management - Plans
Area	Resources	Personnel - Preassignments	Plan Management - Plans
Beat	Resources	Personnel - Preassignments	Plan Management - Plans
Sectors	Resources	Personnel - Preassignments	Plan Management - Plans
Area	Unit Management	Unit Preassignments - General	Plan Management - Plans
Beat	Unit Management	Unit Preassignments - General	Plan Management - Plans
Sectors	Unit Management	Unit Preassignments - General	Plan Management - Plans
Device Type category	Resources	Device Types - General	Read only; workstation and MDT
Capability Group Code	Unit Management	Unit Preassignments - Unit Capabilities	Resources - Capability Groups
Capability	Contractor Rotation	Contractors - General	Resources - Capability/Skill
vehicle capabilities	Mapping	Icons - Unit	Resources - Capability/Skill
Capability	Resources	Vehicle	Resources - Capability/Skill
Capability	Resources	Capability Group	Resources - Capability/Skill
Skill	Resources	Personnel - Details	Resources - Capability/Skill
Capabilities	Unit Management	Unit Preassignments - Unit Capabilities	Resources - Capability/Skill
Capability	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Capability/Skill
Skill	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Capability/Skill
Capability	Unit Recommendation	Run Card - Resp ID	Resources - Capability/Skill
Device Profile	Devices	Radio	Resources - Device Profile - General
Device Type	Resources	Devices - Workstation MDT - General subtab	Resources - Device Types; Workstation and MDT hardcoded
Device (this is Device ID)	Resources	Personnel - Authorization	Resources - Devices - Workstation/MDT
User ID	Address Book	Address Book - New Entries - General subtab	Resources - Personnel - Details
Recipients	Authentication	Agency Setting - System Notification	Resources - Personnel - Details
Users	Authentication	Agency Setting - Force Password Change	Resources - Personnel - Details
Owned by	Chat Room	Chat Rooms - General	Resources - Personnel - Details

Table 3-3 Provisioning Field Interdependencies – Sorted by Where Defined (Cont.)

Field	Configuration Item Where Used	Tab	Where Defined
User ID	Interface	Infotrak	Resources - Personnel - Details
User ID	Interface	Records	Resources - Personnel - Details
Contacts	Notification	Manual Notification	Resources - Personnel - Details
Recipients	Notification	Emergency Notification	Resources - Personnel - Details
Recipients	Notification	Manual Notification	Resources - Personnel - Details
Recipients	Resources	Device Types - Login	Resources - Personnel - Details
User	Role Permission	Roles - Resources	Resources - Personnel - Details
User ID	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Personnel - Details
Toning System Name	Interface	Alerting - Toning System	Resources - Systems - Toning
Vehicle ID	Resources	Personnel - Resource Assignments	Resources - Vehicle
Vehicle ID	Unit Management	Unit Preassignments - Personnel & Vehicles	Resources - Vehicle
Vehicle Type Max Speed	Unit Recommendation	Settings - Vehicle Type	Resources - Vehicle
Role	Address Book	Address Book - Add Existing Entries	Role Permission - Roles
Role	Address Book	Address Book - New Entries - General subtab	Role Permission - Roles
Role	Address Book	Group - Entries	Role Permission - Roles
Role	Chat Room	Chat Rooms - Add Member	Role Permission - Roles
Role	Resources	Devices - Workstation MDT - Login Settings - General	Role Permission - Roles
Role	Resources	Personnel - Roles	Role Permission - Roles
Duty Type	Interface	Alerting - In Station Record	Unit Management - Duty Type
Duty Type	Interface	Alerting - Out of station Record	Unit Management - Duty Type
Duty Type	Unit Management	Unit Preassignments - General	Unit Management - Duty Type
Unit Status	Mapping	Cadence	Unit Management - Unit Status Codes - Unit Status Codes - Properties subtab
Unit status	Status Monitor	Agency Defaults - MDT - Unit Status Colors subtab - Day mode, night mode	Unit Management - Unit Status Codes - Unit Status Codes - Properties subtab
Default Unit Status	Unit Management	Settings - Transactions	Unit Management - Unit Status Codes - Unit Status Codes - Properties subtab
Response Category Code	Resources	Capability/Skill	Unit Recommendation - Response Category

Table 3-3 Provisioning Field Interdependencies – Sorted by Where Defined (Cont.)

Field	Configuration Item Where Used	Tab	Where Defined
Response Class	Jurisdiction	Area	Unit Recommendation - Response Class
Response Class	Jurisdiction	Beat	Unit Recommendation - Response Class
Response Class	Jurisdiction	Location	Unit Recommendation - Response Class
Response Class	Jurisdiction	Sector	Unit Recommendation - Response Class
Response Class	Unit Recommendation	Run Card - Resp ID	Unit Recommendation - Response Class
Response ID	Incident Management	Incident Response Factors - IRF Attributes	Unit Recommendation - Response IDs
Response ID	Unit Recommendation	Run Card - Resp ID	Unit Recommendation - Response IDs
Response Mode	Unit Recommendation	Run Card - Resp ID	Unit Recommendation - Response Mode

Diagrams of Field Interdependencies

The following diagrams show the field interdependencies for incident management, resource management, recommendations, and interfaces. The diagrams are provided for import relationship overviews and are not intended to be comprehensive.

Incident Management Field Interdependencies

The following diagram shows the field interdependencies for incident management.

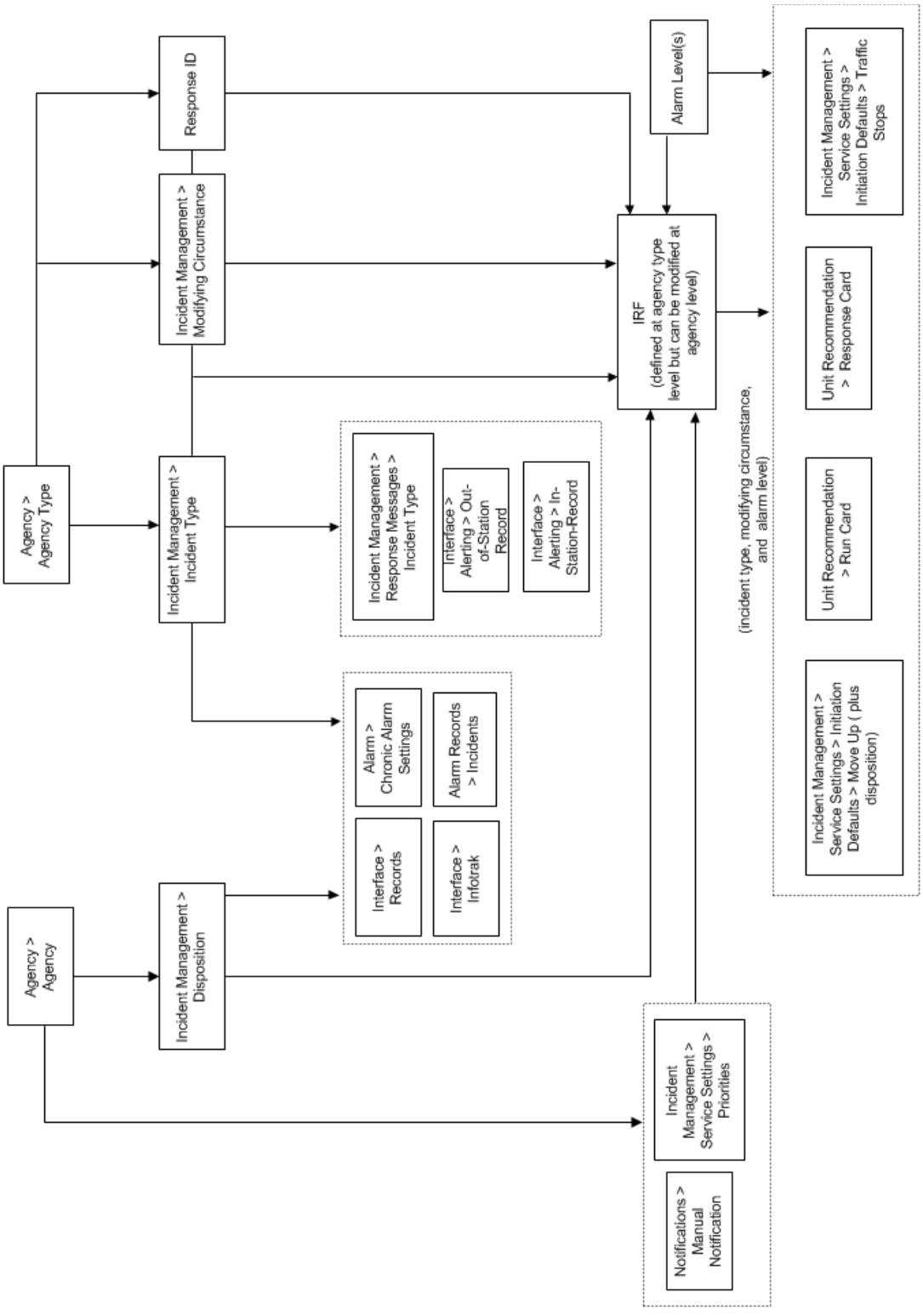


Figure 3-1 Diagram of Field Interdependencies for Incident Management

Resource Management Field Interdependencies

The following diagram shows the field interdependencies for resource management.

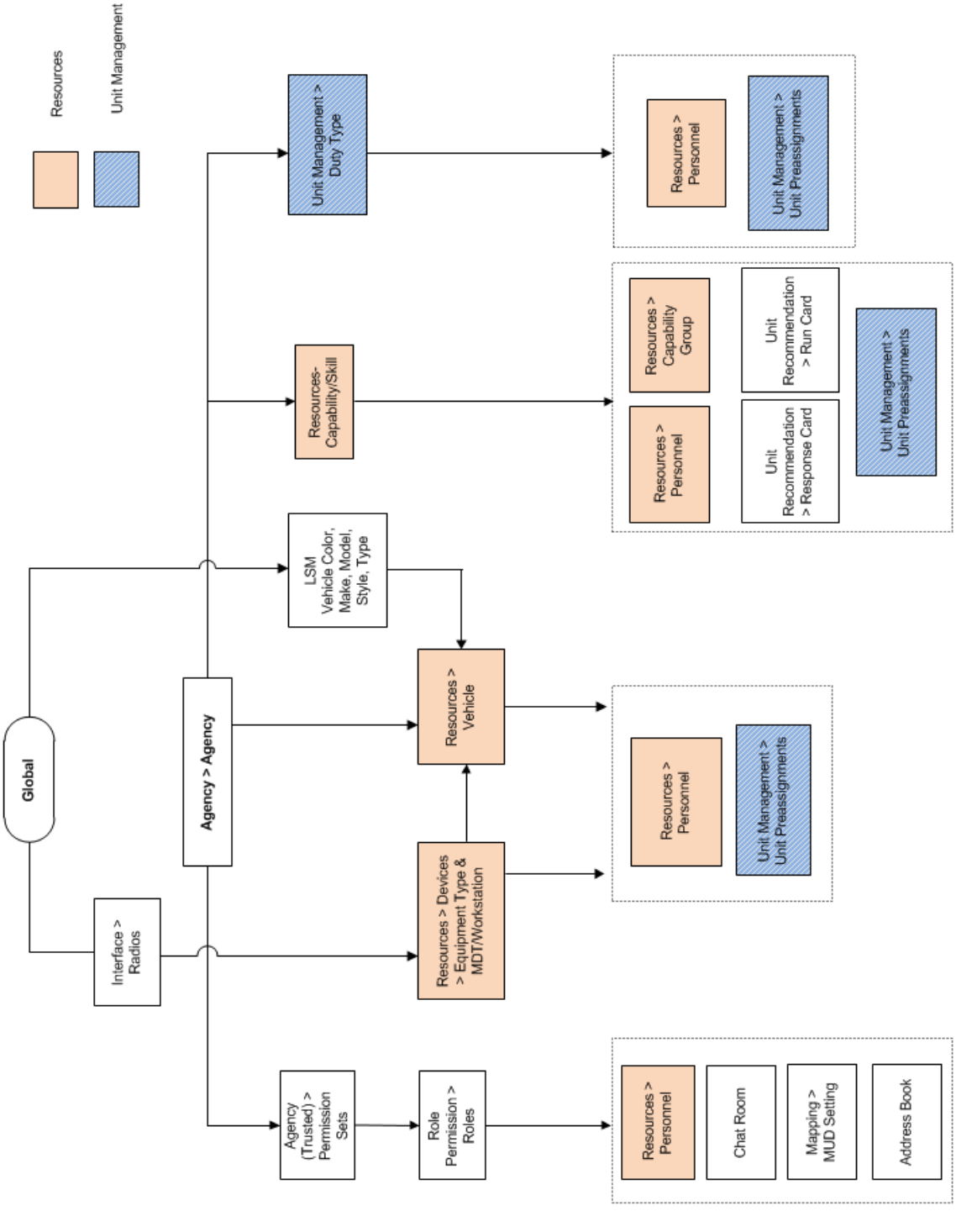


Figure 3-2 Diagram of Field Interdependencies for Resource Management

Recommendations Field Interdependencies

The following diagram shows the field interdependencies for recommendations.

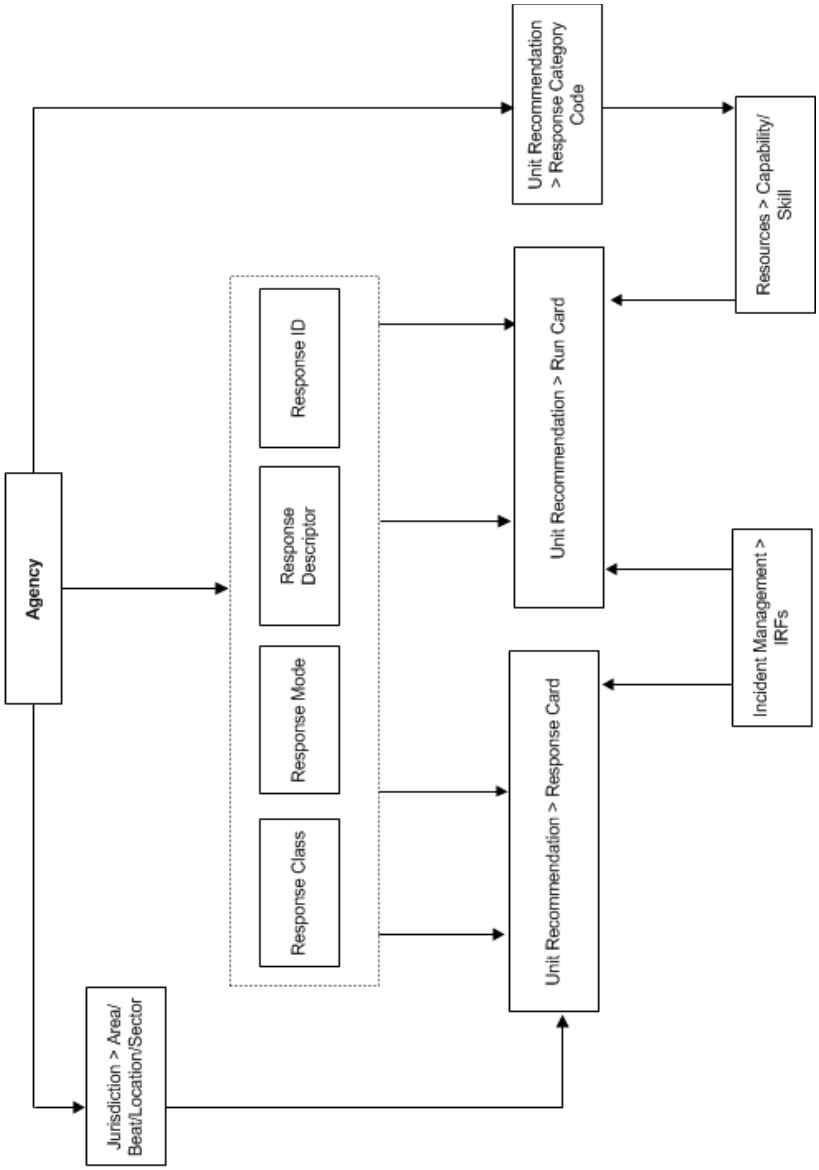


Figure 3-3 Diagram of Field Interdependencies for Recommendations

Interfaces Field Interdependencies

The following diagram shows the field interdependencies for interfaces.

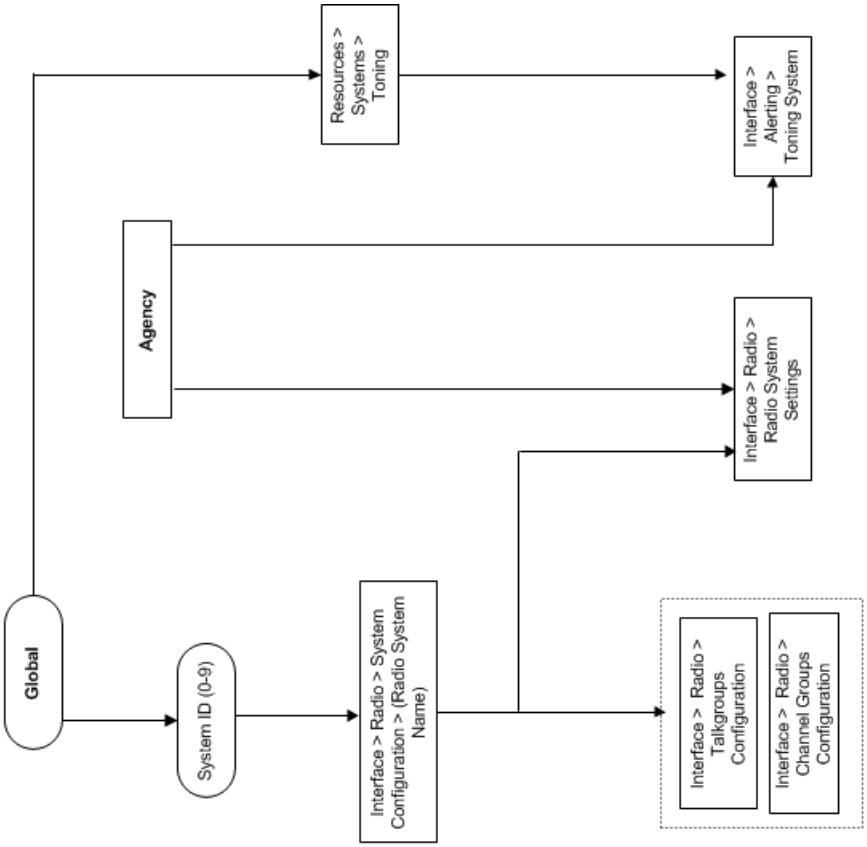


Figure 3-4 Diagram of Field Interdependencies for Interfaces

CHAPTER 4

Configuring Agencies and Agency Types

The Agency configuration item contains the following items:

- Agency Types – Where you set the names and descriptions for agency types, such as fire, law, and EMS. For details, see “Configuring Agency Types” on page 4-2.
- Agencies – Where you set the details for the agencies you work with, such as agency ID, agency type, agency name, and default area. For details, see “Configuring Agencies” on page 4-3.

PremierOne can operate in a variety of Public Safety Answering Points (PSAPs):

- Single Agency
- Multi-Agency/Single Jurisdictional
- Multi-Agency/Multi-Jurisdictional

In addition to these, any number of PSAPs can share a single CAD system. This is known as a distributed PSAP environment. Any agency within a multi-agency PSAP facility can operate autonomously from all other agencies within the PSAP, while using the same CAD system as everyone else.

NOTES

For a multi-agency environment, configure the Lists (code tables) BEFORE adding the individual agencies. If the Lists configuration is not done before adding individual agencies, then each agency must be also individually configured.

If you create an agency for equipment only, be sure that you assign an active agency for radio coverage for off duty radios in emergency. If you do not, then activation of the emergency button on an off duty radio may go unnoticed because there is no CAD coverage for the off duty radio.

Configuring Agency Types

Use the Agency Type configuration item to create or modify agency types. You can add, modify, and delete agency types. For details on modifying and deleting agency types, see “Working With Configuration Items” on page 2-9. You cannot change the Agency Type Name. If you want to change the name, you must delete and re-add the record.

To add new agencies, you must create the new agency types first.

Adding Agency Types

When you add an agency type, you enter information on the Details tab of the Agency Type form.

To add an agency type:

1. From the navigation panel, select **Agency**, and then select **Agency Type**.

   The Agency Type form appears in the work area. A list of existing agency types displays on the left side of the window.

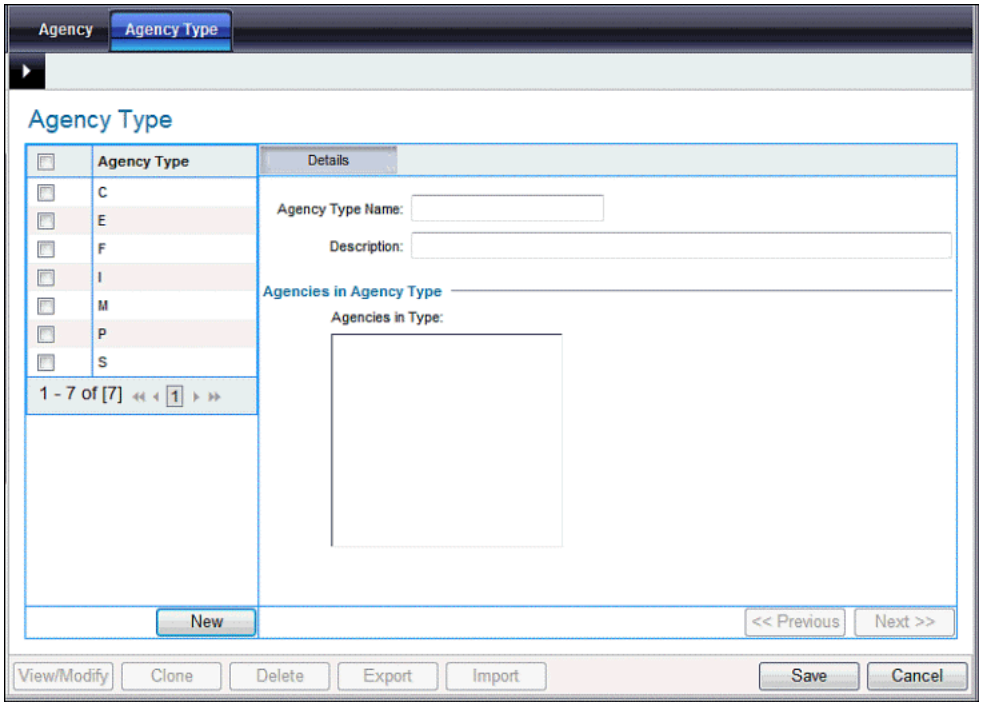


Figure 4-1 Agency Type Form

2. At the bottom of the Agency Type list, click the **New** button.

3. In the Agency Type Name field, type a name for the new agency type.

   While this field allows for 15 characters, shorter agency type names are easier to manage.

4. In the Description field, type a description for the new agency type.

   The Agencies in Agency Type section is a view-only field that displays which agencies use the selected type.

   The unsaved agency type appears in the list on the left in blue text.

5. Click **Save**.

   The agency types you added appear in the list on the left in black text.

Configuring Agencies

Use the Agency configuration item to set the details for the agencies you work with, such as agency ID, agency type, agency name, and default area.

You can add, modify, clone, and delete agencies. For details on modifying and deleting agencies, see “Working With Configuration Items” on page 2-9. You cannot change the Agency ID. If you want to change the ID, you must delete and re-add the record.

To add new agencies, you must create the new agency types first.

CAUTION

Be sure to assign the correct agency type to your agencies. If you assign the wrong agency type to an agency, the only way to correct the problem is to delete the agency and add the agency under a different name. This may also require database changes.

Adding Agencies

When you add an agency, you enter information on the Agency tab of the Agency form. You can also add an agency by cloning an existing agency that closely matches the one you want to add.

Agency details include the agency ID, agency name, agency type, default area, contact information, whether this is a foreign agency, whether to use stations rather than areas, the default units for time, distance, height, and weight, and alias display settings.

To add agency details:

1. From the navigation panel, select **Agency**, and then select **Agency**.

   The Agency form appears. A list of existing agencies displays on the left side of the window.

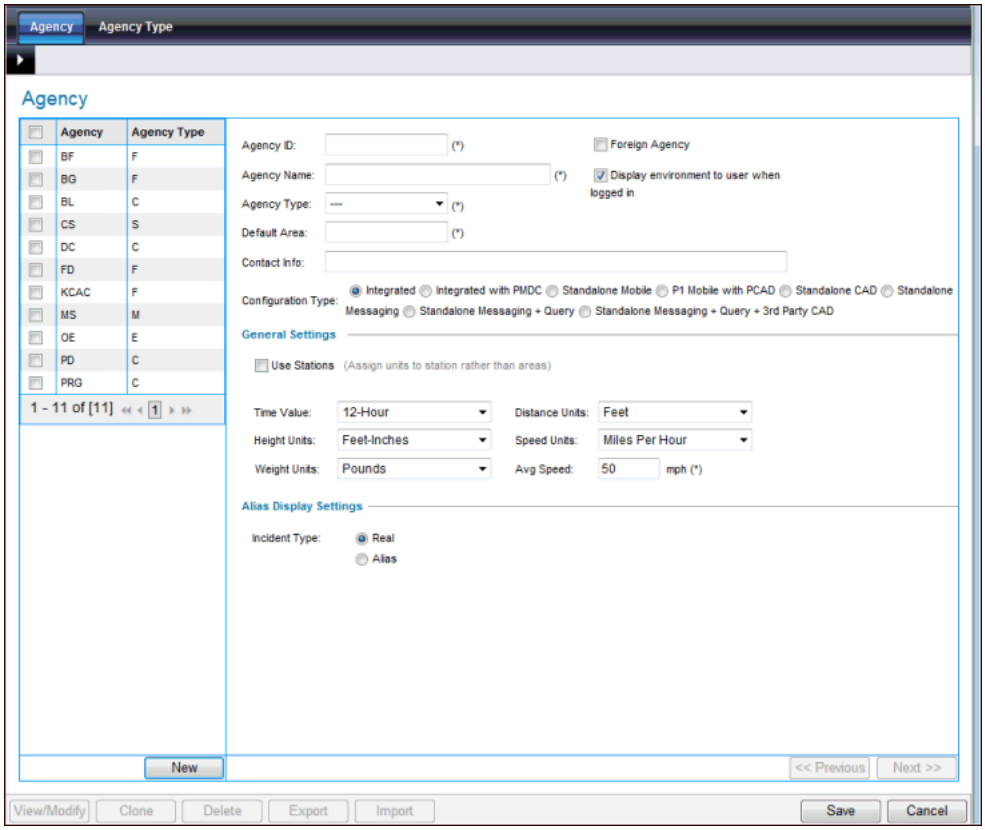


Figure 4-2 Agency Form

2. At the bottom of the Agency list, click the **New** button.
3. In the Agency ID field, type agency identification code.

   The agencies you set up must match the agencies in your GIS file.

4. If this is a foreign agency, select the Foreign Agency check box.

A foreign agency is an agency being managed within a foreign, or external, CAD system connected to PremierOne via the Cad-to-Cad interface.

5. In the Agency Name field, type the name of the agency.
6. If you want to display the environment to users when they are logged in, such as Production, select the Display Environment to Users When Logged In check box.

   The environment displays in the Information panel.
7. In the Configuration Type section, select your deployment mode. The options that appear on the screen depend on the options that were selected when PremierOne was installed. The options include:

   - Integrated – Includes all the components of PremierOne: Common Services, Mobile, and PremierOne CAD.
   - Integrated with PMDC – Includes all the components of PremierOne: Common Services, Mobile, and PremierOne CAD, plus PMDC.
   - Standalone Mobile – Includes only Common Services and Mobile.
   - P1 Mobile with PCAD – Includes Common Services and PremierCAD.
   - Standalone CAD – Includes only Common Services and PremierOne CAD.
   - Standalone Messaging – Includes Common Services only for messaging.
   - Standalone Messaging + Query – Includes Common Services only for messaging and query.
   - Standalone Messaging + Query + 3rd Party CAD – Includes Common Services only for messaging, query, and 3rd Party CAD.
8. In the General Settings section, do the following:

   - To use stations instead of areas, select the **Use Stations** check box.
   - Select the time format: 24-hr or 12-hr. The 12-hr format will display AM or PM.
   - Select the default units to use for distance, height, weight, speed, and average speed. The average speed is used to calculate the time required to travel between two points using known distance and determine the estimated time of arrival (ETA).
9. In the Alias Display section, do one of the following:

   - To display the real incident type in CAD forms, select Real.
   - To display the alias incident type in CAD forms for incidents created with an alias, select Alias.
10. In the Foreign CAD Settings section, do the following:

- From the Foreign CAD System list, select the foreign CAD system to use.
- If you want to transfer all incidents created for the signed-on agency on the local CAD system to the foreign CAD system, select the Transfer (to the foreign CAD system) all incidents created for this agency on the local CAD system check box.
- If you want to receive unit status updates from the sign-on agency on the local CAD system, select the Receive (on the local CAD system) unit status updates from this agency check box.

11. To add another agency, click **New**, and then repeat the previous steps.

    Each unsaved agency appears in the Agency list on the left in blue text.

12. Click **Save**.

    The agencies you added appear in the Agency list on the left in black text.

Adding Agencies by Cloning

Add an agency by cloning when you already have an agency that closely matches the one you want to add.

To add an agency by cloning:

1. Access the form for a new agency. For instructions, see “Adding Agencies” on page 4-4.

   The Agency form appears in the work area (see Figure 4-2). A list of existing agencies displays on the left side of the form.

2. From the Agency list on the left side of the form, select the agency you want to clone. Selecting the check box does not select the item.

3. Click **Clone**.

The Cloning Agency dialog box appears.

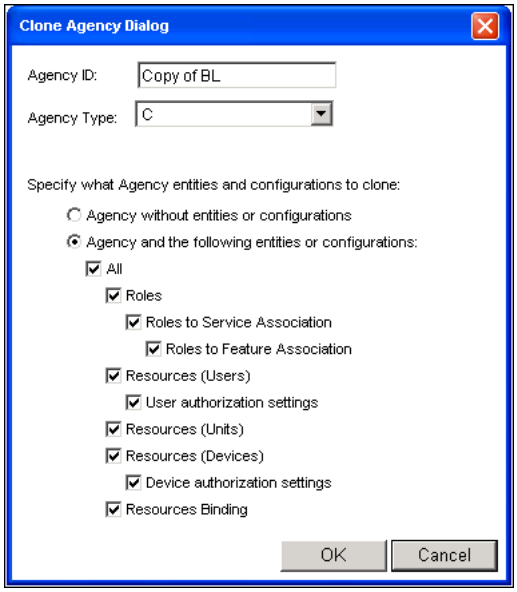


Figure 4-3 Cloning Agency Dialog Box

4. In the Agency ID field, type the name of the new agency you are creating.
5. If necessary, change the Agency Type value.
6. In the Agency entities and configurations section, select the items you want to include.

   You can include roles, role associations (the levels that cloning should include), user resources, unit resources, device resources, or any combination of those options.

   - The Roles to Service Association option maintains the relationship between roles and services. Services include the various functions provided by PremierOne such as address books, chat, GIS mapping, Provisioning, messaging, query, and so on.
   - The Roles to Feature Association option maintains the relationship between roles and features. Features include the various commands and functions associated with a service.
   - The Resources Binding option maintains the association of equipment to a person.

7. Click **OK**.
8. Click **Save**.
9. To modify the cloned record, click **View/Modify**.

CHAPTER 5

Configuring Trusted Agencies

The Agency (Trusted) configuration item contains one item:

Permission Set – Where you set the permission levels for other agencies to access and manage the incidents in your agency. The ability to share CAD data across agencies is at the discretion of each agency. For details, see “Configuring Trusted Agencies” on page 5-3.

In a multi-agency environment, the sharing of CAD data across agencies is dependent on the arrangement of their operations within the environment:

- If the agencies have a common set of call takers, the call takers must be able to create incidents for all of the agencies.
- If the agencies operate with separate call takers, the sharing of data must be secured and controlled in order to separate the agencies into their respective operations.

To differentiate agencies, the following terms are used:

- Owning agency – The agency that grants access to another agency.
- Trusted agency – The agency that is granted access to another agency’s data.

The provisioning of trust relationships assumes the implementation of the single environment per CAD system. Otherwise, the trust relationships are established for all agencies within an Environment.

NOTE

Unless explicitly granted permission to the Agency, Authorization & Roles Provisioning feature, another agency can never administer another agency's permission set.

Commands Exempt from Trusted Agency Provisioning

The following list contains the commands that are **not** controlled by trusted agency provisioning.

- BOLO Read
- Location Detail
- Message Read
- Notification Read
- Online Mode
- Query Request
- Query Response
- Reports Menu
- Send Message (NT)
- Send Notification
- Clear work area

Understanding Permission Sets

A permission set is a group of agencies that have the same combination of Provisioning access and CAD command-level access. The number of permission sets that need to be provisioned for an agency is dependent on the different combinations of access that the Owning agency may grant to Trusted agencies.

When a user signs on to CAD or Provisioning, the role that the user selects at the time of signon determines what access the user has during the session. The user can only access Provisioning or CAD commands based on the permissions granted to the user's role.

The following access is available for Provisioning elements:

- No Access
- Read-Only access
- Full administrative access (Read, Insert/Add, Update, and Delete)

The following access is available for CAD commands:

- No access
- Access

Configuring Trusted Agencies

Use the Permission Set configuration item to create or modify permission sets, a group of agencies that have the same combination of Provisioning access and CAD command-level access.

You cannot import or clone permission sets, but you can export and modify them. For details on exporting and modifying permission sets, see "Working With Configuration Items" on page 2-9. You cannot change the Permission Set Name. If you want to change the name, you must delete and re-add the record.

Adding Permission Sets

When you add a permission set, you enter a name and description, and then select the agencies to add to the permission set.

To add a permission set:

1. From the navigation panel, select **Agency (Trusted)**, and then select **Permission Set**.

The Permission Set form appears in the work area. A list of existing permission sets displays on the left side of the form.

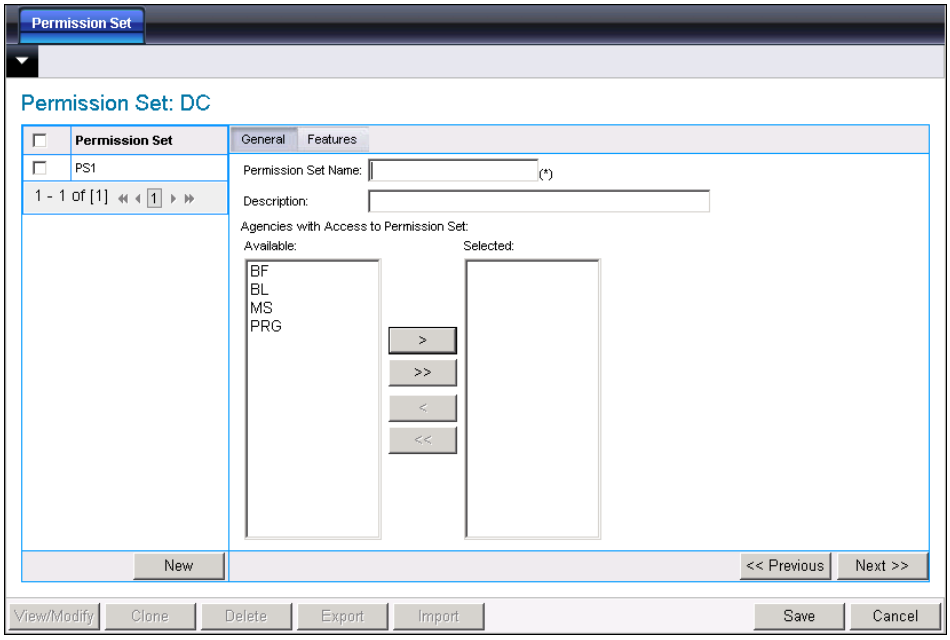


Figure 5-1 Permission Set Form – General Tab

2. At the bottom of the list of permission sets, click the **New** button.
3. In the Permission Set Name field, enter a name for the permission set.
4. In the Description field, enter information describing the permission set.
5. From the Available list, select the agency you want to add to the permission set and add it to the Selected list.

   An Owning agency can only assign one permission set to each Trusted agency. If you assign a permission set to a Trusted agency, the agency does not display in the Available list for other permission sets.

   The permission set must include access to all Provisioning elements or commands that the Trusted agency is expected to perform.

Setting Permissions Within a Permission Set

For each permission set, you must set access to Provisioning elements and CAD commands.

To set permissions within a permission set:

1. Access the form for permission sets. For instructions, see "Adding Permission Sets" on page 5-3.

   The Permission Set form appears in the work area (see Figure 5-1). A list of existing permission sets displays on the left side of the form.

2. Select the permission set for which you want to configure access.

3. Click the Features tab.

   The Commands (Trusted) and Provisioning (Trusted) items display on the left side of the window in the Services list.

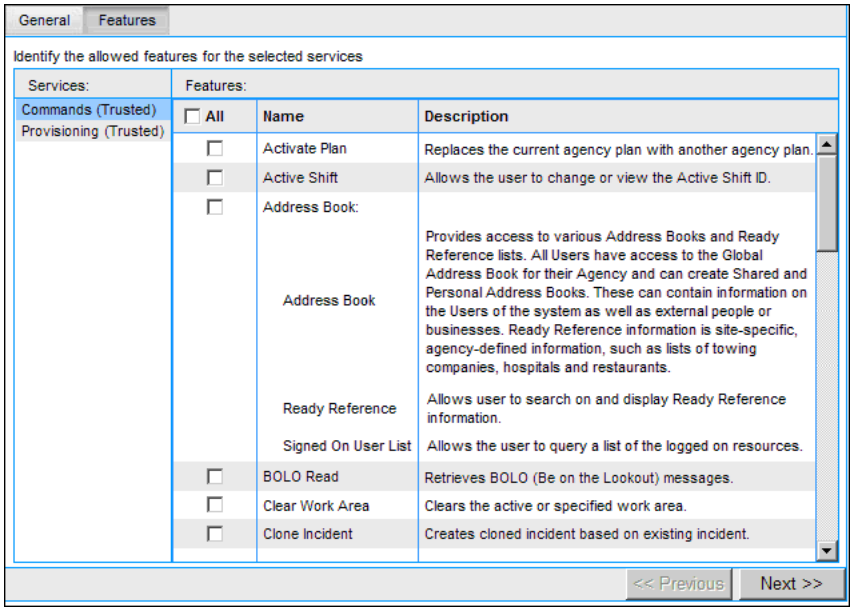


Figure 5-2 Permission Set Form – Features Tab For Commands (Trusted)

4. Continue with the following procedures:

   - "Setting CAD Command Access for Trusted Agencies" on page 5-6
   - "Setting Provisioning Access for Trusted Agencies" on page 5-7

Setting CAD Command Access for Trusted Agencies

You set CAD command access and Provisioning access separately. For details on setting Provisioning access, see “Setting Provisioning Access for Trusted Agencies” on page 5-7.

To set CAD command access for trusted agencies:

1. Open the Features tab.

   For details, see “Setting Permissions Within a Permission Set” on page 5-5.

2. Select the agency and click **View/Modify**.

3. In the Services list, select the **Commands (Trusted)** service.

   A list of available commands and their description display on the right side of the window (see Figure 5-2).

4. Select the access for each command for the permission set.

   - To grant access to all commands, select the **All** check box.
   - To grant access to specific commands, select the check box for the commands.

NOTE
Access cannot be set for command aliases.

There are three types of command groups:

- Independent commands – Consist of a single command. When you grant access to the command, only the command receives access.
- Command groups – Consist of similar or related commands, such as message read and send message. When you grant access to the group, then all commands in the group receive access. You cannot individually select any of the commands in the group. Relational groups consist of the following:

  Address Book (Address Book, Ready Reference, Signed On User List)

  Messaging (Message Read, Send Message)

  Notification (Notification Read, Send Notification)

  Premise Hazard (Create Record, View Record)

  Query (Query Request, Query Response)

  Radio (Console Talkgroups, Select Group)

  Unit Duty (Off Duty, On Duty, Unit Assignment)

Unit Status (Call Stacking, Unit Status)

Read-Only (Incident Recall, Incident History)

- Hierarchical command groups – Consists of commands that overlap in functionality; Incident is the only hierarchical command group. The highest level in the group is Incident Dispatch. If you select Incident Dispatch, then access is automatically granted to the commands below it: Contractor Rotation, Contractor Update, Incident Update, and Read-Only Incident Recall and Incident History.

  When you select one of the check boxes within the hierarchical command group, the check boxes for all the *lower-level* commands are automatically selected.

  When you clear a check box within the hierarchical command group, the check boxes for all the *higher-level* commands are automatically unselected.

Setting Provisioning Access for Trusted Agencies

You set CAD command access and Provisioning access separately. For details on setting Provisioning access, see "Setting CAD Command Access for Trusted Agencies" on page 5-6.

NOTE

As of version 3.3, Workload Transfer is now enabled under the Sign On Coverage feature.

To set Provisioning access for trusted agencies:

1. Open the Features tab.

   For details, see "Setting Permissions Within a Permission Set" on page 5-5.

2. Click **View/Modify**.

3. In the list of services, select the **Provisioning (Trusted)** service.

   A list of available Provisioning features and their description display on the right side of the window.

Provisioning features are grouped together into sets. There isn't a direct correlation between features and the Provisioning elements in the Provisioning folder list.

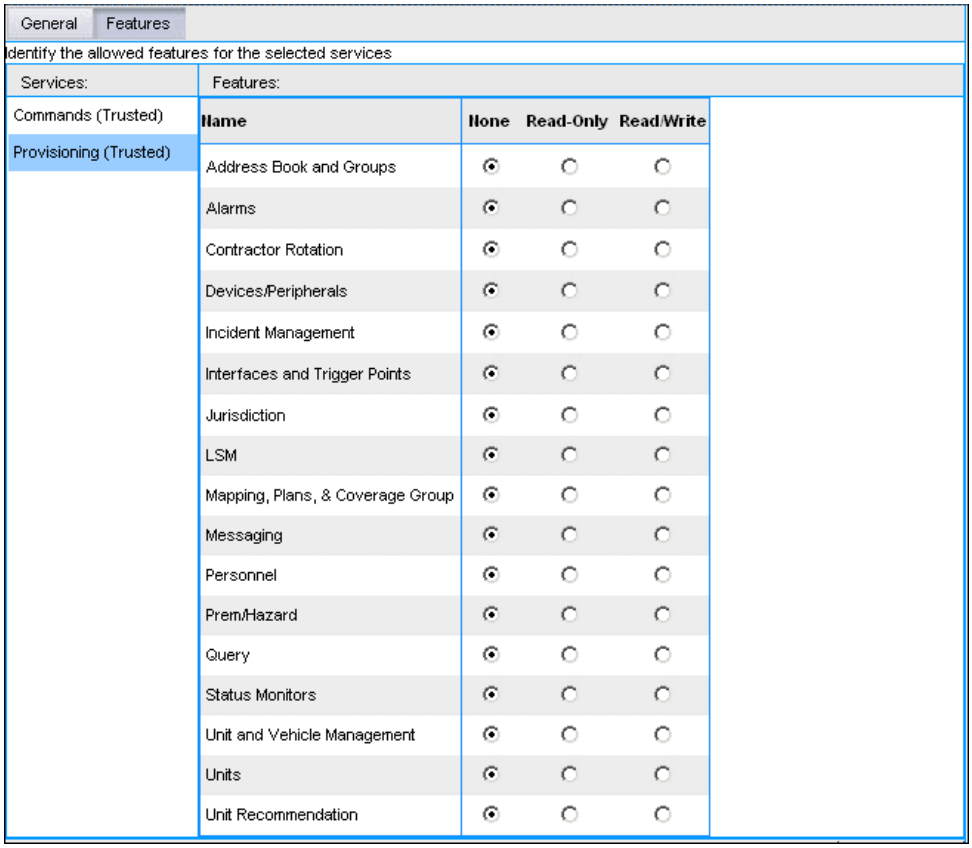


Figure 5-3 Permission Set Form – Features Tab For Provisioning (Trusted)

4. Select the access for each Provisioning element for the permission set.

   - None – Trusted agency has no access.
   - Read Only – Trusted agency can only view the item.
   - Read/Write – Trusted agency can View, Insert/Add, Update, and Delete the item.

   Each Provisioning element must be granted permission individually; there is not a global setting, as there is for commands.

5. Click **Save**.

   The permission set is created and is available to the Trusted agency. The Trusted agency can use the permission set as you created it or make modifications to it. Access can only remain unmodified or be lowered; it cannot be increased.

Granting Role Permissions by Owning Agencies

Once the permission sets are created by the Owning agency, the system administrator can make modifications to the access granted to the Owning agency. The system administrator can only leave the access as it is or lower the access.

To grant role permissions by owning agencies:

1. Access the form for a role. For instructions, see "Adding Roles" on page 8-2.

   The Roles form appears with the General tab in focus (see Figure 8-2). A list of existing roles displays on the left side of the tab.

2. Select the role for which you want to configure permissions.

3. Click **View/Modify**.

   The tabs and fields become editable.

4. Click the Permissions tab.

5. Select the Services subtab.

   Available services display in the left box and Selected services display in the right box.

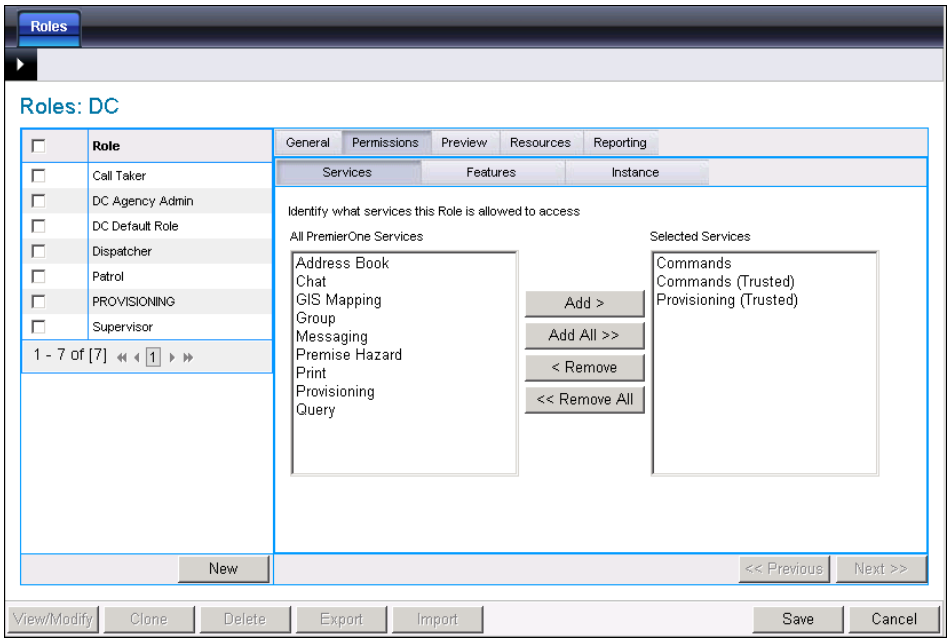


Figure 5-4 Roles Form – Permissions Tab, Services Subtab

6. Do any of the following:

   - To grant access to commands in trusted agencies for the role, select **Commands (Trusted)** and add it to the list of Selected Services.

- To grant access to Provisioning features in trusted agencies for the role, select the **Provisioning (Trusted)** service and add it to the list of Selected Services.

7. Continue with the following procedures:

   - “Setting CAD Command Access for Roles” on page 5-10
   - “Setting Provisioning Access for Roles” on page 5-11

Setting CAD Command Access for Roles

You set access to CAD commands and Provisioning elements separately. To set permissions for Provisioning, see “Setting Provisioning Access for Roles” on page 5-11.

To set CAD command access for roles:

1. In the Roles form, open the Features tab for your agency.

   For details, see “Granting Role Permissions by Owning Agencies” on page 5-9.

2. In the Services list, select the Commands (Trusted) service.

   The list of commands and trusted agencies that granted command access to your agency displays. Commands are listed on the left side of the tab and the trusted agencies are listed along the top of the tab. By default, all check boxes are not selected.

If an Owning agency did not grant your agency access to a command, then a check box will not be in the respective column for that agency.

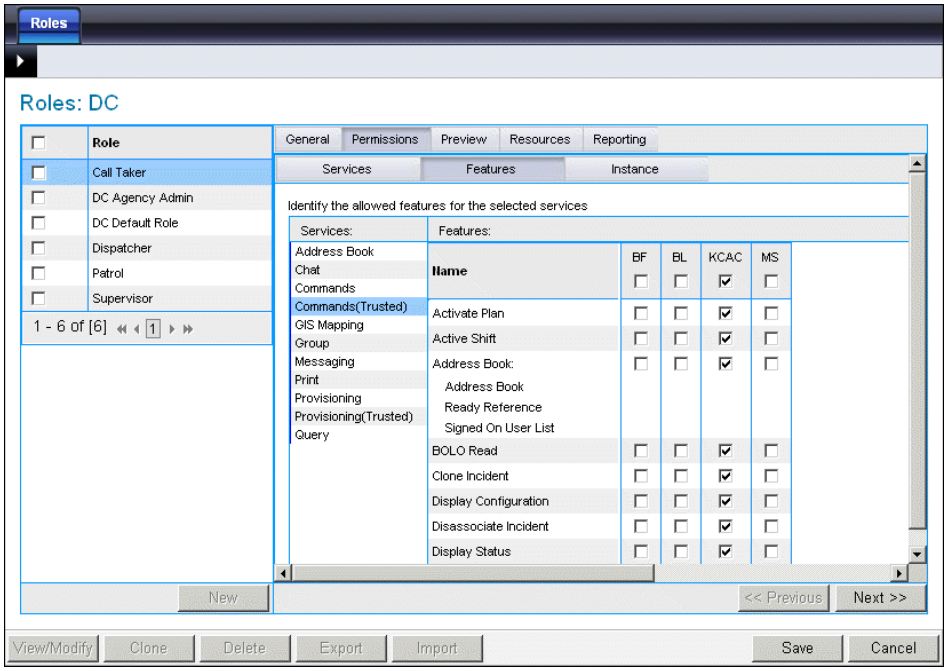


Figure 5-5 Roles Form – Permissions – Features Subtab For Commands (Trusted)

3. Make any modifications you need to the command access.

   You can select the check box at the top of the column below an agency name to select all commands in the column.

   If the Owning agency should make changes to the permission set, the updates are inherited as follows:

   - Access granted – A new check box appears for the Trusted agency and corresponding command.
   - Access denied – The existing check box is removed from the Trusted agency and corresponding command.

Setting Provisioning Access for Roles

You set access to CAD commands and Provisioning elements separately. To set permissions for Provisioning, see “Setting CAD Command Access for Roles” on page 5-10.

To set Provisioning access for roles:

1. In the Roles form, open the Features tab for your agency.

   For details, see “Granting Role Permissions by Owning Agencies” on page 5-9.

2. In the Services list, select the **Provisioning (Trusted)** service.

   The list of Provisioning elements and agencies granting access to the elements displays. Radio buttons only display for the access rights your agency was granted.

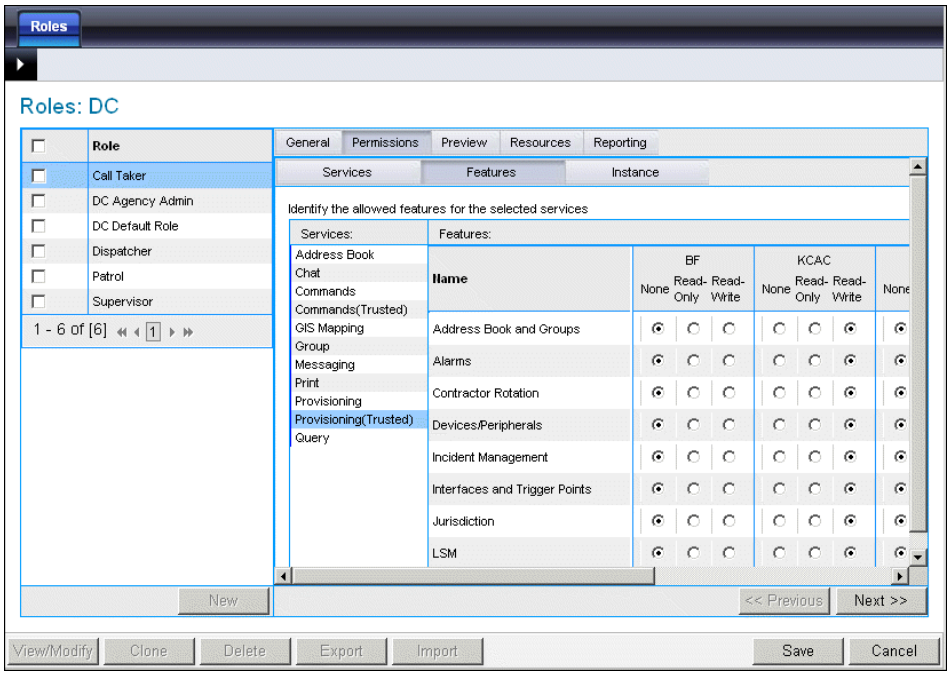


Figure 5-6 Roles Form – Permissions – Features Subtab For Provisioning

3. Make any modifications you need to the Provisioning access.

   If the Owning agency should makes changes to the permission set, the updates are inherited as follows:

   - None to Read-Only – None and Read-Only radio buttons appear for the Trusted agency and corresponding Provisioning feature. The default value is None.
   - None to Read/Write – None, Read-Only, and Read/Write radio buttons appear for the Trusted agency and corresponding Provisioning feature. The default value is None.
   - Read-Only to Read/Write – The Read/Write radio button appear for the Trusted agency and corresponding Provisioning feature. The current value is maintained.
   - Read-Only to None – Existing radio buttons are removed from the Trusted agency and corresponding Provisioning feature.

- Read/Write to Read-Only – The Read/Write radio button is removed from the Trusted agency and corresponding Provisioning feature. The current value is maintained unless it is Read/Write; then the value is set to Read-Only.
- Read/Write to None – Existing radio buttons are removed from the Trusted agency and corresponding Provisioning feature.

4. Click **Save**.

CHAPTER 6

Configuring Lists and Codes

The Lists and Statue Management configuration item contains the following item:

LSM – Where you manage lists of items with their descriptions, qualifiers, and codes, such as vehicle colors, makes, models, and styles. For details, see "Configuring Standard Lists" on page 6-2 and "Configuring New Lists and List Items" on page 6-6.

NOTE

Configuration of codes should be done first globally so it will apply to all agencies. If the configuration is not done before adding individual agencies, then each agency must be individually configured.

Understanding Global Codes

Unlike many of the other Provisioning items, LSM codes can be provisioned at a global level. All LSM codes provisioned at this level are propagated down to the agency level *only* if the codes are provisioned PRIOR to creating the agency. Any codes that are provisioned at the global level AFTER an agency has been created *are not* propagated to that agency. Therefore, these global codes will be unavailable for use by these agencies until they are provisioned directly against these agencies.

Provisioning LSM codes at the agency level does not impact codes at the global level. Provisioning LSM codes at the global level (either creating new codes or modifying existing ones) has no impact on the LSM codes that already exist at the agency level.

The LSM codes at the agency level are the ones that PremierOne uses. With the exception of City and State codes, the global level codes are only used to propagate the values down as described previously.

NOTE

Once global level codes are propagated to an agency, the agency can modify the code without affecting the global value. Editing the global value also does not affect the agency value.

As an example:

1. Provision global LSM codes.
2. Create agency PD.

   All existing global LSM codes are propagated to agency PD when it is created.
3. Provision additional global LSM codes.

   The newly provisioned global LSM codes are not propagated to agency PD and are therefore unavailable for use by the agency.

Configuring Standard Lists

The following standard lists are provided by Motorola. With the exception of Auto Club and Payment Method, these lists are used for submitting queries to NCIC and other databases. To configure these standard lists, you need to add the codes for the lists you are going to use. If you have a large number of codes, importing them can save time. For details on importing, see “Importing Configuration Items” on page 2-13.

- Auto Cub (used for contractors)
- City – Global only, not available at agency level; cities are automatically loaded from the GIS data.
- County List
- Eye Color
- Gender
- Hair Color
- Payment Method (used for contractors)
- Person Build
- Person Race
- Person Suffix
- Plate Type
- Skin Tone
- State – Global only, not available at agency level

- Vehicle Color
- Vehicle Make
- Vehicle Mode
- Vehicle Style
- Vehicle Type

To add codes to a list:

1. From the navigation panel, select **Lists and Statute Management**, and then select **LSM**.

   The LSM form appears with the General tab in focus. A list of standard codes display on the left side of the form. You do not need to enter any configuration information on this form; the required information has already been entered by Motorola.

NOTE
The Related Lists field and Parent and Child buttons are for future functionality.

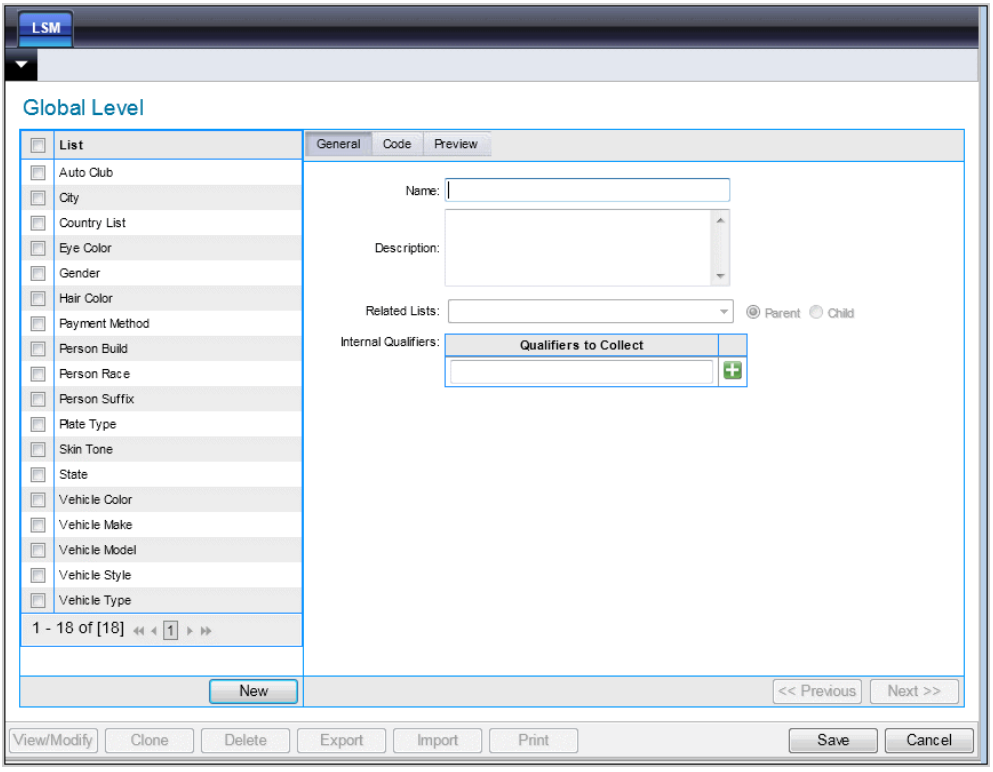


Figure 6-1 LSM – General Tab

2. Select the Code tab.

A list of any codes displays.

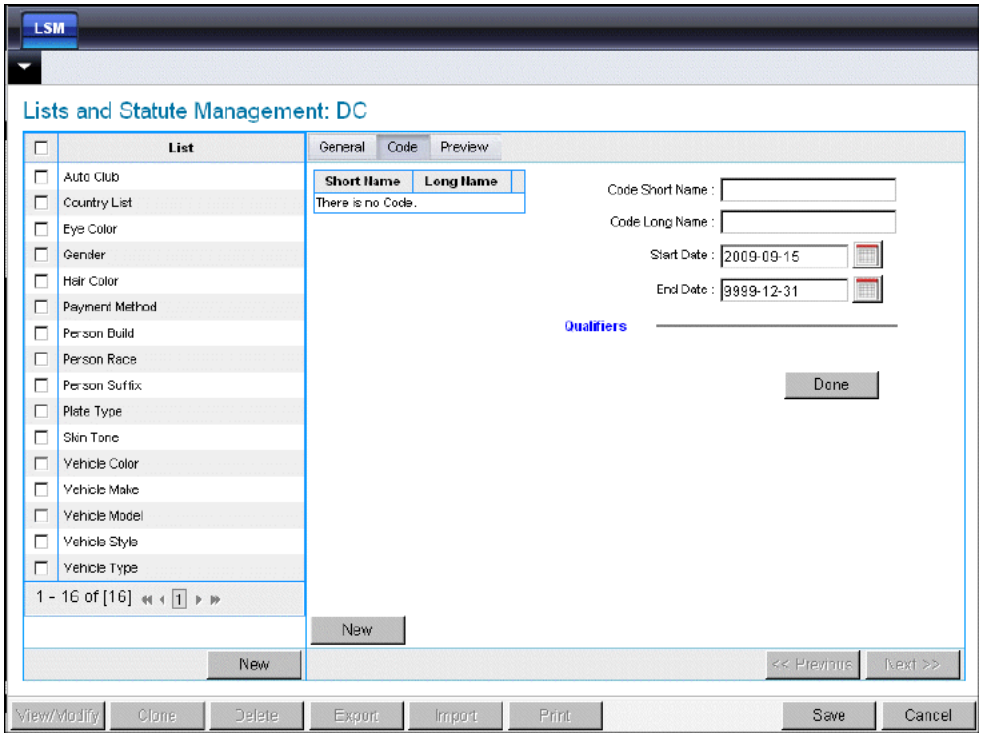


Figure 6-2 LSM – Code Tab

3. Select the list you want to add codes to and click **View/Modify**.
4. In the Code Short Name field, type a short name for your code.

   This is a required field. Short names are used in queries.
5. In the Code Long Name field, type a long name for your code.

   This is a required field. The value you type in the Code Long Name field appears in the code lists on the forms throughout PremierOne and on the Preview Page.

NOTE
City codes must match the cities in the GIS data.

6. Enter a Start and End date.

   The date fields are most commonly used for codes that might be expiring or new codes.

NOTE
The Qualifiers section is related to Qualifiers entered on the General tab. To use these, contact Motorola.

7. For Vehicle Make and Vehicle Model, do of the following:

   - For the Vehicle Make code, select the code you want to use from the All Codes list and add them to the Selected Parent Codes list.

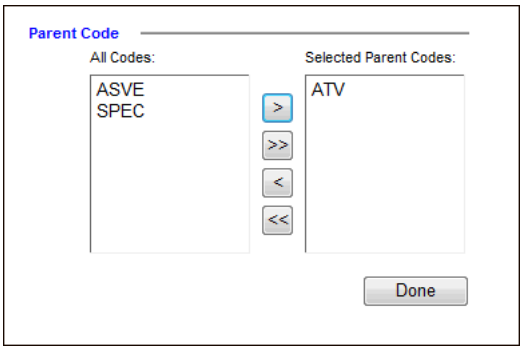


Figure 6-3 Parent Code

   - For the Vehicle Model code, select the codes you want to use from the All Codes list and add them to the Selected Child Codes list.

     For example, the BMW code might have child codes of 325XI, 330XI, 530XI, and so on to show all the possible models of BMW.

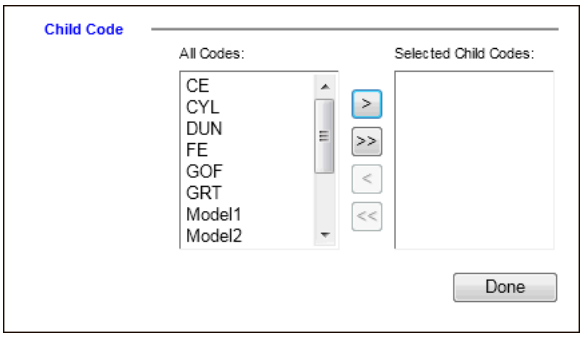


Figure 6-4 Child Code

8. Click **Done**.

> **CAUTION**
> If you do not click **Done**, the code is not saved, even if you click **Save**.

9. Continue adding codes.

10. Click **Save**.

    For details on viewing a list of the codes, see “Previewing Code Lists” on page 6-8.

Configuring New Lists and List Items

Use the LSM configuration item to create new lists of items with their descriptions, qualifiers, and codes. Any new list items are most commonly fields used in queries.

You cannot change the Code Name. If you want to change the Name, you must delete and re-add the record.

Adding Lists and Codes

When you add lists and codes, you enter information on two tabs of the LSM form and preview the new information on the third tab:

- General – Where you enter the name of the list and description for the list.
- Code – Where you create the code short and long names, select starting and ending dates, and select child and parent tables where applicable.
- Preview – Where you can view a preview of your list and list items in a tree view.

NOTE
Anything provisioned at the agency level will override the global setting. For details on global codes, see "Understanding Global Codes" on page 6-1.

Adding General List Information

General list information includes the list name, list description, and internal qualifiers.

To add general list information:

1. From the navigation panel, select **Lists and Statute Management**, and then select **LSM**.

   The LSM form appears with a list of existing codes on the left side of the form (see Figure 6-1).

2. At the bottom of the list of lists, click the **New** button.
3. Type a name and a description for the new list.
4. Click **Save**.

NOTE
The Related Lists field and Parent and Child buttons are for future functionality.

Adding Codes to Lists

Codes are the items that appear in a drop-down list, such as the types of vehicles in a Vehicle field, or vehicle colors in a Vehicle Color field.

To add codes to a list:

1. Access the form for a list. For instructions, see "Adding General List Information" on page 6-6.

   The LSM form appears with the General tab in focus (see Figure 6-1). A list of existing lists displays on the left side of the form.

2. Select the Code tab.

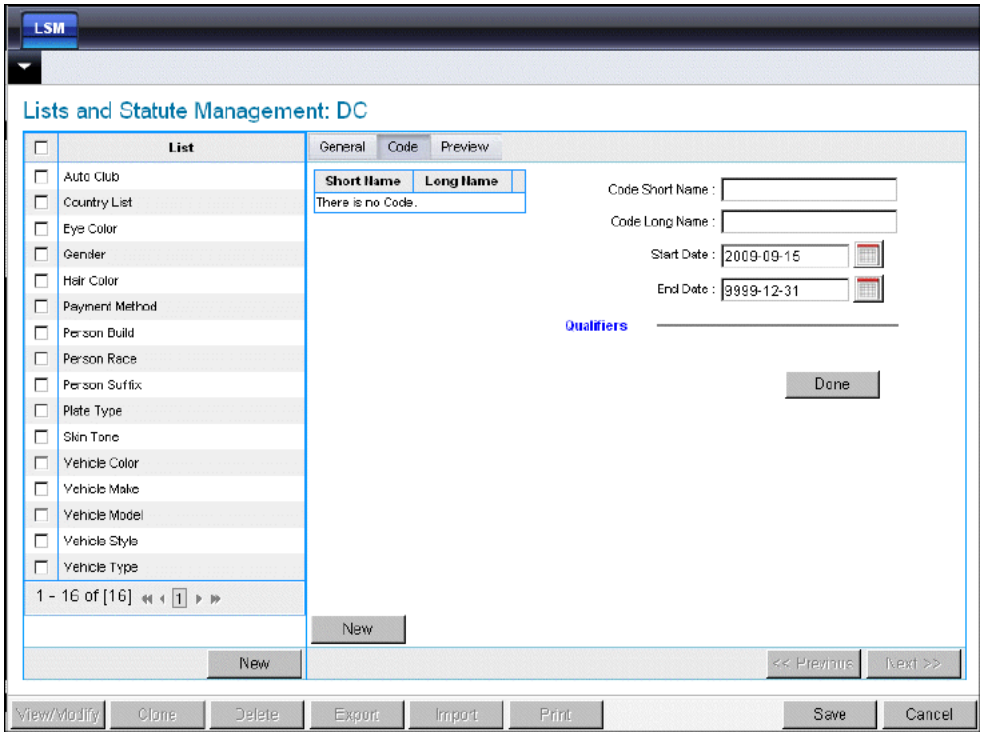


Figure 6-5 LSM – Code Tab

3. Select the code and click **View/Modify**.

4. In the Code Short Name field, type a short name for your code.

   This is a required field.

5. In the Code Long Name field, type a long name for your code.

   This is a required field. The value you type in the Code Long Name field appears in the code lists on the forms throughout PremierOne.

6. Enter a start and end date.

The date fields are most commonly used for codes that might be expiring or for new codes.

NOTE
To use Qualifiers, contact Motorola.

7. Click **Done**.

   The code is added to the list of codes.

CAUTION
If you do not click **Done**, the code is not saved, even if you click **Save**.

8. Click **Save**.

Previewing Code Lists

Use the Preview tab to view the existing codes for a list.

To preview a code list:

1. Access the form for a list. For instructions, see "Adding Lists and Codes" on page 6-6.

   The LSM form appears with the General tab in focus (see Figure 6-1). Existing lists display on the left side of the form.

2. Select the code.

3. Select the Preview tab.

A list of all the defined codes displays.

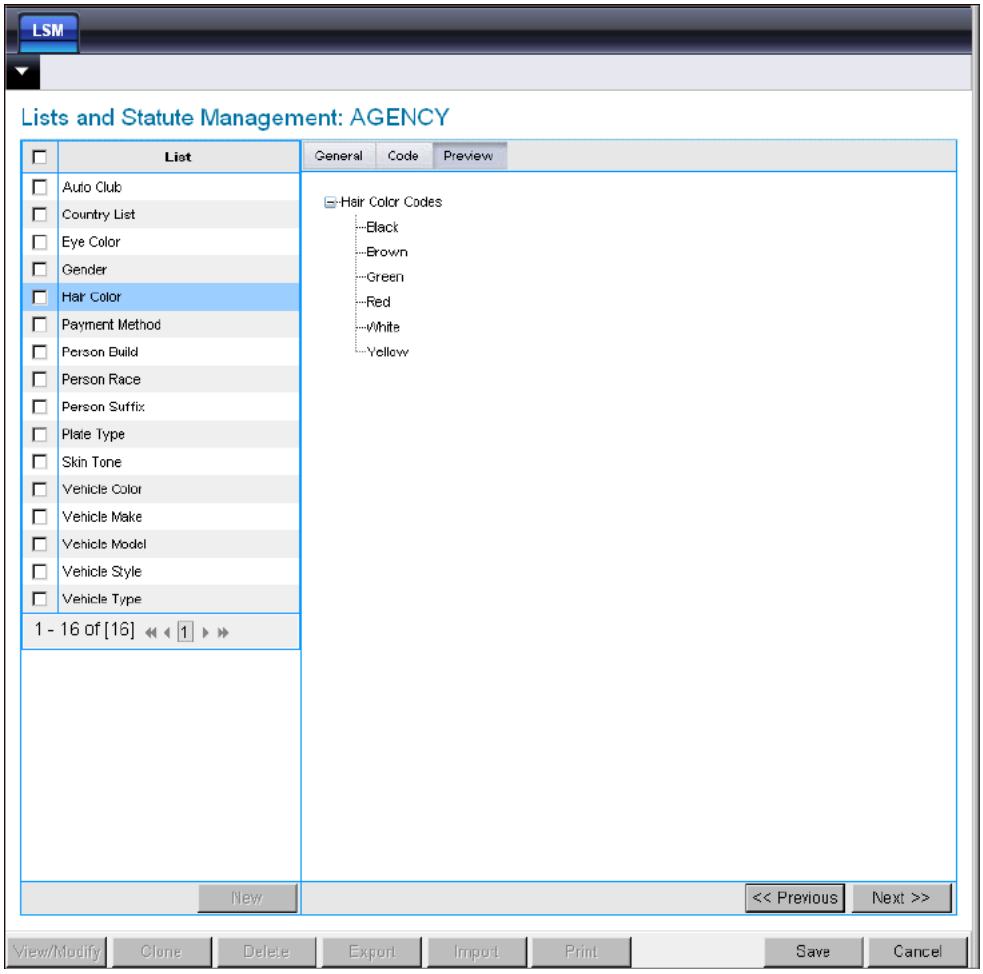


Figure 6-6 LSM – Preview Tab

Configuring Active Directory for Authentication

Use LSM to provision Active Directory (AD) to store the user accounts and password that a CAD or Mobile user would use for authentication. Use this method when you are already using AD to control your user accounts. Using this method, a link is established between PremierOne and your AD and all user account maintenance is done in AD.

AD authentication is configured for each user under Resources – Personnel. For details, see “Configuring Personnel” on page 11-7.

Prerequisites

Before using AD for authentication, the following prerequisites must be met:

- Obtain the necessary information regarding the external active directory: external domain name, domain alias, domain controller IP address, and secondary domain controller IP address.
- Enable external AD access for the PremierOne application servers on which the security token service is hosted. By default, the LDAP service on the external AD controller licenses the port 389. Ensure port 389 is not blocked by the firewalls between the PremierOne application server network and the external AD network.
- Obtain a list of user accounts for the external AD. These user accounts are associated with the PremierOne user. From your perspective as the PremierOne system administrator, the password of the AD user account is *not* necessary, because you only link the PremierOne user with the external AD user. The end user needs to provide the correct password of the AD user account during the sign on process to the PremierOne system.

Example Active Directory Information

External domain name (Code Short Name)	R2-HA
External domain alias (Code Long Name)	R2-HA-Alias
Full name of external domain (FQDN)	R2-HA.org
Primary controller IP address (PrimaryDC)	192.168.28.205
Secondary controller IP address (SecondaryDC)	192.168.28.207
Example user account	test07
Password of example user account	1234ABcd

Configuring AD Authentication

To configure AD authentication, use the LSM General and Code tabs, and the Resources Personnel form.

To configure AD authentication:

1. From the navigation panel, select **Lists and Statute Management**, and then select **LSM**.
2. Select **Add New** and **Global Level** from the filter, and then click **OK**.

The LSM form appears with a list of existing lists on the left side of the form.

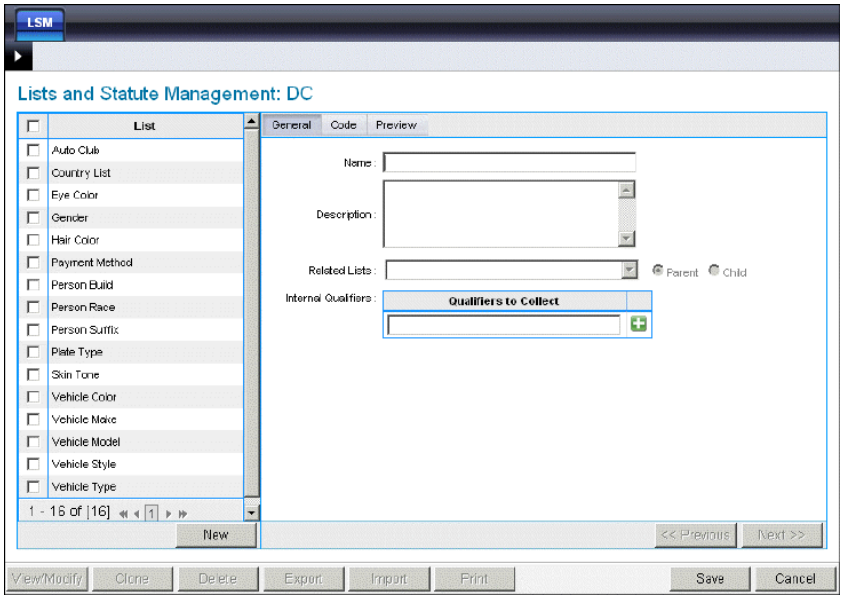


Figure 6-7 LSM – General Tab

3. At the bottom of the list of lists, click the **New** button.
4. In the Name field, type `ActiveDirectoryDomains`.
5. In the Description field, type a description (optional).
6. Add the following qualifiers in the Internal Qualifiers field, clicking the plus symbol after each addition, including the last addition:
   - FQDN
   - NetBiosAlias
   - PrimaryDC
   - SecondaryDC
7. Click **Save**.

8. On the Code tab, click **View Modify**.

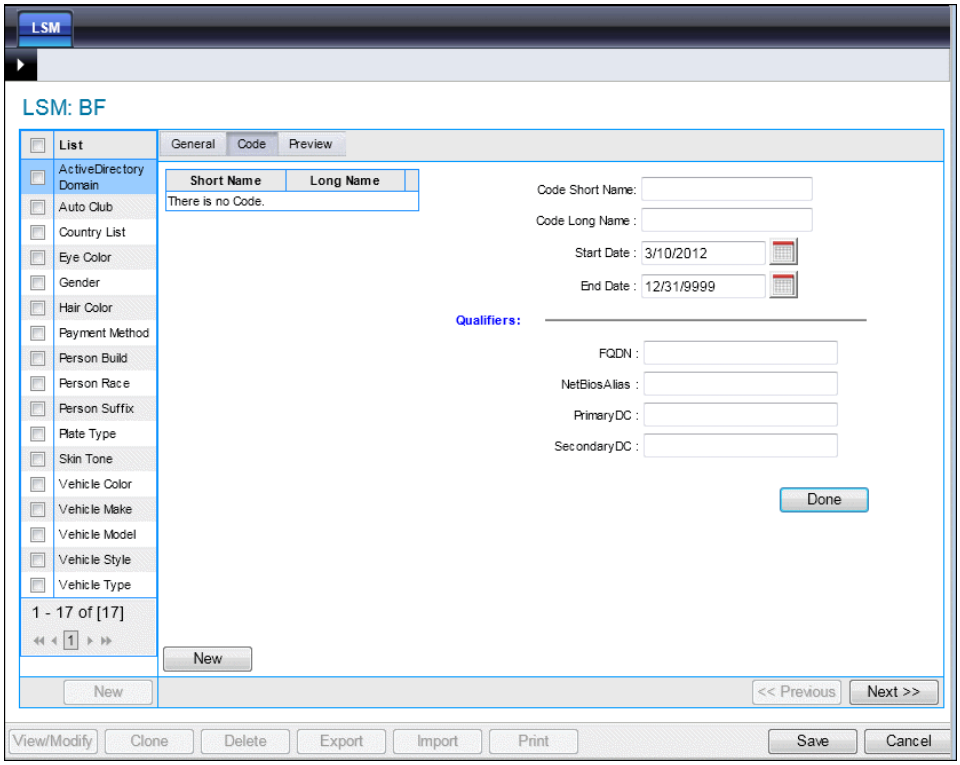


Figure 6-8 LSM – Code Tab

9. Refer to your prerequisites for the following information:

   a. In the Code Short Name field, type `External Domain Name`.

   b. In the Code Long Name field, type `External Domain Name`.

   c. In the FQDN field, type the full name of your external domain, for example `R2-HA.org`.

   d. In the NetBiosAlias field, type the external domain alias.

   e. In the PrimaryDC field, type the primary controller IP address.

   f. In the SecondaryDC field, type the secondary controller IP address.

10. Click **Done**.

    The Short Name and Long Name appear in the list at the left of the form in blue to indicate that they are not yet saved.

11. Click **Save**.

12. From the navigation panel, select **Resources**, and then select **Personnel**.

The Personnel form appears.

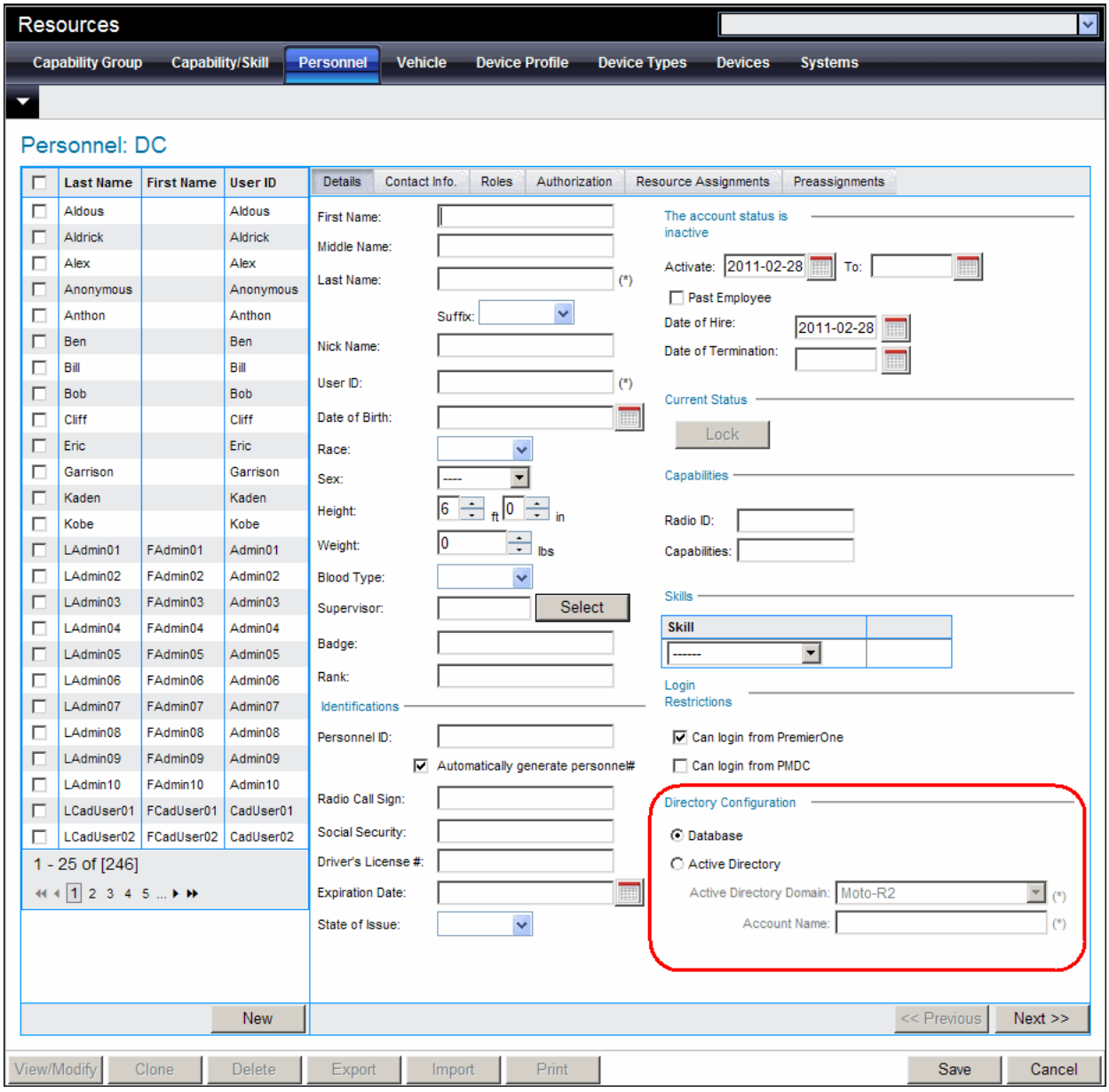


Figure 6-9 Resources – Personnel

13. Create a user using the same information as you did when provisioning LSM. For example, if the User ID there was `test07`, use the same User ID here.

    a. In the Directory Configuration section, select **Active Directory**.

    b. Select the same Active Directory Domain that you entered in LSM, for example, Moto-R2.

    c. You can, but are not required to select the same Account Name that you used in LSM, for example, test07.

CHAPTER 7

Configuring Plans

The Plan Management configuration item contains the following items:

- Plans – Where you manage plans, the highest level geographical grouping for an agency. For details, see "Configuring Plans" on page 7-2.
- Active Plan – Where you set or view the active plan. For details, see "Setting the Active Plan" on page 7-5.

Overview of Plans

Plans contain the following elements:

- Beat – smallest geographical area
- Sector – collection of beats
- Area – collection of sectors (also known as teams/districts)
- Pseudo area – area used to contain units not assigned to a specific area

A plan allows dispatchers to sign on to and monitor different areas; one dispatcher can monitor the north area of town while another can monitor the south area, allowing agencies to split workloads. Plans are also used to assist in recommendations.

Some agencies may define multiple plans to use during different time periods and activity levels. A normal plan can be established to be in effect during the times when normal activity levels are expected. Additional plans can be established to accommodate changes in the normal activity level, such as weekends, holidays, special functions, and night shifts.

Each agency must have two plans, an active one and an inactive one. You can only make changes to the inactive plan. Make sure the two plans match each other.

Configuring Plans

The Plan Management configuration item is where you can view the details for the currently active plan and choose to automatically remove users or units from the geographic messaging groups that are associated with a plan at log on or log off.

You can add, modify, clone, delete, import, and export plans. For details on modifying, cloning, deleting, importing, and exporting plans, see “Working With Configuration Items” on page 2-9. You cannot change the Plan ID. If you want to change the ID, you must delete and re-add the record.

Adding Plans

You can add a plan from the Plans form or by cloning an existing plan. For details on cloning, see “Working With Configuration Items” on page 2-9.

To add a plan:

1. From the navigation panel, select **Plan Management**, and then select **Plan**.

   The Plans form appears.

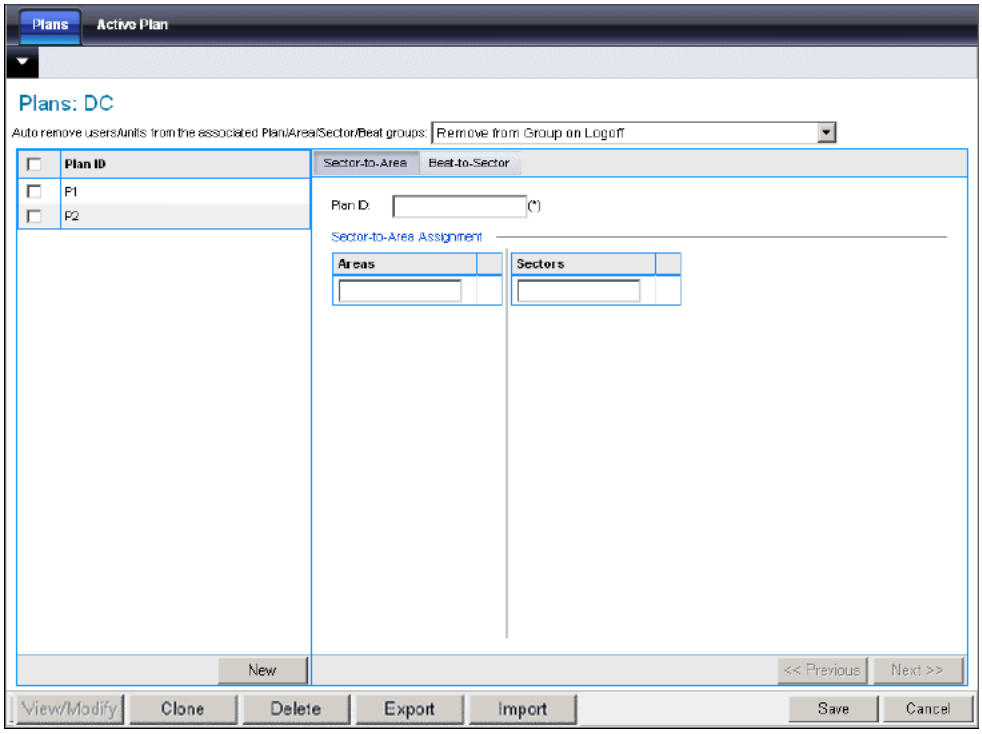


Figure 7-1 Plans Form

2. At the bottom of the Plan ID list, click the **New** button.

3. From the Auto remove users/units from the associated Plan/Area/Sector/Beat groups list, select one of the following:

   - To remove a user or unit from the geographic group (plan/area/sector/beat) they are covering when they log off, select Remove from Group on Logoff.

     CAD can use message groups, where messages are sent to all the users within a geographic group, such as an area or a beat. This option removes the user from the messaging group when they log off.

   - For the user to continue to receive messages sent to a geographic group even after the user signs off from covering that area, select Remove from Group on Logon at different Geographic hierarchies.

     With this option, the user isn't removed from the group unit the user logs back on again.

     For details on groups, see "Configuring Groups" on page 18-12.

4. In the Plan ID field, type the name of the new plan.

5. In the Areas field and type the first area you want as part of your plan.

   You can provision a pseudo area by specifying only an agency and an area without specifying a sector.

   Pseudo areas are used to contain units that are not assigned to a specific area. CAD automatically assigns units to this area when the activation of a plan caused the unit's area to be inactive, such as when an area is disabled.

6. Press the **Tab** key once to move the cursor to the first Sector field.

7. Enter the sector associated with that area.

   If more than one sector will be associated with that area, press **Tab** after entering the first sector; otherwise skip to the next step. This opens a new Sector field. Type the next sector, and repeat as needed.

8. Once all sectors for that area are entered, use the mouse to select the next (blank) Area field.

   The Sector field will revert to a single, blank field. The sectors you entered are still associated with the area.

9. Enter the area name, and then press **Tab** to enter the sector associated to that area.

   If more than one sector is associated to that area, press Tab from the Sector field to open a new sector field.

10. After all areas and their associated sectors are entered, save the plan.

11. Select the Beat-to-Sector tab, and click **View/Modify**.

12. For each beat displayed, click in the Sector field and select the sector containing that beat.

    The associated area will be automatically populate. Repeat this for every beat. The same sector can be assigned to multiple beats.

    The beats shown are derived from your geofile.

    When you select a sector, PremierOne automatically selects the associated area based on what you selected in the first part of this procedure. Alternatively, you can select the area and then select the sector.

    You can save at any time. However, PremierOne saves the plan as “partial” until you assign all of the sectors.

    Each unsaved plan appears in the Plan ID list in blue text.

    NOTE
    The Beat ID must be blank for pseudoareas.

13. Click **Save**.

    The plans you added appear in the Plan ID list in black text.

Modifying a Plan

You can modify a plan from the Plans form. You cannot modify an active plan.

To modify a plan:

1. From the navigation panel, select **Plan Management**, and then select **Plan**.

   The Plans form appears (Figure 7-1).

2. Select the plan you want to modify and then click **View/Modify**.

3. Make any changes necessary.

4. Click **Save**.

Setting the Active Plan

Set the active plan when you need to change the plan that is currently in effect.

To set the active plan:

1. From the navigation panel, select **Plan Management**, and then select **Active Plans**.

   The Plans form appears.

2. Click **Active Plan**.

   The Active Plans form appears.

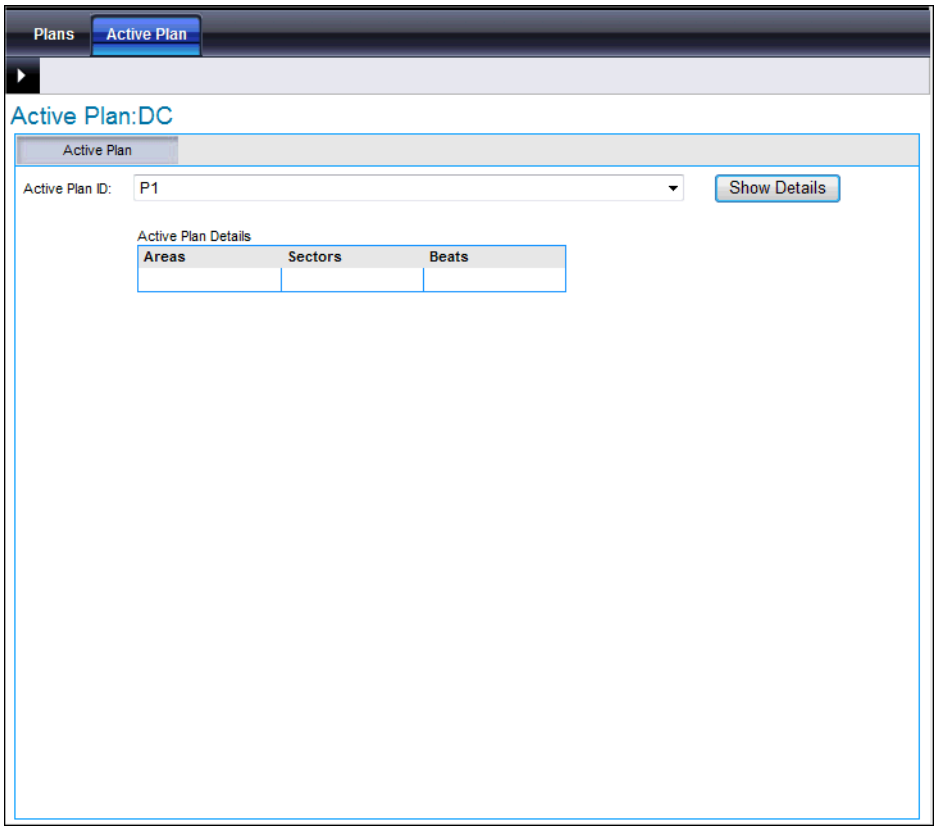


Figure 7-2 Active Plans Form

3. Click **View/Modify**.

4. From the Active Plan ID list, select the plan ID you want to use.

   To view the details of the plan, select the **Show Details** button.

5. Click **Save**.

Viewing the Current Plan

You can view the details for the currently active plan.

To view the current plan:

From the navigation panel, select **Plan Management**, and then select **Active Plan**.

The form for the active plan appears (see Figure 7-2).

CHAPTER 8

Configuring Role Permissions

The Role Permission configuration item contains the following item:

Roles – Where you configure groups of users who perform similar tasks, such as dispatchers, call takers, and supervisors. Role settings include the following:

- General settings, such as the role name, start and expiration dates for the roles, whether concurrent logins are allowed, session lockout times, whether the role can access CAD and/or MDTs, and whether priority comments and update notifications display. For details, see “Adding Role General Information” on page 8-2.
- The services the role can access, such as commands and provisioning. For details, see “Adding Role Permissions” on page 8-5.
- A display of the role permissions. For details, see “Viewing a Role Preview” on page 8-13.
- The resources that belong to the role. For details, see “Adding Resources to Roles” on page 8-13.
- The roles that can access reporting. For details, see “Adding Reporting Permissions” on page 8-16.

By default, Provisioning creates two roles for an agency, the Agency Admin role, and the Default role; these are reserved names. Additionally, when a personnel record is created, the agency Default role is automatically assigned to the record.

- The Agency Admin role has access to all features and cannot be modified.

  This role is only available at the admin level, where the agency is the Admin agency. The Agency Admin role cannot assign the Agency Admin role to another user. The Agency Admin role is prevented from accessing the Agency Admin and Default roles within the Role Permission – Roles page and the Resources – Personnel – Roles pages.

- The Default role has no permissions but can be modified.

  All personnel are assigned to the Default role and the Default role cannot be removed. The Default role is used internally to log onto PremierOne from general purpose consoles (where no role selection is available), or from interfaces. During logon, the Default role cannot be selected within the CAD and Mobile clients or the Provisioning application.

Configuring Roles

The Role Permission configuration item is where you set the details for each of the roles in your agency. You set the general description information for the role, such as name, when the role becomes effective or expires, and session timeouts; which services and features the role has permissions for; and the groups or individual users assigned to the role.

You can add, export, modify, import, and delete roles. For details on modifying, exporting, importing, and deleting roles, see "Working With Configuration Items" on page 2-9.

Adding Roles

When you add a role, you enter information on three tabs of the Roles form and preview your information on a fourth tab.

- General – Where you give the role a name, start and expiration time, log in settings, description, inactivity settings, and timeout settings.
- Permissions – Where you identify which PremierOne services the new role is allowed to access, the features of each of those services, and the specific instances of address books, dynamic groups, query types, and printers allowed for each role.
- Preview – Where you preview the settings for each role.
- Resources – Where you define the groups to which the new role has access.
- Reporting – Where you define the reports to which the new role has access.

Adding Role General Information

Role general information includes the role name and description, start and expiration time and date, concurrent login settings, sign off restrictions, lockout settings, timeout setting, and whether priority comment notifications and priority updates are enabled for role members.

When agency is added, the role `Default Role` is assigned to all users; the role does not have any permissions and you cannot add permissions to the role (the permission set is view-only).

To add role general information:

1. From the navigation panel, select **Role Permission**, and then select **Roles**.

   The Roles form appears. A list of existing records displays on the left side of the form.

If you selected Existing in the filter, then a list of existing records displays. If you entered search criteria in the filter, only the matching records display.

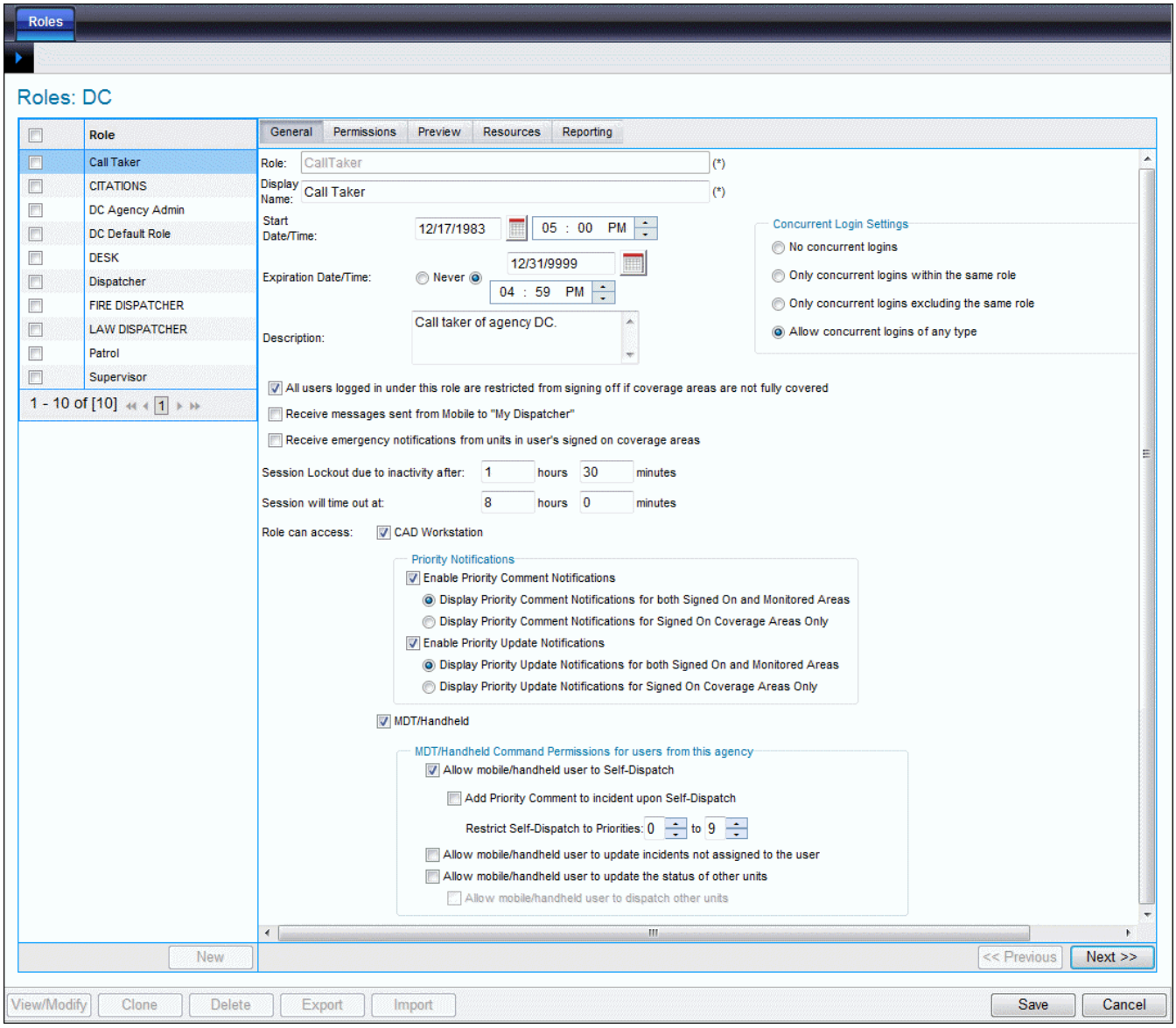


Figure 8-1 Roles Form – General Tab

2. Access the form for a role. For instructions, see "Adding Roles" on page 8-2.

   The Roles form appears with the General tab in focus (see Figure 8-1). A list of existing roles displays on the left side of the tab.

3. At the bottom of the Role list, click the **New** button.

4. In the Role field, type the name of your new role.

5. In the Display Name field, type the name of the new role.

6. Enter a start date and time for this role to take effect.

This is not the work shift for the role, but the date and time you want the role to actually go into effect.

7. Select whether and when you want this role to expire.

8. In the Description field, type a description for the role.

9. In the Concurrent Login Settings section, select how you want to handle concurrent logins.

   Concurrent logins allow users to log in to more than one device at a time. Concurrent logins can also be set for the agency in the Authentication–Agency Setting configuration item and an individual user in the Resources–Personnel configuration item. For details, "Adding Personnel Authorization Information" on page 11-14 and "Adding Personnel Authorization Information" on page 11-14.

10. Select whether users logged in under this role are restricted from signing off if their coverage areas are not fully covered (this includes the Default Area).

11. Select whether you want this dispatcher to receive messages from Mobile/Handheld users when they send a message to "My Dispatcher."

12. Set the lockout due to inactivity time.

    For a lockout period of none, enter the value 0.

13. Set the timeout time.

14. Select whether the role is for the CAD workstation or Mobile/Handheld.

15. For CAD workstation users, select any of the following:

    - To display a priority notification dialog box when priority comments are entered by another user, select the **Display Priority Comment Notifications** check box.

      Priority comments draw the attention of users to an incident when there is urgent information. Users enter priority comments in angle brackets. Priority comments are always enabled and the format of priority comments is not configurable.

    - To display a priority notification dialog box when priority fields are updated, select the **Display priority update notification** check box.

      For instructions on enabling priority updates and selecting the priority fields, see "Configuring Priority Updates" on page 13-28.

    To configure status monitors so that an icon or text displays indicating priority comments or updates exist that have not been viewed, see "Adding Status Monitor Displays" on page 32-26 (configure the Priority Notification icon).

16. To allow dispatch permissions for Mobile/Handheld users so that users with this role can dispatch for themselves, do the following:

    a. Select the **Mobile/Handheld** check box.

b. Select the **Allow Mobile/Handheld users to Self-Dispatch** check box.

c. From the Restrict Self-Dispatch to Priorities boxes, select the valid dispatch priorities for which mobile users can dispatch incidents to themselves.

Being able to select valid dispatch priorities allows an agency to restrict units in different roles to performing self-dispatch transactions only on specific priorities, such as high priority incidents only.

d. If you want add a priority comment added to the incident when the mobile user self-dispatches, select the **Add Priority Comment to incident upon self-dispatch** check box.

e. To allow the mobile user in this role to update incidents or the status of other units, select any of the following:

- **Allow mobile/mobile handheld user to update incidents not assigned to the user**
- **Allow mobile/mobile handheld user to update the status of other units**
- **Allow mobile/mobile handheld users user to dispatch other units;** for this option to be enabled, you must also select **Allow mobile/handheld user to update the status of other units**

Self-dispatch permissions must also be provisioned for the mobile user for the ID and US commands. For details, see "Adding Role Permissions for Mobile Users" on page 8-11.

17. Click **Save**.

Adding Role Permissions

Role permissions include the services the role is allowed to access, the features of each of those services, and the specific instances of address books, dynamic groups, query types, and printers allowed for each role. Examples of services include messaging, chat, query, and Provisioning.

NOTE
If you also configure permissions for the workstation, the most restrictive permissions will apply.

To add role permissions:

1. Access the form for a role. For instructions, see "Adding Roles" on page 8-2.

   The Roles form appears with the General tab in focus (see Figure 8-1). A list of existing roles displays on the left side of the tab.

2. Select the role for which you want to set permissions.

3. In the Roles window, select the Permissions tab.

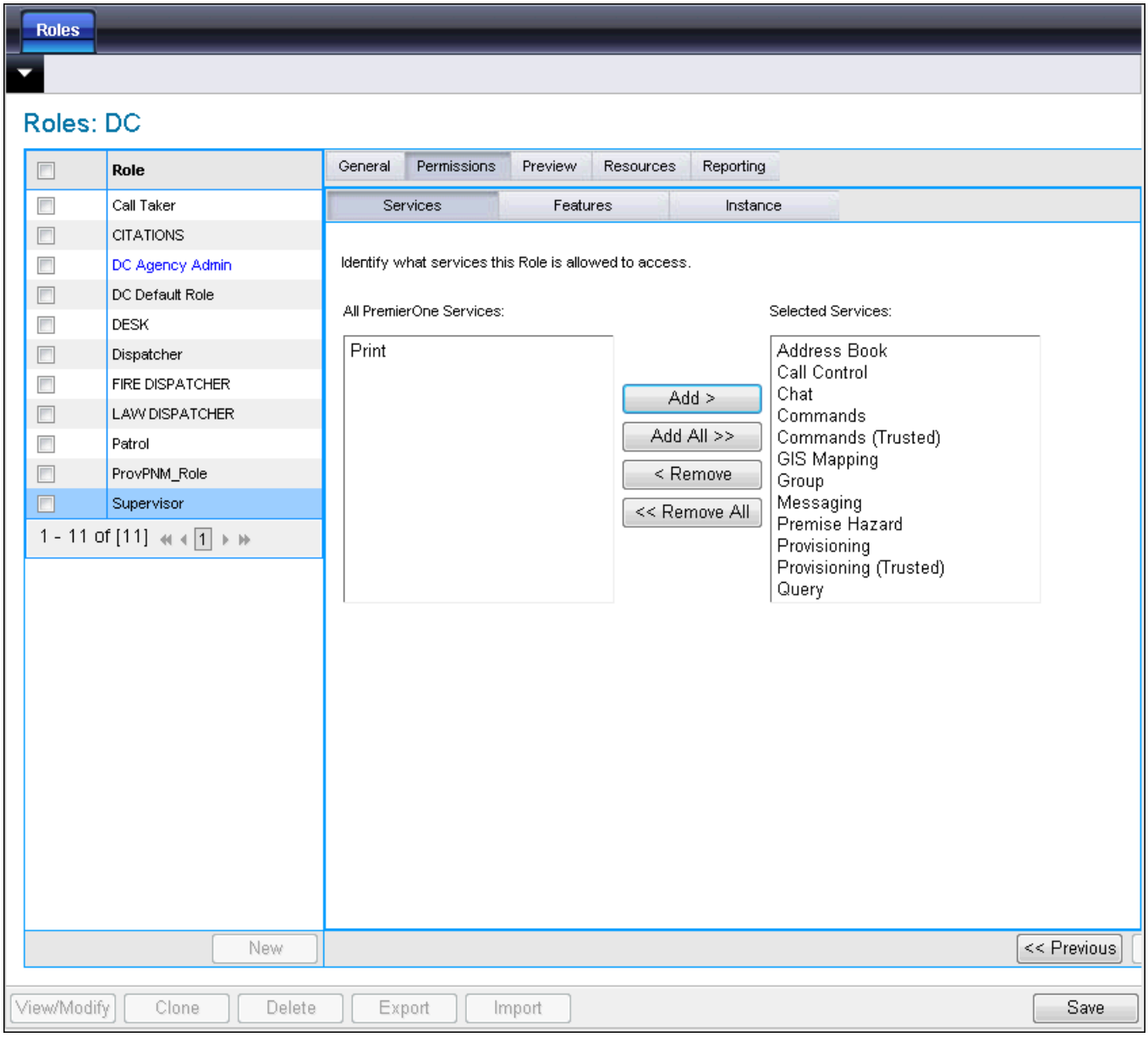


Figure 8-2 Roles Form – Permissions Tab, Services Subtab

4. On the Services subtab, select the services this role will be allowed to access in the All PremierOne Services box and click **Add**.

   For details on Commands (Trusted) and Provisioning (Trusted), see "Setting CAD Command Access for Trusted Agencies" on page 5-6 and "Setting Provisioning Access for Trusted Agencies" on page 5-7.

5. Click the Features tab to configure the permissions for the services.

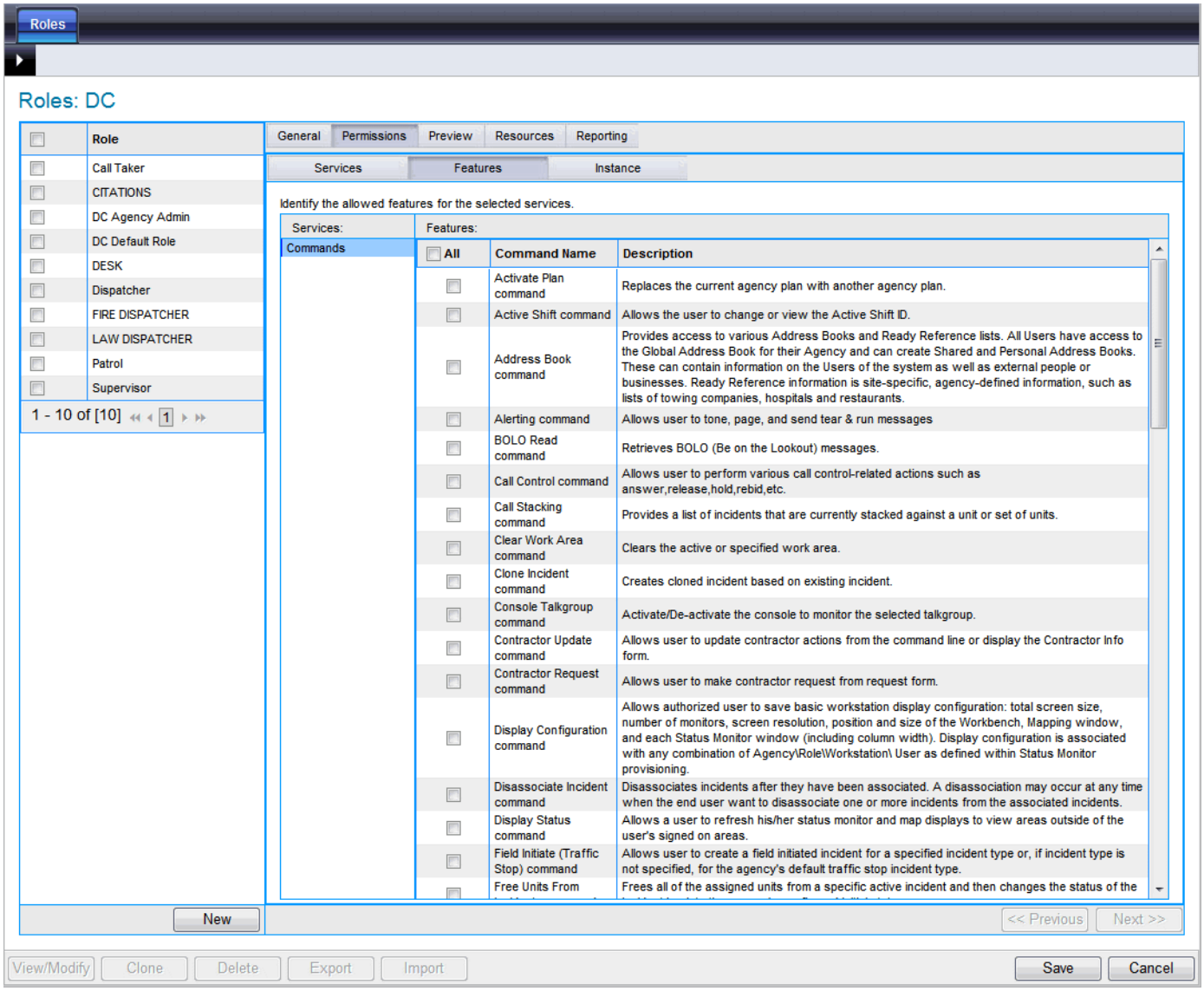


Figure 8-3 Roles Form – Permissions Tab, Features Subtab

6. On the Features subtab, select the service from the Services list.

   A list of features associated with the service display.

> **NOTE**
> As of version 3.3, Workload Transfer is now located under the Sign On Coverage feature.

7. In the Features list, select the features to which you want to grant permission for the role.

   Most of the features are self-explanatory. Following are features that may need more explanation.

- Call Control: Listen & Join – This feature is a supervisory function that allows the supervisor to listen to other positions without the call taker knowing that the call taker is being monitored. The supervisor can join a call to speak/be heard by selecting Join in the Positions list.
- Call Control – Manual ALI query– This feature allows the user to type in a phone number and receive the ALI information without the need to be active on a call with that number.
- View SMS/TDD Transcripts – This feature allows the MDT user to view transcripts for SMS (text) and TDD calls.

8. Repeat for each of the services.

NOTE

When Commands (Trusted) or Provisioning (Trusted) is selected from the Services list, a set of index links appears at the top of the screen, allowing you to filter the view by trusted agency. You can view All agencies, numeric agencies only (0-9), all alphabetic agencies (A-L), or only the agencies that begin with a specified letter (A, B, C, and so on).

For details on configuring Trusted agency settings, see “Configuring Trusted Agencies” on page 5-3.

9. Click the Instance tab to configure access to address books, dynamic groups, query types, and printers for the role.

   The Instance tab contains four subtabs for these items.

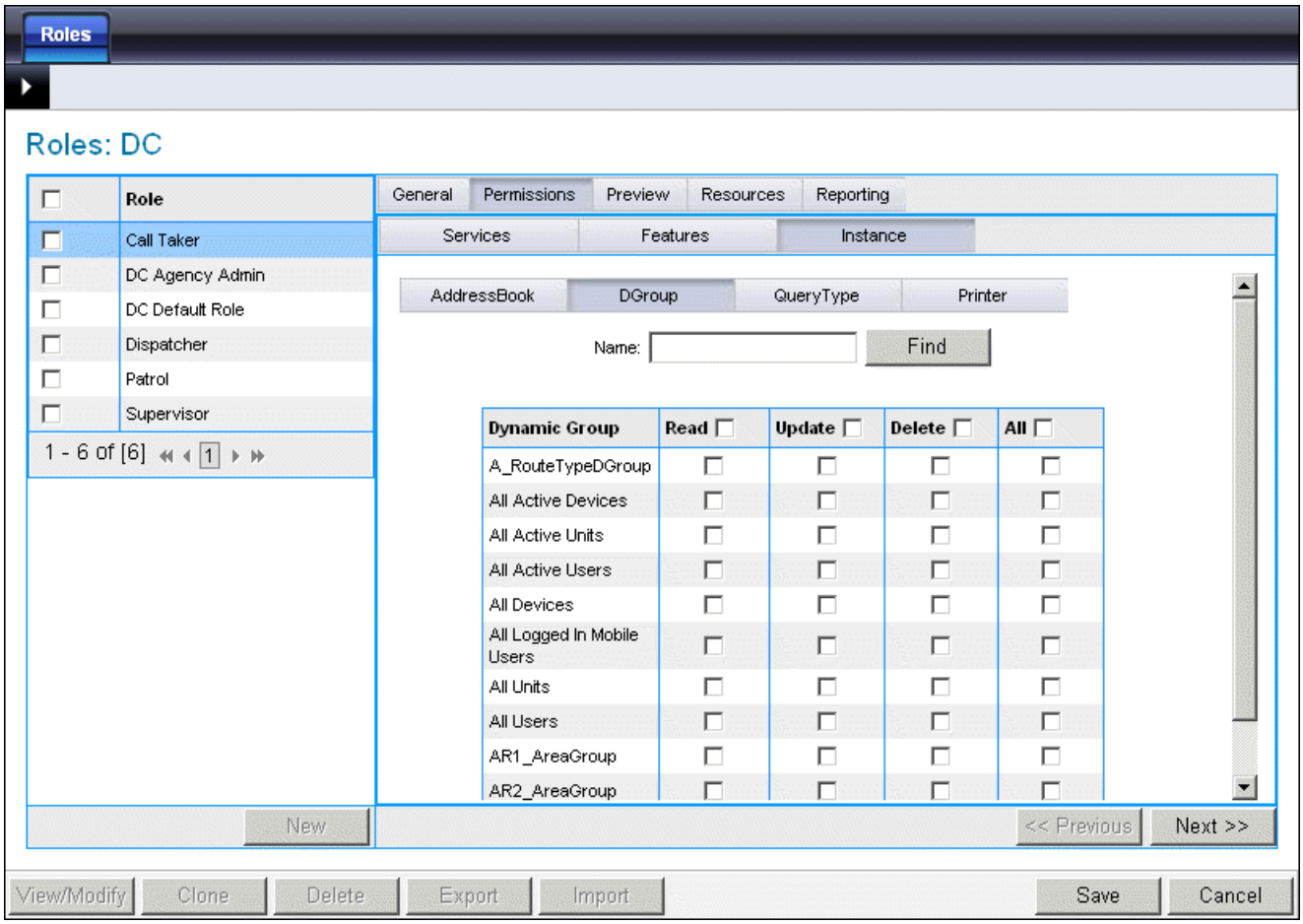


Figure 8-4 Roles Form – Permissions Tab, Instance Subtab, DGroup

   a. On the Address Book tab, select the check box to indicate whether this role has read, update, delete, or all rights to each address book.

      The AddressBook tab lists all the system-generated and shared address books. To find a specific address book, type the name of the book in the Name field and click **Find**. The address book appears in the table.

   b. On the DGroup tab, select whether this role has read, update, delete, or all rights to each dynamic group listed. Dynamic groups are groups that do not have static members, such as all users currently logged on to Area 1.

      To find a specific group, type the name of the group in the Name field, and click **Find**. The group appears in the table.

   c. On the Query Type tab, select whether this role has access to each query type. Query types can exist for many entities, such as queries for businesses, events, guns, persons, and vehicles.

To find a specific query type, type the name of the query type in the Name field, and click **Find**. The query type appears in the table.

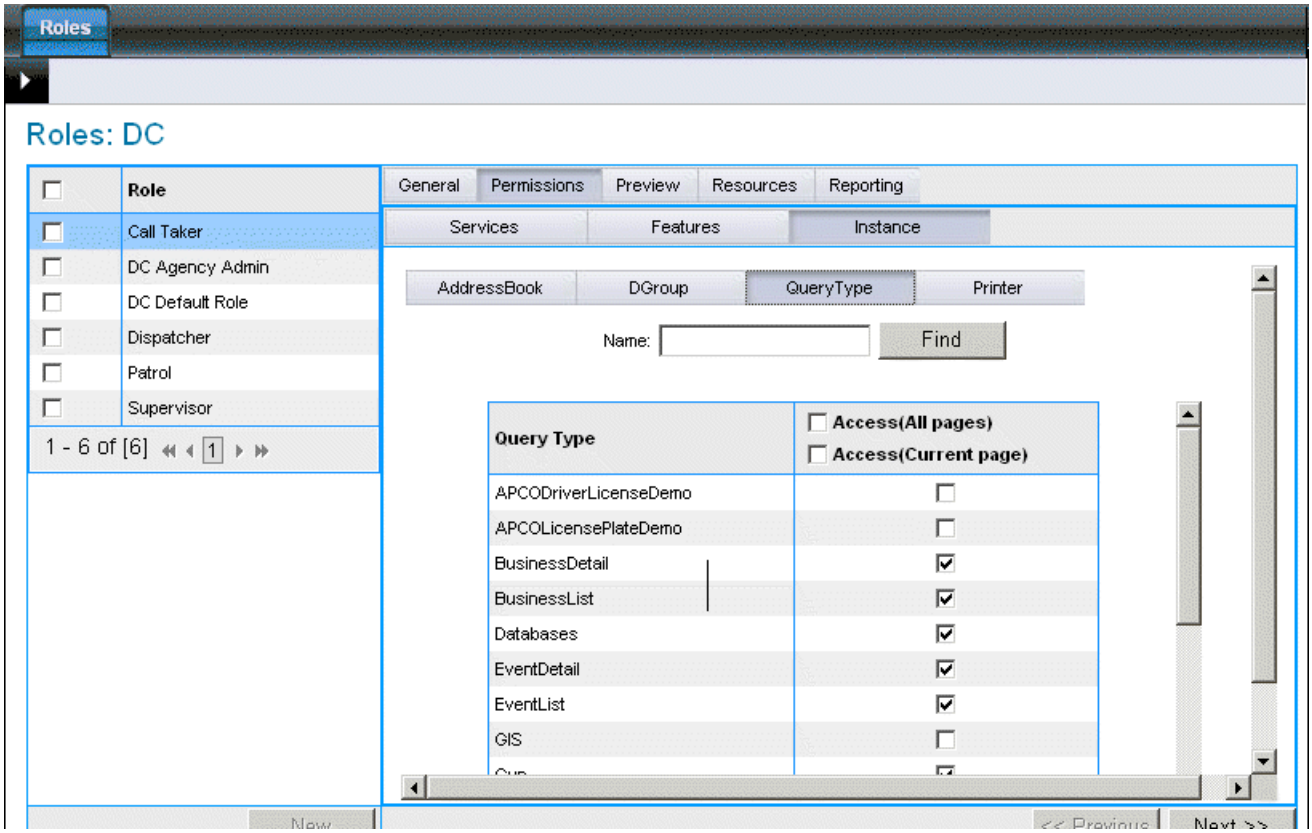


Figure 8-5 Roles Form – Permissions Tab, Instance Subtab, Query Type

d. On the Printer tab, select whether this role has access to each printer. To find a specific printer, type the name of the printer in the Name field, and click **Find**.

The printer appears in the table.

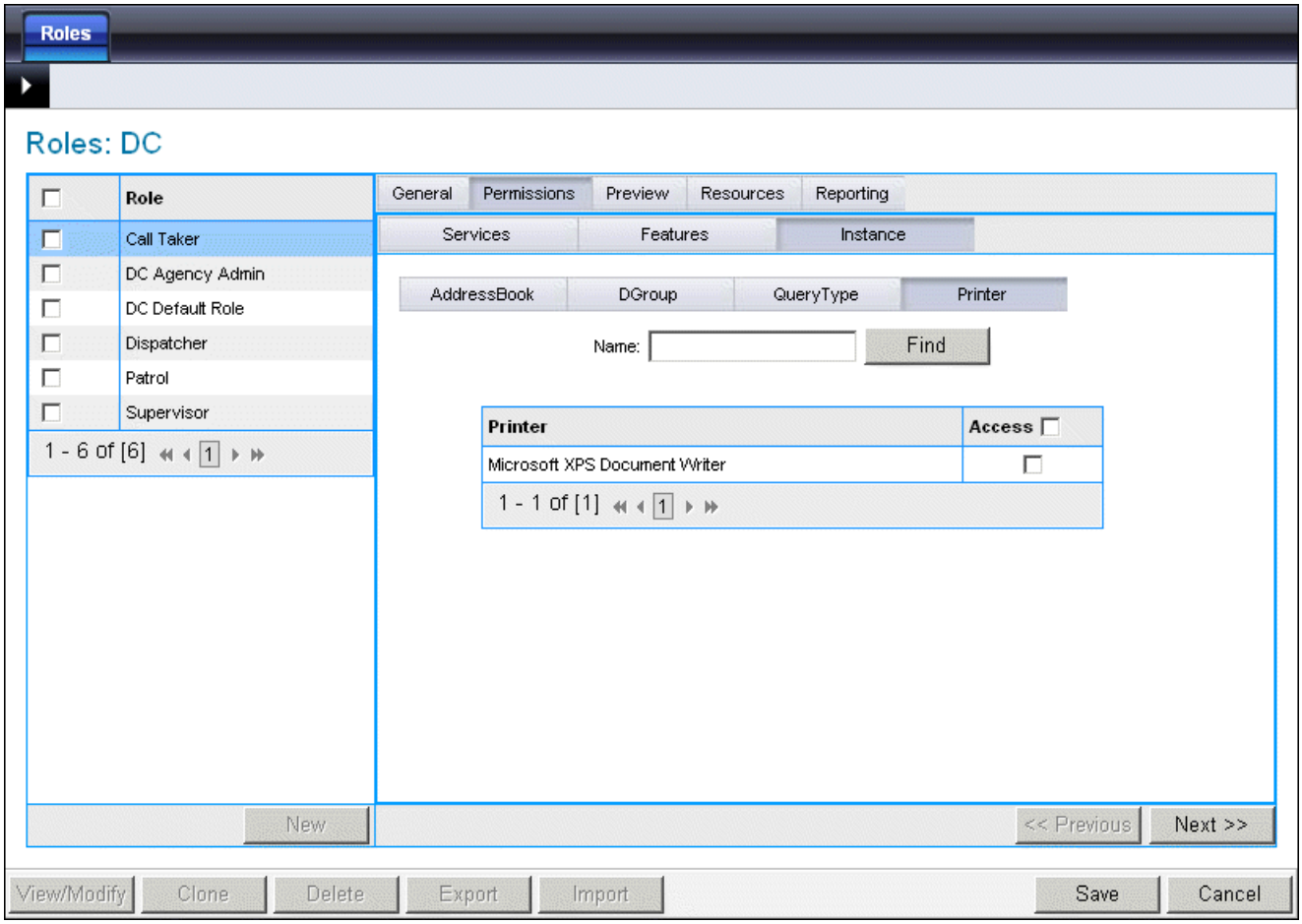


Figure 8-6 Roles Form – Permissions Tab, Instance Subtab, Printer

Adding Role Permissions for Mobile Users

Mobile users must be explicitly granted permissions to the II, FI, IU, ID, and US commands to create and update incidents, and to dispatch units to incidents. This includes self dispatch. Additionally, agencies can grant permissions to other agencies, called Trusted agencies, so that mobile users can use these commands in their agencies. For details on assigning trusted agency permission, see “Configuring Trusted Agencies” on page 5-3.

NOTE

You need to set up permissions for your own agency before granting permissions to another agency.

The following table summarizes the permissions that must be set for Incident Initiation and Incident Update:

Table 8-1 Permissions Required For Mobile Users – Incident Initiation and Incident Update

To	Permission Required	Location Roles – Permissions – Features
Create an incident for the user's agency using the II command:	Permission must be granted for the mobile user's role by the mobile user's agency for the Incident Initiation command.	Commands – Incident Initiation command
Create an incident for *other* agencies using the II command:	Trusted agency permission must be granted to the mobile user's role for the Incident Initiation command by the agency that the mobile user is attempting to create an incident for.	Commands (Trusted) – Incident Initiation command
Create a field-initiated incident/ traffic stop for the user's agency:	Permission must be granted for the mobile user's role by the mobile user's agency for the Field Initiate (Traffic Stop) command.	Commands – Field Initiate (Traffic Stop) command
The Trusted agency permissions for the II command are followed when the mobile user attempts to create a Traffic Stop incident for an agency *other* than the user's agency (based on the Foreign Unit settings provisioned for the user's agency).		
Update incidents for the user's agency using the IU command:	Permission must be granted for the mobile user's role by the mobile user's agency for the Incident Update command.	Commands – Incident Update command
Update incidents with the IU command for *other* agencies:	Trusted agency permission must be granted to the mobile user's role for the IU command by the agency that the mobile user is attempting to create an incident for.	Commands (Trusted) – Incident Update command

The following table summarizes the permissions that must be set for Incident Dispatch and Unit Status.

Table 8-2 Permissions Required For Mobile Users – Incident Dispatch and Unit Status

To	Permission Required	Location Roles – Permissions – Features
Dispatch units onto the incident (considers the incident and checks permissions for dispatching to the incident ID):	Permission must be granted for the mobile user's role by the mobile user's agency for the Incident Dispatch command.	Commands – Incident Dispatch command
Dispatch units onto the incident for *other* agencies (considers the incident and checks the permissions for dispatching to the incident ID):	Trusted agency permission must be granted to the mobile user's role for Incident Dispatch commands by the agency for which the mobile user is attempting to dispatch units.	Commands (Trusted) – Incident Dispatch command
Dispatch units onto the incidents (considers the units and checks the permissions for dispatching the units):	Permission must be granted for the mobile user's role by the mobile user's agency for the Unit Status update command.	Commands – Unit Status command
Dispatch units onto incidents for *other* agencies (considers the units and checks the permissions for dispatching the units):	Trusted agency permission must be granted to the mobile user's role for the US command by the agency that the mobile user is attempting to create an incident for.	Commands (Trusted) – Unit Status command

Viewing a Role Preview

View a role preview when you want to see a role's permissions in a single-page tree view.

To view a role preview:

1. Access the form for a role. For instructions, see "Adding Roles" on page 8-2.

   The Roles form appears with the General tab in focus (see Figure 8-1). A list of existing roles displays on the left side of the tab.

2. From the list of roles, select the role you want to preview.

3. In the Roles window, select the Preview tab.

   The services and features assigned to the role display.

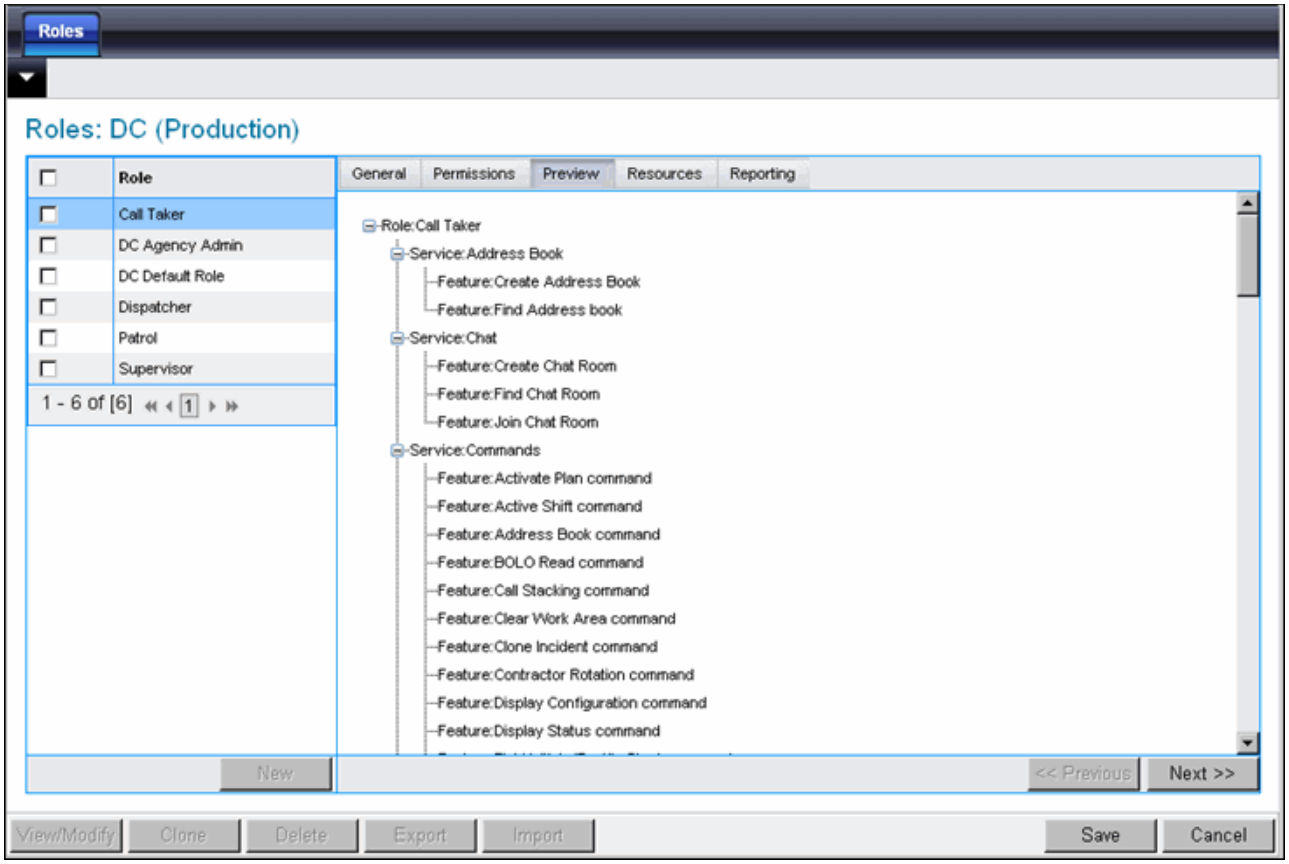


Figure 8-7 Roles Form – Preview Tab

Adding Resources to Roles

When you add resources to a role, you select the groups of resources that can potentially be assigned to the role. To add a person to a role, see "Adding Personnel Roles Information" on page 11-13.

To add resources to a role:

1. Access the form for a role. For instructions, see "Adding Roles" on page 8-2.

   The Roles form appears with the General tab in focus (see Figure 8-1). A list of existing roles displays on the left side of the tab.

2. In the Roles window, select the Resources tab.

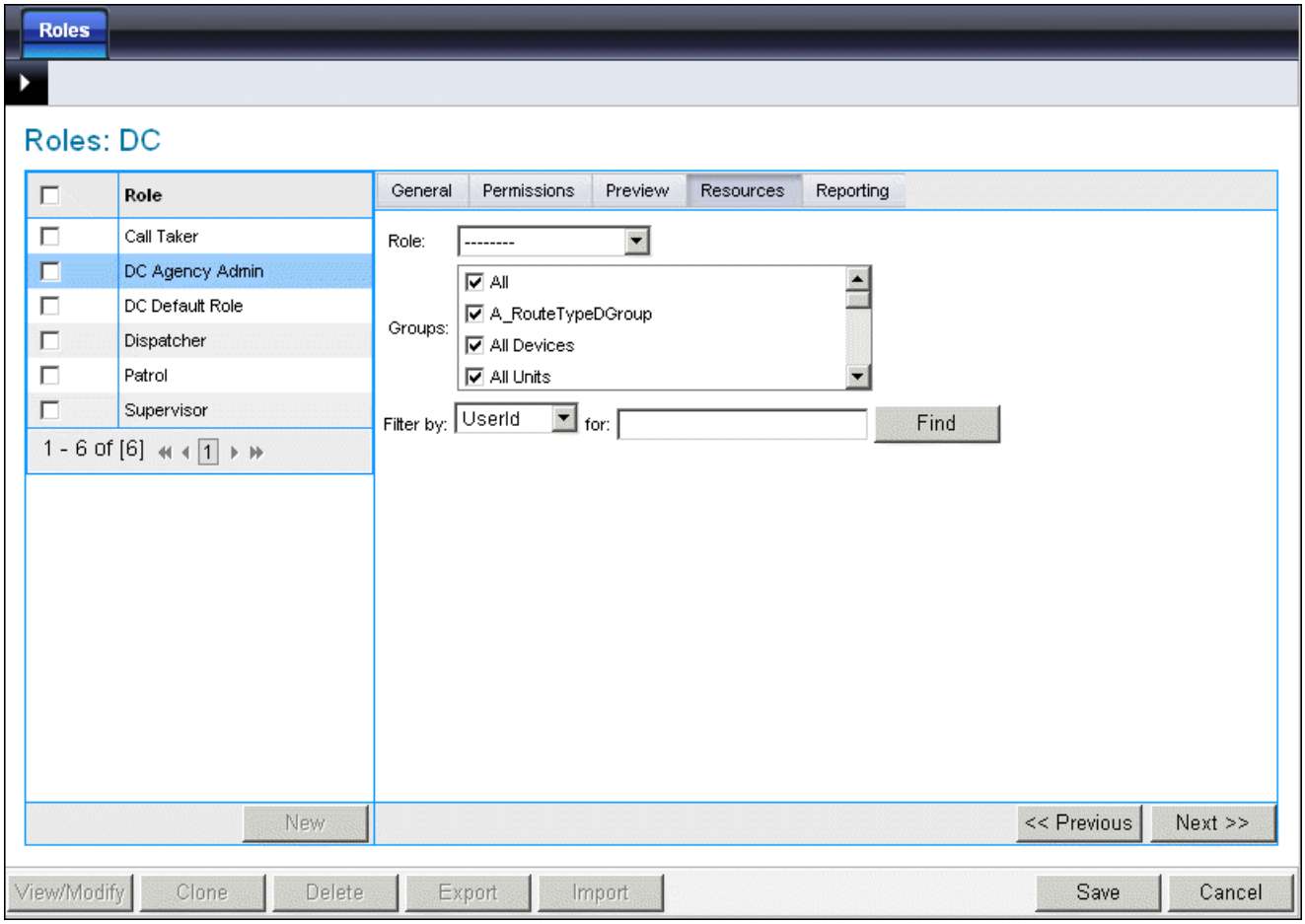


Figure 8-8 Roles Form – Resources Tab

3. From the Role list, make sure the correct role is selected.
4. In the Groups box, select the message groups that the role should be a member of.

   Groups are defined in the Address Book configuration item.

5. To add a specific person to role, do the following:

   a. From the Filter by list, select the Filter (Name or UserID).

   b. Enter the Name or user ID in the adjacent for box.

      These values are case-sensitive.

c. Click **Find**.

The matching persons display.

d. Select the check box to the left of the users and then click the **Add** button to add the users to the role.

NOTE

You can also add individuals to roles in the Resources item. For details, see "Adding Personnel Roles Information" on page 11-13.

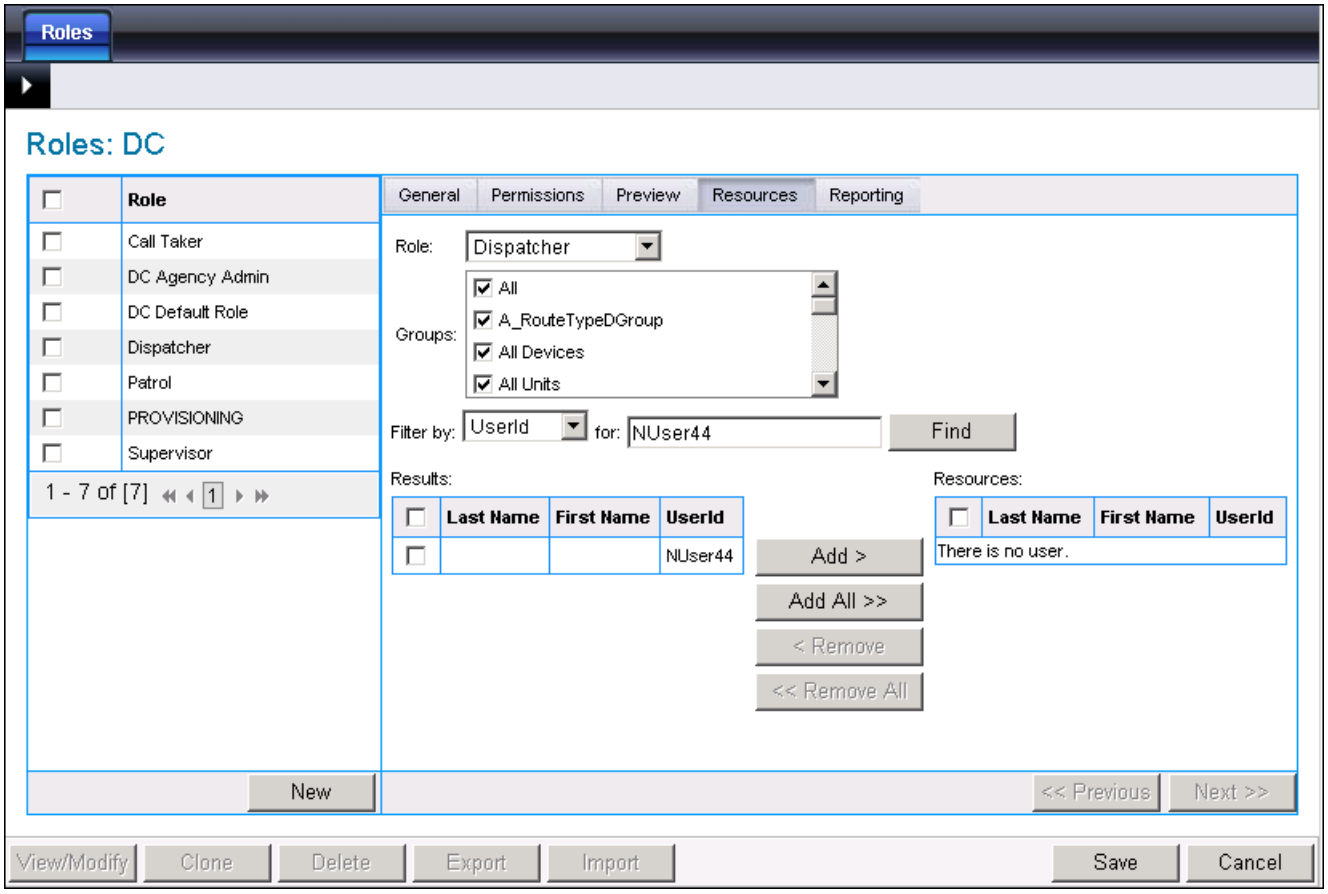


Figure 8-9 Roles Form – Resources Tab Showing Added User

6. Click **Save**.

Adding Reporting Permissions

You access reports in the System Management Portal through the PremierOne Reports item. In Provisioning, you can set permissions individually for each of the different data warehouses.

To add reporting permissions:

1. Access the form for a role. For more information, see "Adding Roles" on page 8-2.

   The Roles form appears with the General tab in focus (see Figure 8-1). A list of existing roles displays on the left side of the tab.

2. Click the Reporting tab.

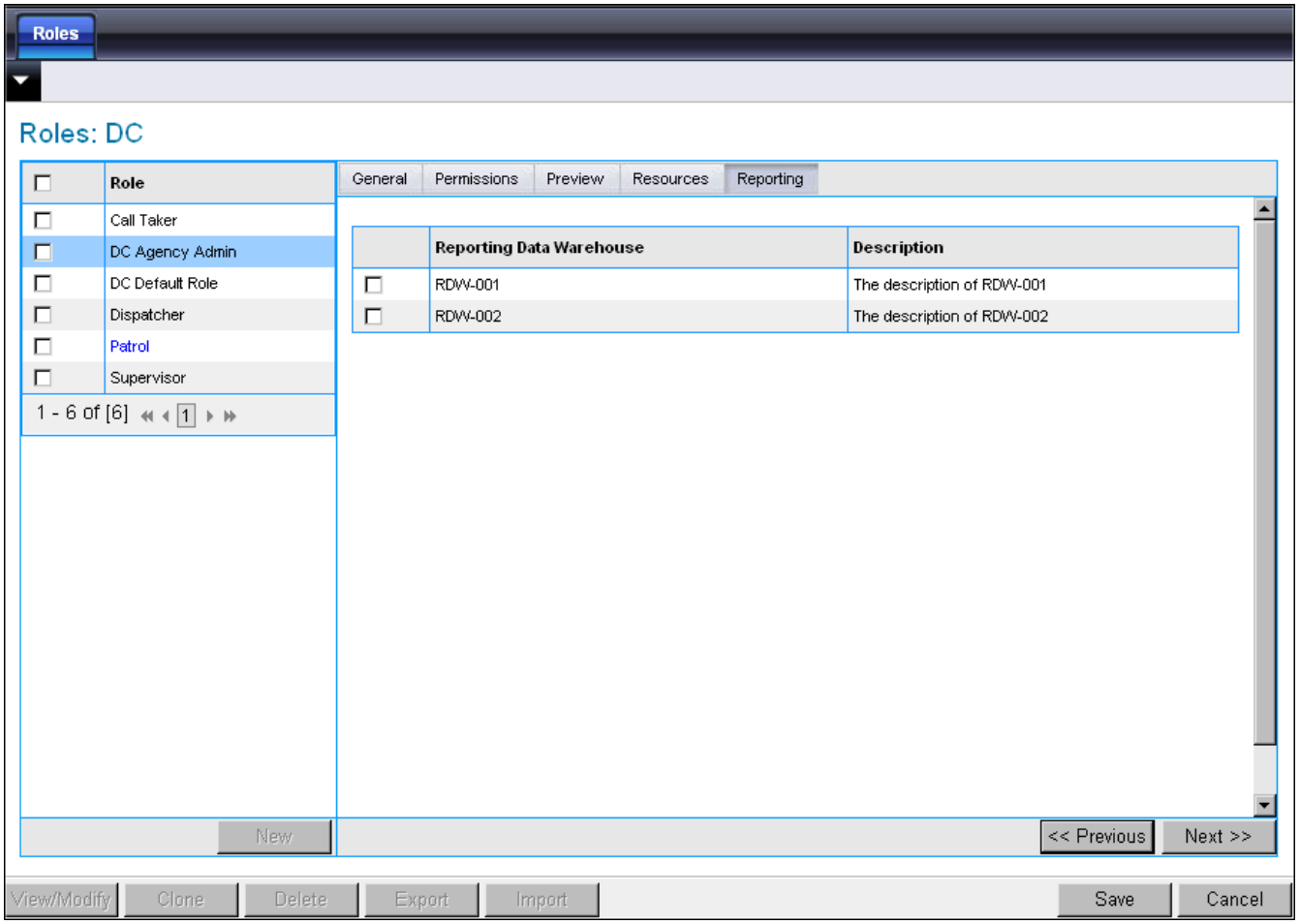


Figure 8-10 Roles Form – Reporting Tab

3. Select the role for which you want to set reporting permissions.

4. To grant access to a reporting data warehouse, select the check box for the data warehouse.

5. Click **Save**.

CHAPTER 9

Configuring Authentication

The Authentication configuration item contains the following item:

Agency Setting – Where you control agency settings for the following:

- General – Authentication settings, including maximum number of login retries, transfer workload defaults, concurrent login settings, logon features, inactivity timer, session timer, and offline request expiration. For details, see “Configuring General Agency Authentication Settings” on page 9-2.
- Password Config – Password creation rules, password duration settings, and password logon rules. For details, see “Configuring Passwords for Your Agency” on page 9-6.
- Emergency Mode – Whether to enable emergency mode. For details, see “Enabling the Emergency Mode” on page 9-8.
- System Notification – Optional logon banner, and notifications for user account lock, workstation lock, login attempt on locked user accounts, and login attempt on locked workstations. For details, see “Configuring System Notifications” on page 9-9.
- Forced Password Change – Users who will be forced to change their passwords at their next login. For details, see “Forcing Password Changes” on page 9-11.

For information about using Lists and Statute Management to provision Active Directory for authentication, see “Configuring Active Directory for Authentication” on page 6-9.

Configuring Agency Authentication Settings

The Agency Authentication configuration item is where you set the authentication parameters for your agency, including general settings, password settings, emergency mode settings, system notifications, and forced password changes.

Configuring General Agency Authentication Settings

General agency authentication settings include BOLO settings, maximum number of login retries, transfer workload default settings, concurrent login settings, logon features, inactivity timer settings, session timer settings, and offline request expiration settings.

To configure general agency settings:

1. From the navigation panel, select **Authentication**, and then select **Agency Setting**.

The Authentication Settings form appears with the General tab in focus.

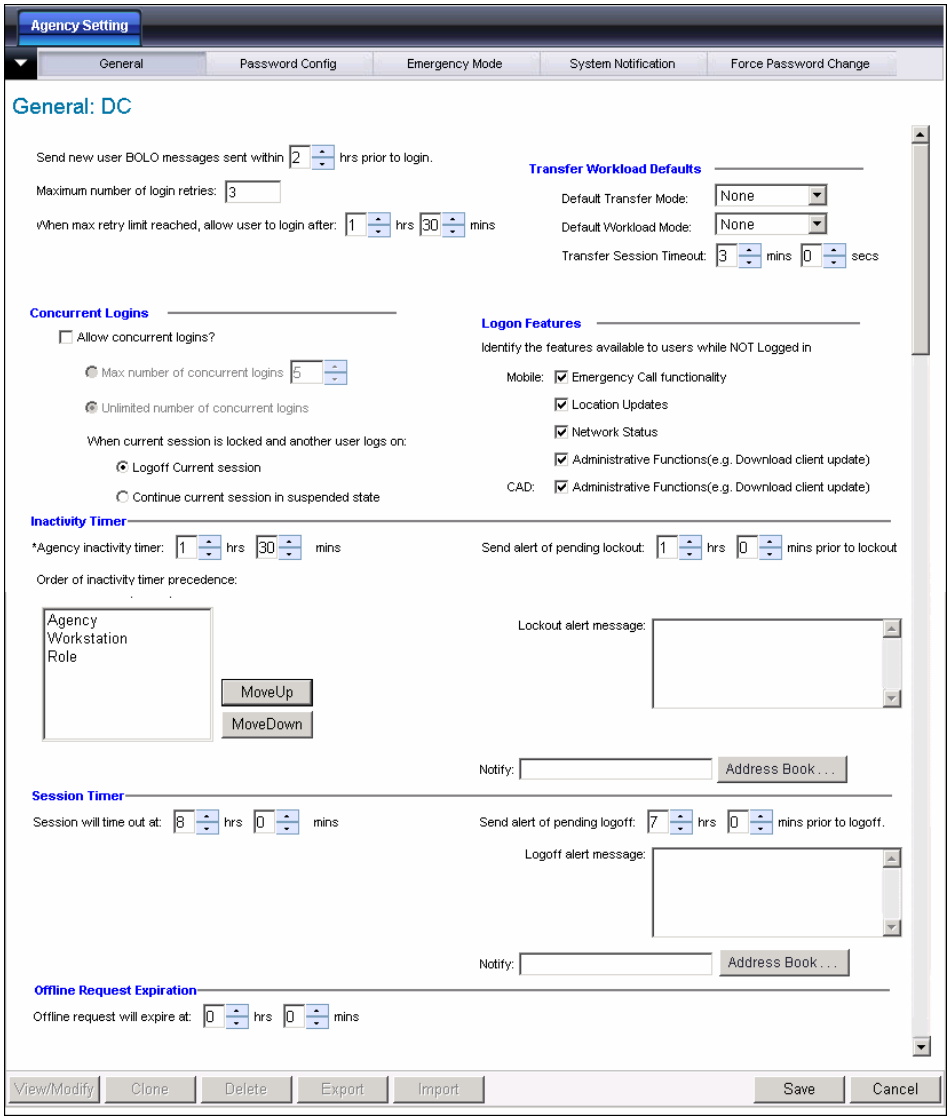


Figure 9-1 Authentication Settings – General Tab

2. Click **View/Modify**.

3. In the Send new user BOLO messages sent within X hrs prior to login field, enter how many hours to search to retrieve BOLO messages for a user that has just logged in.

4. In the Maximum number of login retries field, enter how many login attempts a user can make before the user is locked out of the system.

5. In the Transfer Workload Defaults section, do the following:

a. From the Default Transfer Mode list, select **None**, **Move**, or **Share**.

This will be the value used in the Workload Transfer command unless the user specifies a different value. Items that are transferred can be moved or shared. When they are moved, they are removed from the originator's console. A null value disables a default value.

b. From the Default Workload Mode list, select **None**, **Areas**, or **Incidents**.

This will be the value used in the Workload Transfer command unless the user specifies a different value. Incidents or areas can be transferred. A null value disables a default value.

c. In the Transfer Session Timeout field, enter the number of minutes and seconds before a user's session times out.

6. In the Concurrent Logins section, do the following:

a. To allow concurrent logins, select the **Allow concurrent logins** check box. This allows a user to log in to more than one system at a time.

If you selected **Yes**, enter a number for the Max number of concurrent logins or select Unlimited number of concurrent logins.

Concurrent logins allow users to log in to more than one device at a time. Concurrent logins can also be set for a device type in the Resources-Personnel configuration item and for an individual person in the Resources-Personnel configuration item. For details, see "Adding Device Type Login Information" on page 11-36 and "Adding Personnel Authorization Information" on page 11-14.

The most restrictive setting will apply. For example, if the agency level is set to not allow concurrent logins, the settings for devices and personnel are disregarded.

b. In the When current session is locked and another user logs on field, select how you want the locked session handled.

NOTE

If a call taker is using NG9-1-1 Call Control functionality, Motorola strongly recommends that the user is NOT allowed concurrent logins. NG9-1-1 Call Control requires that the same user ID only be active within the Call Control module one session at a time. If a user is active in two call control sessions simultaneously, statistics regarding 9-1-1 call handling would be incorrect. The SMS Text messaging gateway between citizen cell phones would also be affected and the call control could potentially misdirect messages.

7. In the Logon Features section, select the features that are available to users who are *not* logged in

- Emergency Call functionality – Whether the Mobile user can send an Emergency status by selecting the Emergency button on the Mobile login screen

- Location Updates – Whether the Mobile unit continues to report its location through ARL even though the unit is not logged in
- Network Status – Whether the mobile user can view the network status
- Administrative functions (e.g., Download client update) – Whether the CAD and Mobile users can perform administrative functions such as downloading updates

8. In the Inactivity Timer section, do the following:

   a. In the Agency inactivity timer field, enter the number of hours and minutes for the inactivity timer at an agency level. Once the time is exceeded, the workstation is locked and the user must login again.

      To set the inactivity timer for the role, see the Session Lockout due to inactivity after field in "Adding Role General Information" on page 8-2.

      To set the inactivity timer for the workstation, see the Inactivity Timer (HH:MM) field in "Adding Workstation/MDT/Handheld General Information" on page 11-44.

   b. In the Order of inactivity time precedence box, reorder the Agency, Role, and Workstation in order of importance, where the top entry takes precedence over the other entries if the timers are different.

   c. In the Send alert of pending lockout X hrs X mins prior to logout field, enter the number of hours and minutes before an alert is sent.

   d. In the Lockout alert message field, type the text for the message that will be appear based on the information in the Send alert of pending lockout X hrs X mins prior to logout field.

   e. To send notification messages to specific users when an inactivity lockout occurs, click the **Address Book** button and select the users to notify.

      The Search Address Book dialog box appears. Select the users you want to notify, and then click **Save**.

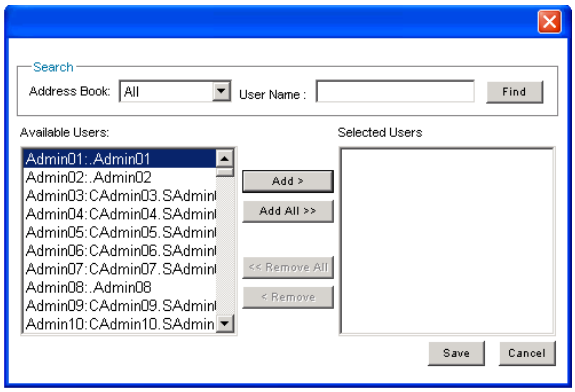


Figure 9-2 Search Address Book Dialog Box

9. In the Session Timer section, do the following:

   a. In the Session will time out at field, enter the number of hours and minutes for the session timer at an agency level.

   b. In the Send alert of pending logoff X hrs X mins prior to logoff field, enter the number of hours and minutes before an alert is sent.

   c. In the Logoff alert message field, type the text for the message that will be sent based on the information in the Send alert of pending logoff X hrs X mins prior to logoff field.

   d. To send notifications when the session times out, click the **Address Book** button and select the users to notify.

      A Search Address Book dialog box appears (see Figure 9-2).

10. In the Offline Request Expiration section, enter how many hours and minutes the users in your agency can work in offline mode before a dialog box displays asking them if they want to work in offline mode.

11. Click **Save**.

Configuring Passwords for Your Agency

Password configuration settings include password creation rules, password duration settings, and password logon rules.

To configure passwords for your agency:

1. Access the form for authentication settings. For instructions, see "Configuring General Agency Authentication Settings" on page 9-2.

   The Authentication Settings form appears with the General tab in focus (see Figure 9-1).

2. Select the Password Config tab and click the **View/Modify** button.

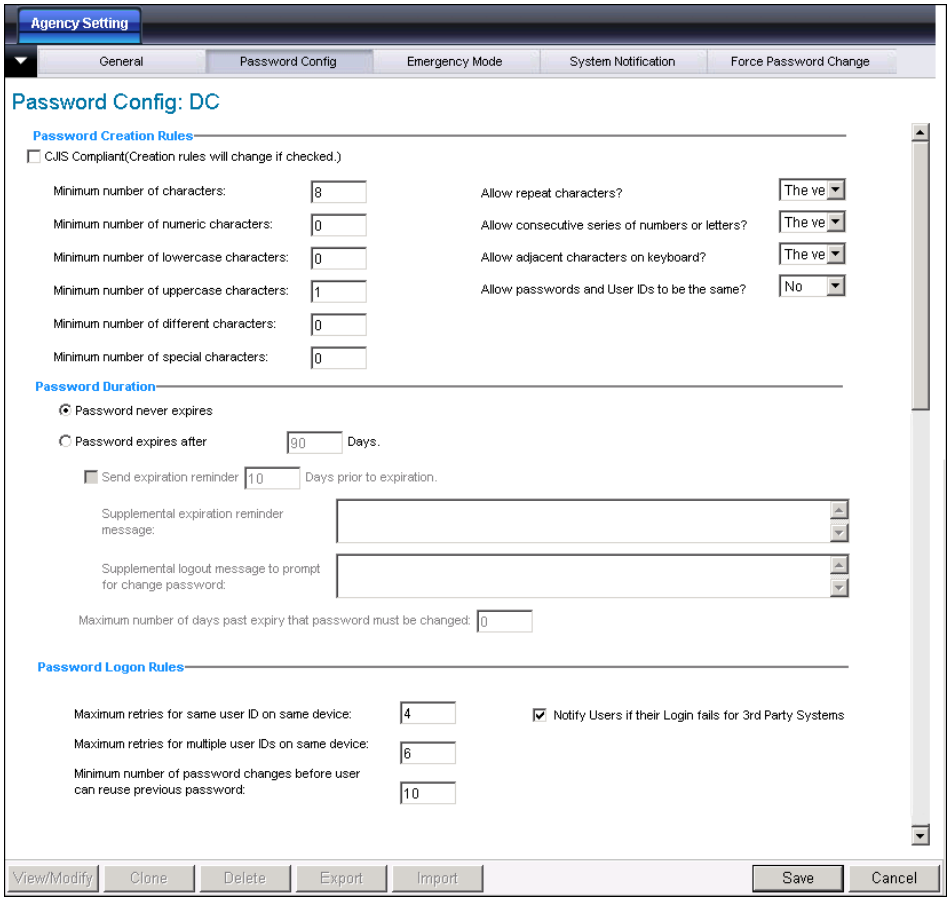


Figure 9-3 Authentication Settings – Password Config Tab

3. In the Password Creation Rules section, specify the rules for passwords for your agency.

   For PremierOne to check that passwords are CJIS (Criminal Justice Information System) compliant, select the **CJIS Compliant** check box (see *CJIS Security Policy* for password requirements).

   Following is a description of fields that may need further clarification:

   - Allow repeat characters – Whether characters can be repeated, such as KK, LLL or 99.
   - Allow consecutive series of numbers or letters – Whether numbers and letters that are consecutive can be in a password, such as 1234, 67, AB, ABCD, and so on.
   - Allow adjacent characters on keyboard – Whether adjacent characters on the keyboard can be in a password such as asd, qw, jk, nm, 78, and so on.

- Allow passwords and User IDs to be the same – Whether a user's logon ID and password can be the same, for example, user ID `jsmith` and password `jsmith`.

4. In the Password Duration section, indicate whether the password expires. If the password expires:

   a. Specify when the password expires.

   b. Select whether to send a reminder and how many days before expiration to send the reminder.

   c. Type a reminder message.

   d. Type a message to appear when the user logs out to prompt him or her to change the password.

   e. Enter the number of days past the expiration during which the password may still be changed. This is the grace period.

5. In the Password Logon Rules section, specify the rules for password retries, changes, and failures.

6. Click **Save**.

Enabling the Emergency Mode

If your agency has an emergency situation, such as a major event or disaster, you may want more workstations. Enabling emergency mode removes the security from workstations so authorized users can use the workstations.

To enable the emergency mode:

1. Access the form for authentication settings. For instructions, see "Configuring General Agency Authentication Settings" on page 9-2.

   The Authentication Settings form appears with the General tab in focus (see Figure 9-1).

2. Select the Emergency Mode tab and click the **View/Modify** button.

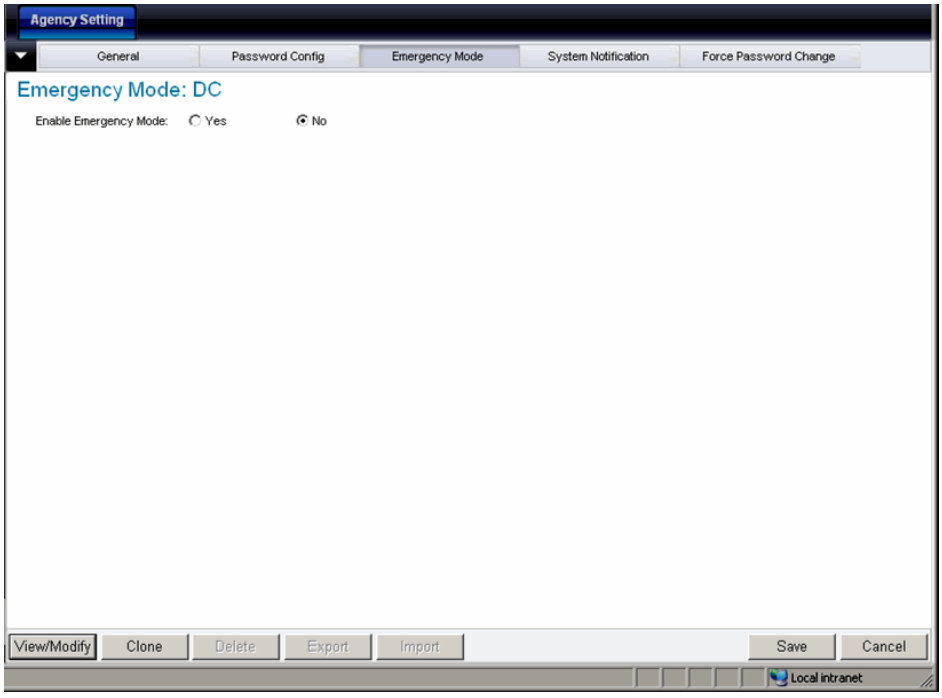


Figure 9-4 Authentication Settings – Emergency Mode Tab

3. Select **Yes** to enable emergency mode. Select **No** to cancel emergency mode.

4. Click **Save**.

Configuring System Notifications

System notification settings affect the banner that displays before the user logs on to PremierOne, notifications for user account lock and workstation lock, login attempts on locked user accounts, and login attempts on locked workstations.

To configure system notifications:

1. Access the form for authentication settings. For instructions, see “Configuring General Agency Authentication Settings” on page 9-2.

   The Authentication Settings form appears with the General tab in focus (see Figure 9-1).

2. Select the System Notification tab, and then click the **View/Modify** button.

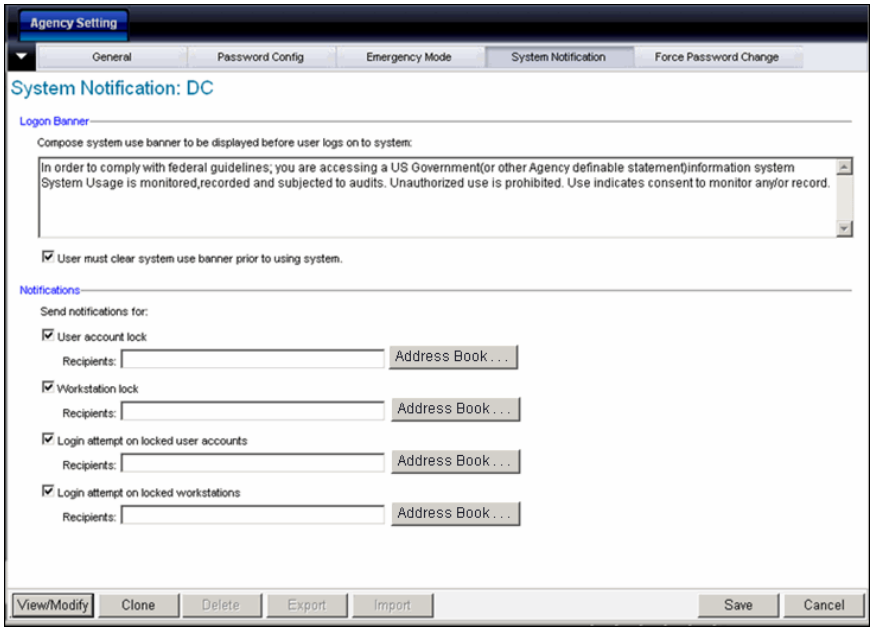


Figure 9-5 Authentication Settings – System Notification Tab

3. In the Logon Banner section, type a statement that you want to appear on the Login Successful dialog box when users log in to any PremierOne application.

4. Select whether users must clear the Login successful dialog box prior to using the application.

5. In the Notifications section, select which lock situations require that someone should be notified. For each selected situation, indicate the recipients by clicking **Address Book**.

   The Search Address Book dialog box appears.

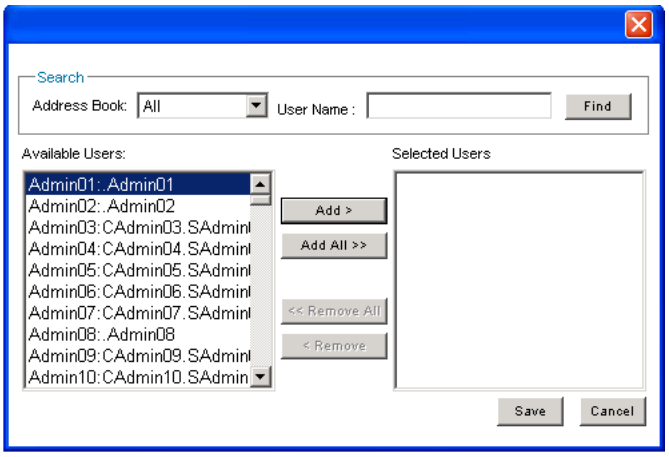


Figure 9-6 Search Address Book Dialog Box

   Select the users you want to notify about locked accounts or workstations.

6. Click **Save** to close the Search Address Book dialog box.

7. Click **Save**.

Forcing Password Changes

Force password changes affect selected users who will be forced to change their password the next time they log in.

To force password changes:

1. Access the form for authentication settings. For instructions, see "Configuring General Agency Authentication Settings" on page 9-2.

   The Authentication Settings form appears with the General tab in focus (see Figure 9-1).

2. Select the Force Password Change tab, and then click the **View/Modify** button.

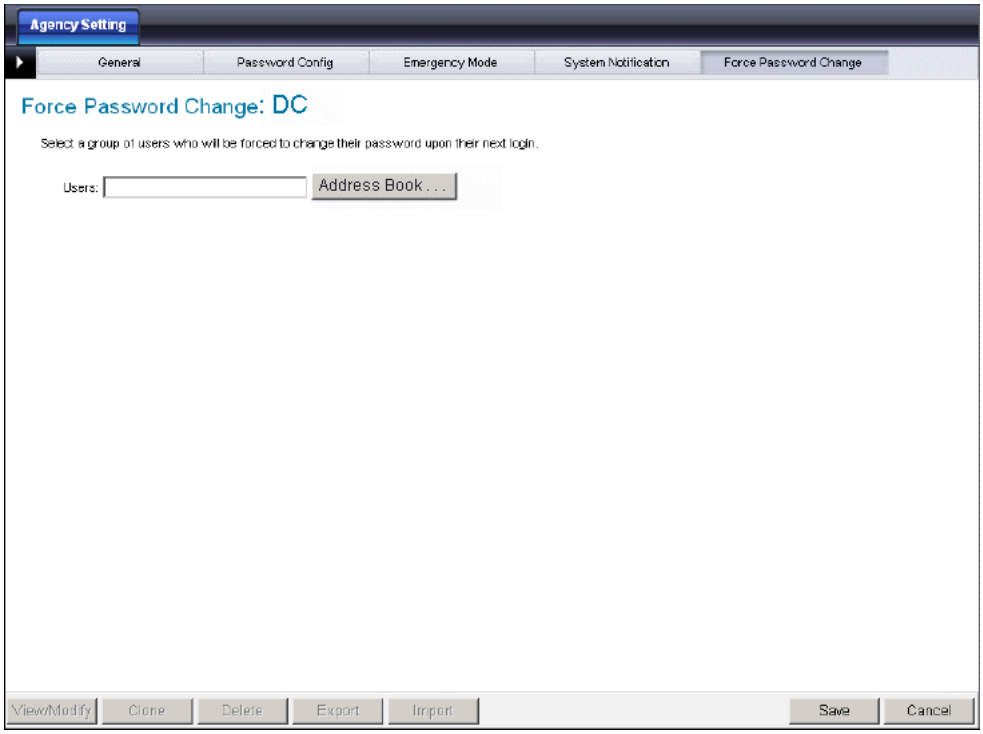


Figure 9-7 Authentication Settings – Force Password Change Tab

3. Click **Address Book**.

The Search Address Book dialog box appears.

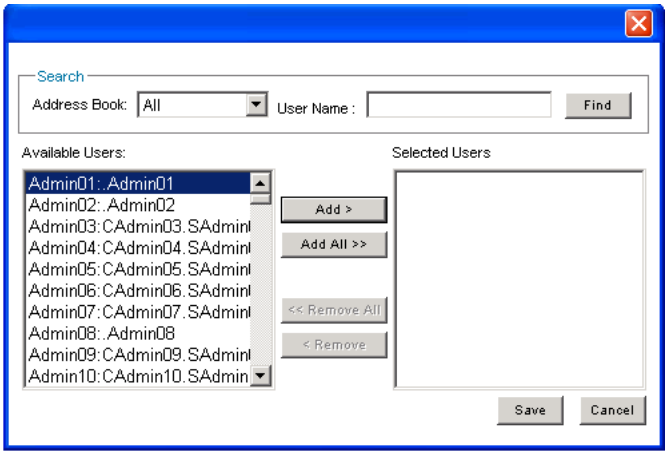


Figure 9-8 Search Address Book Dialog Box

Select the users who must change their passwords, and then click **Save** to close the Search Address Book dialog box.

4. Click **Save**.

   The next time you return to the Force Password Change Tab, the names you selected in the previous step will no longer be displayed. This feature allows you to select new names each time.

CHAPTER 10

Configuring Unit Management

The Unit Management configuration item contains the following items:

- Units – Where you create unit IDs and configure unit preassignments. For details, see “Configuring Units” on page 10-2.
- Unit Status Codes – Where you create status codes and set the order that the status codes display in Mobile units. For details, see “Configuring Unit Status Codes” on page 10-11.
- Cross Staffing Groups – Where you define sets of units to apply special availability rules to. For details, see “Configuring Cross Staffing Groups” on page 10-19.
- Settings – Where you set command line options for incident numbers and unit call sign, configure shift ID codes and activation times, and configure unit transactions and status settings. For details, see “Configuring Unit Management Settings” on page 10-21.
- Activity Codes – Where you configure the codes used to categorize activity and time spent by units other than the time tracked by unit status codes. For details, see “Configuring Activity Codes” on page 10-29.
- Duty Type – Where you manage the equipment categories for units. For details, see “Configuring Duty Types” on page 10-30.

The Move Up command (MU) allows dispatchers to replenish stations or areas that have been depleted of resources (for example, a station that sends all of its units to fight a fire). The feature is configured under several different configuration items. For details, see “Configuring Move Ups” on page 10-32.

Configuring Units

Use the Unit Management configuration item to configure unit IDs and set up unit preassignments for call sign, equipment, personnel, and vehicles.

Unit IDs are used to place a unit on duty and are similar to the call sign for the unit. The only difference between the unit ID and the unit call sign is that the unit ID contains the shift ID and potentially the agency ID when multiple agencies are involved.

You can add, modify, clone, and delete units. For details on cloning, modifying, and deleting, see "Working With Configuration Items" on page 2-9.

The Unit Management item has two tabs:

- Unit ID – Where you configure unit IDs.
- Unit Preassignments – Where you configure preassignments for call sign, equipment, personnel, and vehicles.

Adding Unit IDs

Add unit IDs when you need one of the following:

- You want unit IDs to be validated.

  Add unit IDs when you require existing unit IDs to be used in your agency. Unit IDs are only validated when you select the Validate unit ID check box in Unit transactions. For details, see "Configuring Unit Status Transaction" on page 10-24.

- You want off-duty unit IDs to display on the unit status monitor. PremierOne uses Unit IDs to update display information. The unit must have been on duty at some time in the past for it to appear in the status monitor.

To add a unit ID:

1. From the navigation panel, select **Unit Management** and then select **Unit**.

The Unit IDs form appears.

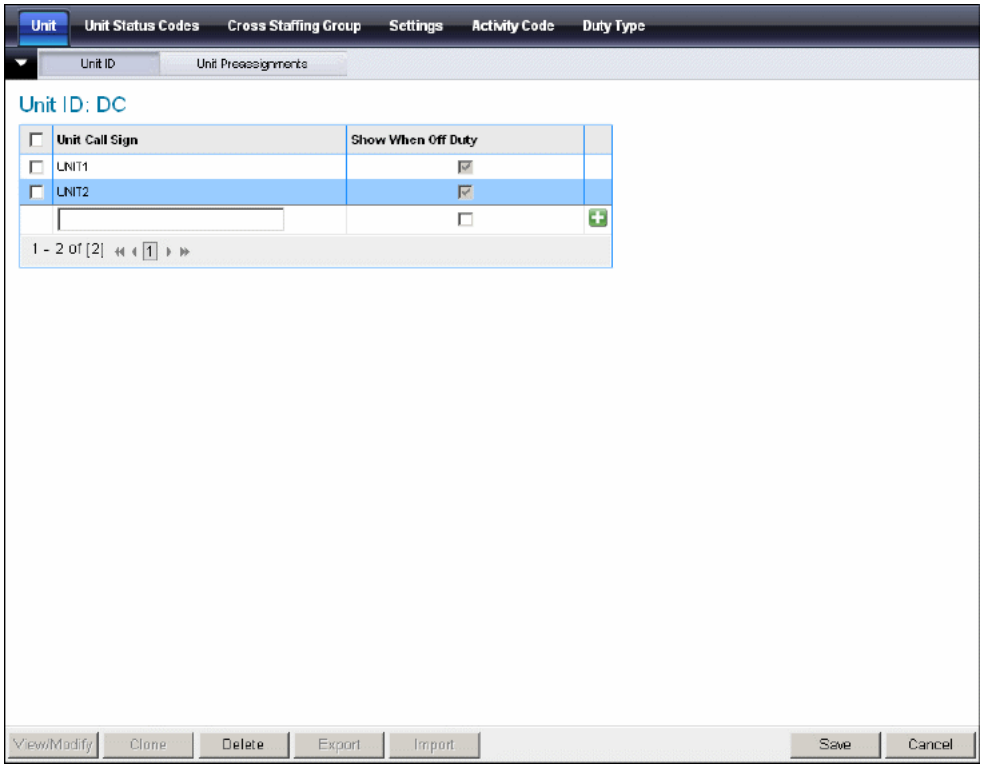


Figure 10-1 Unit Form – Unit ID Tab

2. Click **View/Modify**.

   A new row displays for the unit ID.

3. In the Unit Call Sign field, type the call sign.

4. Select whether you want to display the unit ID on status monitors when the unit is off duty.

5. Press **Enter** or click the plus symbol at the end of the row to save the unit call sign and to add another row.

> **CAUTION**
> If you do not press **Enter** or the plus symbol, PremierOne does not save the unit call sign, even after you click **Save**.

6. Click **Save**.

   The Unit ID is added.

Configuring Unit Preassignments

Use the Unit Preassignments configuration item to preconfigure unit assignments for your agency. Properties consist of call sign, Shift ID, supervisor, jurisdiction, vehicle information, personnel information, and unit equipment. Unit assignment information can be changed when a unit is placed on duty.

If an agency is provisioned to validate Unit IDs (see validate unit ID when placing unit on duty in “Configuring Unit Status Transaction” on page 10-24), (see “Adding Unit IDs” on page 10-2).

Adding New Unit Preassignments

To add a unit, you enter information on five tabs of the Unit form:

- Gen. Preassignments – Where you enter or change the agency, call sign, shift ID, supervisor, and jurisdiction information.
- Personnel & Vehicle – Where you enter or change the vehicle ID, capabilities, equipment types, and equipment IDs.
- Unit Equipment – Where you enter or change any equipment assigned to the unit.
- Unit Capabilities – Where you enter or change the Capability Group Code and any additional capabilities for the unit.
- Capability Settings – Where you view and set the default Capability and Skill Settings.

Adding Unit General Preassignments

Add general preassignments when you need to set up the unit identification and define its jurisdiction.

To add unit general preassignments:

1. From the navigation panel, select **Unit Management**.
2. Select **Unit**, and then select **Unit Preassignments**.

The General tab of the Unit Preassignments form appears. A list of existing records displays on the left side of the form.

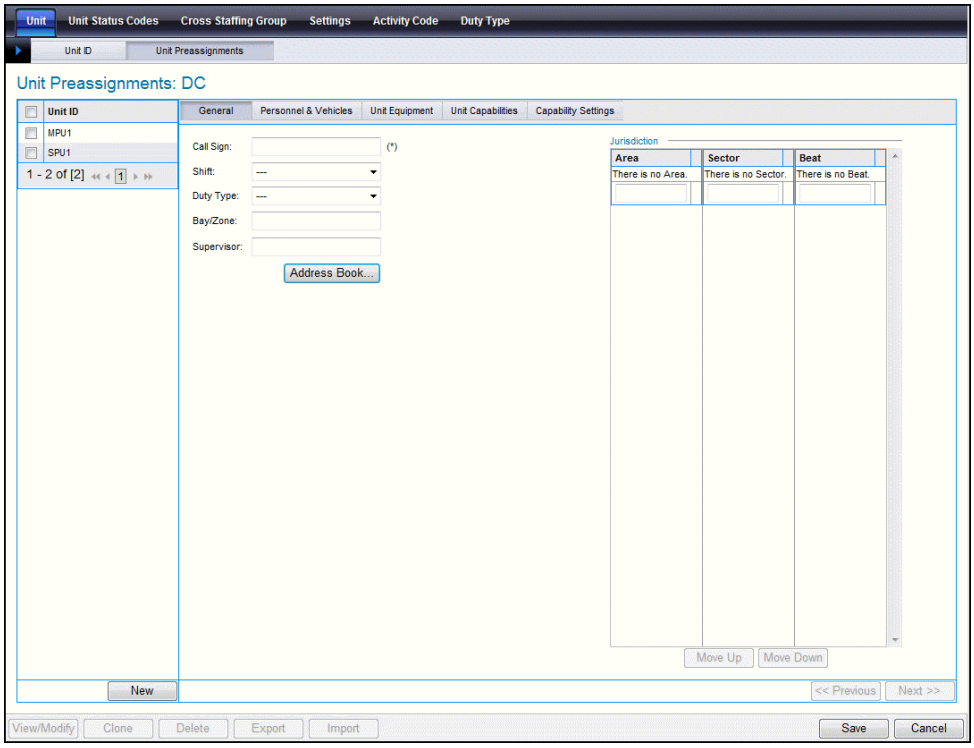


Figure 10-2 Unit Form – Gen. Preassignments Tab

3. At the bottom of the Unit IDs, click the **New** button.
4. In the Call Sign field, type the call sign for the unit.
5. If the unit will always be assigned to the same shift ID, select the shift ID to which the unit will be assigned from the Shift list.
6. In the Duty Type field, select the duty type to which this unit is assigned.
7. In the Bay/Zone field, type the bay or zone to which this unit is assigned.
8. If the unit will always be assigned to the same supervisor, click the **Browse** button below the Supervisor list and search for and select the supervisor.
9. If stations are being used, select the station from the Station field.
10. In the Jurisdiction section, enter the areas, sectors, and beats for the unit assignment for the unit.

    The order of the assignments are used for recommendations based on jurisdictional assignments. Assignments at the top of the list are considered first. To change the order, select the area, sector, or beat that you want to move, and then click **Move Up** or **Move Down**.
11. Click **Save**.

Adding Personnel and Unit Vehicle Information

Add personnel an unit vehicle information to a unit when you want to permanently assign personnel and a vehicle to a unit.

To add personnel and unit vehicle information:

1. Open the Unit Preassignments form.

   For details, see “Adding New Unit Preassignments” on page 10-4.

2. In the Unit Preassignments form, select the Personnel & Vehicles subtab.

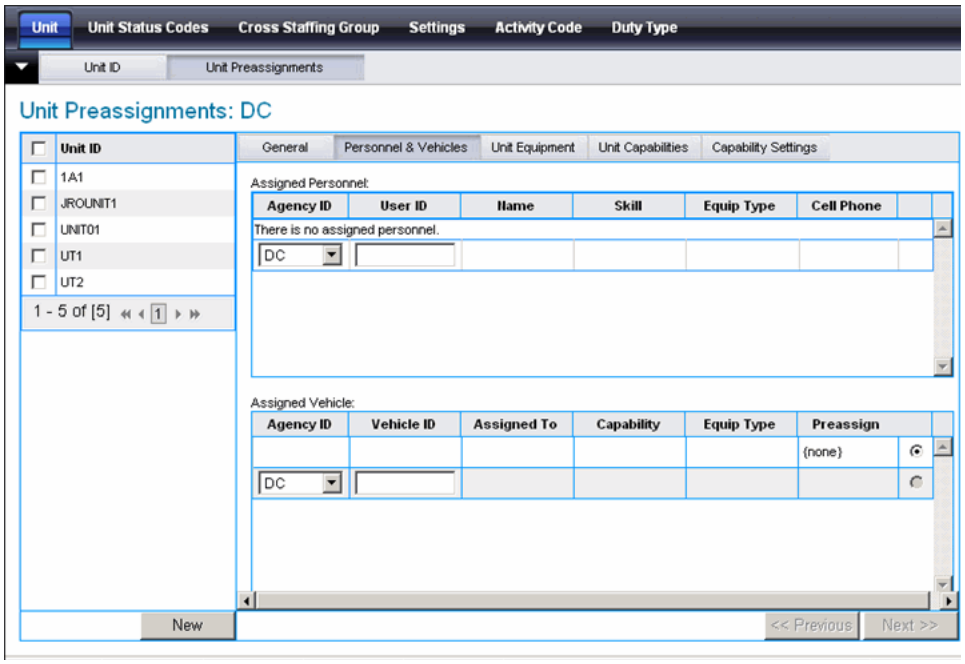


Figure 10-3 Unit Form – Personnel & Vehicles Subtab

3. From the Agency ID list, select the appropriate agency.

4. From the Assigned Personnel section:

   a. In the Agency ID field, select the ID for the agency of the person you are assigning to the unit.

   b. In the User ID field, type the ID of the person you are assigning to the unit.

   c. Press **Tab** or **Enter**.

      The Name, Skill, Equip Type, and Cell Phone fields populate according to the information available in “Adding Personnel Records” on page 11-8.

      If a vehicle was assigned to the person in “Adding Personnel Records” on page 11-8, the information in the Assigned Vehicle section for that Vehicle ID populates when you press the Tab or Enter key.

5. From the Assigned Vehicle section, do one of the following:

   a. If a vehicle was assigned to the person in "Adding Personnel Records" on page 11-8, you can choose that vehicle by selecting the button at the end of that row. Or you can assign a different vehicle using the procedure in step b.

   b. If there was no preassigned vehicle, {none} appears in the first line in the Preassign field. On the second line:

      1) In the Agency ID field, select the ID for the agency.

      2) In the Vehicle ID field, type the ID of the vehicle you are assigning to the unit.

         Any Capabilities and Equipment Types assigned to that vehicle appear in their respective fields.

      3) Press **Tab** or **Enter**.

         The Assigned To, Capability, Equip Type, and Preassign fields populate according to the information available in "Adding Equipment" on page 11-41.

      4) Select the button at the end of the row.

   c. Select no vehicle by leaving the first row selected.

6. Click **Save**.

Adding Unit Equipment Information

Add equipment to a unit when you want to permanently assign the equipment to the unit.

To add unit equipment:

1. Open the Unit Preassignments form.

   For details, see "Adding New Unit Preassignments" on page 10-4.

2. Select the Unit Equipment subtab.

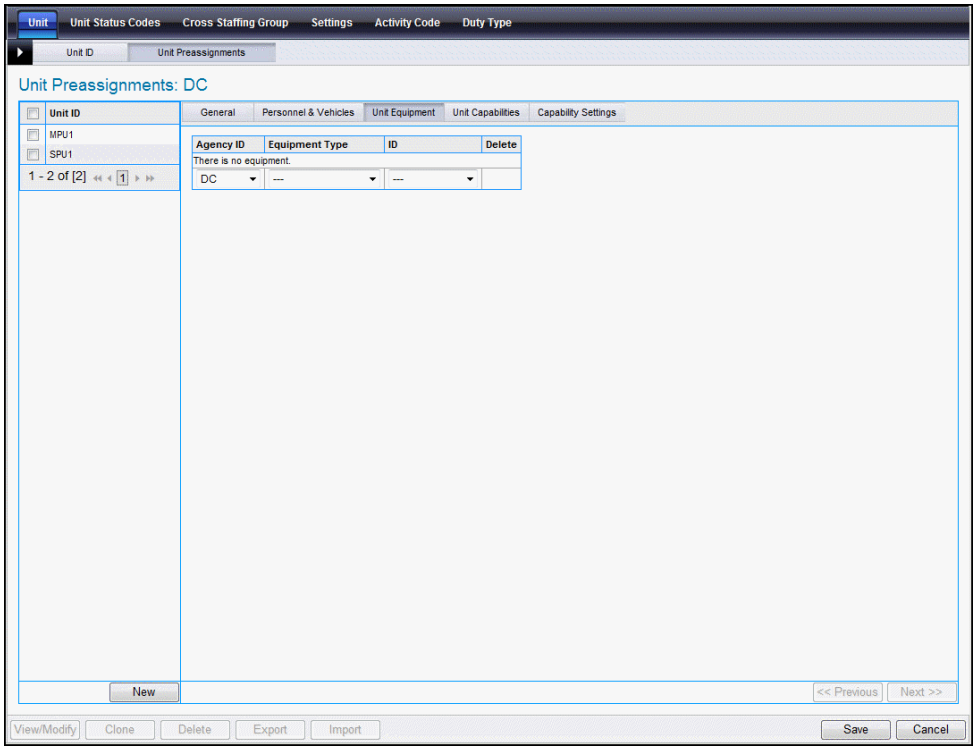


Figure 10-4 Unit Form – Unit Equipment Subtab

3. From the Agency ID list, select the agency with which this equipment is associated.
4. From the Equipment Type list, select the equipment that is assigned to this unit. Unit equipment can include one or more radios, MDTs, pagers, handhelds, and so on.
5. From the ID list, select the device ID for the equipment.

   PremierOne adds another row.
6. Click **Save**.

Adding Unit Capabilities Information

Add unit capabilities to a unit when you want to change the provisioned assignment.

To add unit capabilities:

1. Open the Unit Preassignments form.

   For details, see “Adding New Unit Preassignments” on page 10-4.

2. In the Unit Preassignments form, select the Unit Capabilities subtab.

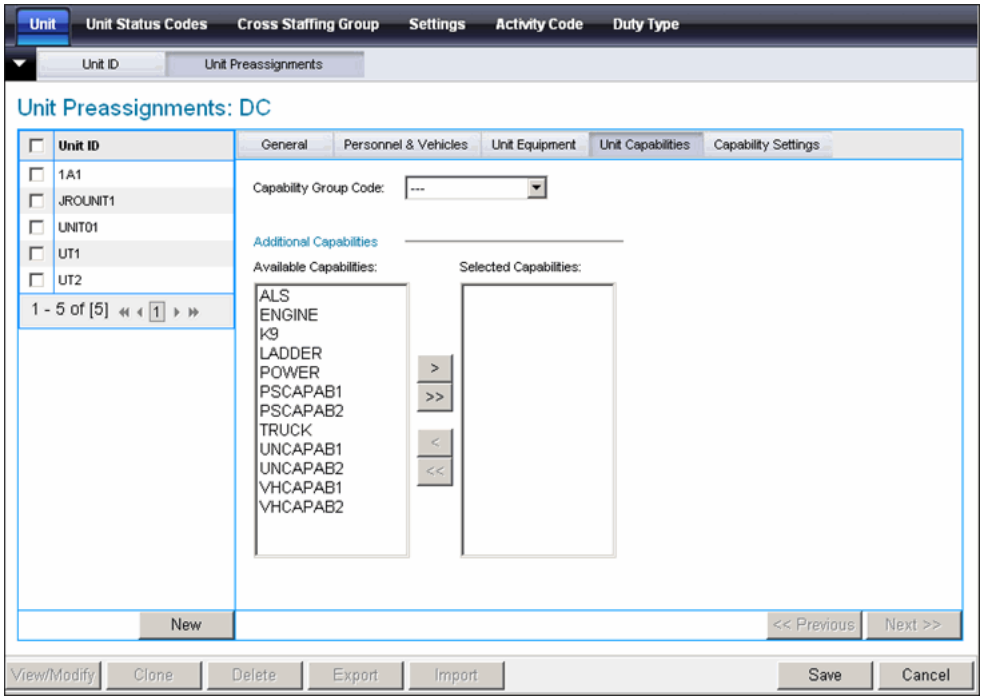


Figure 10-5 Unit Form – Unit Capabilities Subtab

3. From the Capability Group Code list, select the Capability Group for the capabilities for this unit.

   See “Configuring Personnel” on page 11-7 for more information about defining and using capability groups.

4. In the Additional Capabilities section, select capabilities from the Available Capabilities box and move them to the Selected Capabilities box.

5. Click **Save**.

Adding Capability Settings

Add capability settings for a unit when you want to change the provisioned assignment.

To add unit capability settings:

1. Open the Unit Preassignments form.

   For details, see “Adding New Unit Preassignments” on page 10-4.

2. Select the Capability Settings subtab.

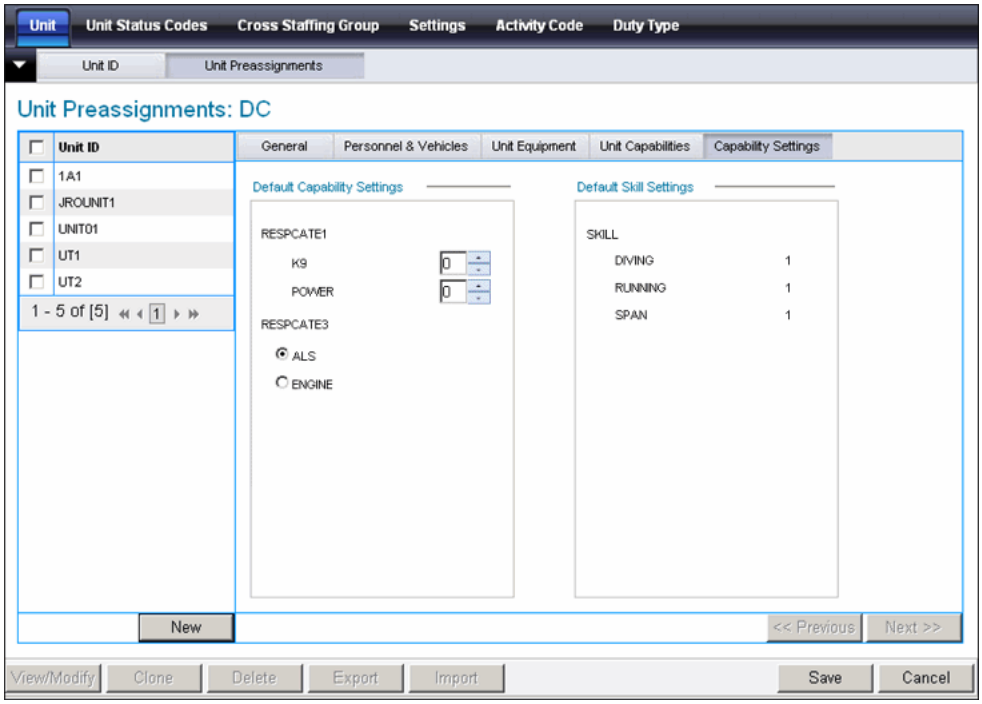


Figure 10-6 Unit Form – Capability Settings Subtab

3. From the Unit ID list, select the unit for which you want to view or modify capability settings.

   The Default Capability Settings box lists all capabilities that are provisioned for the unit. They are grouped by their provisioned response category and the response categories are ordered alphabetically. Within each response category, capabilities are sorted by capabilities that do not allow numeric entry, followed by capabilities that do allow numeric entry.

   The Default Skill Settings box lists all skills and their occurrences, in alphabetical order, that are provisioned for the personnel and that are provisioned for the unit.

4. Click **View/Modify**.

5. In the Default Capability Settings box, make any required changes.

6. Click **Save**.

Configuring Unit Status Codes

Use the Unit Management Unit Status Codes configuration item to configure unit status codes and to set the order that the status codes display in MDTs. You can also set the option for a Mobile user to remain active in CAD when logged out of Mobile.

You can add, modify, clone, deleting, import, and export unit status codes. For details on modifying, cloning, deleting importing, and exporting codes, see "Working With Configuration Items" on page 2-9.

Adding Unit Status Codes

When you add a unit status code, you enter information on two tabs of the Unit Status Codes form:

- Properties – Where you enter the agency type, agency, status code, description, category, and options.
- Timeouts – Where you enter the timeouts for each priority.

You cannot modify unit status codes. To change a code, you must delete and then re-add the record.

Adding Unit Status Code Properties Information

Add unit status code properties information when you are setting up new status codes and need to define the basic information.

To define unit status code properties information:

1. From the navigation panel, select **Unit Management**, and then select **Unit Status Codes**.

The Unit Status Codes form appears. A list of existing records displays on the left side of the form.

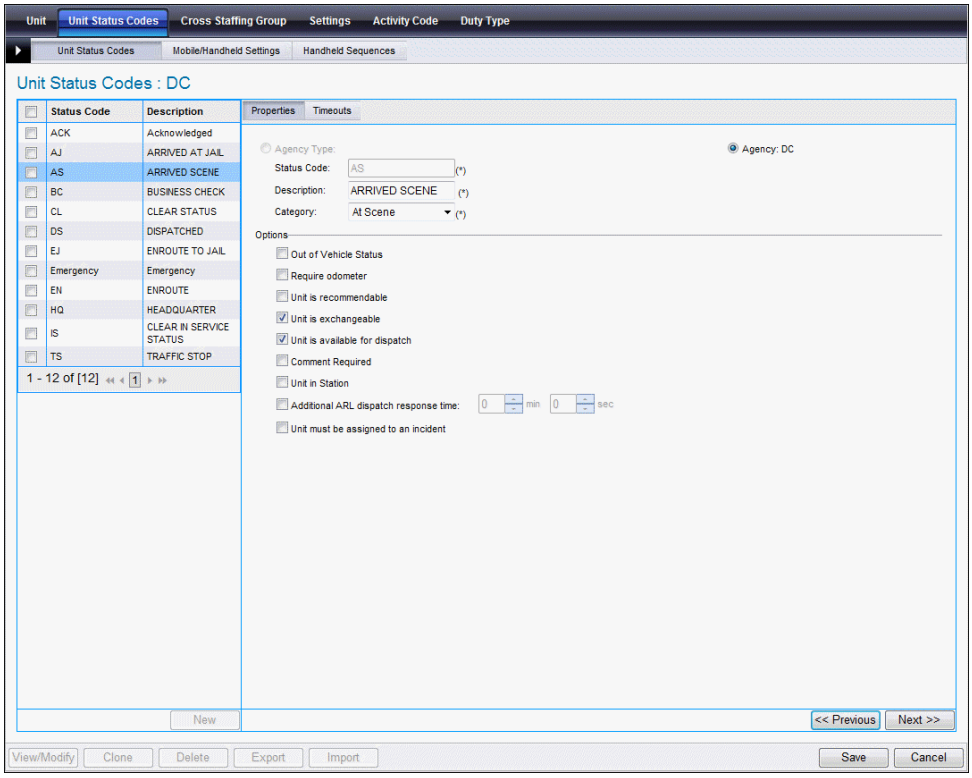


Figure 10-7 Unit Status Codes Form – Properties Tab

2. At the bottom of the Status Code list, click the **New** button.
3. In the Status Code field, type your new code.
4. In the Description field, type a description for the new code.
5. From the Category list, select the category for the status code.

   Categories are groups for statuses that are used for reporting. For example, you could have multiple statuses that are all in the Administrative category, such as HG (headquarters), ML (meal), and OS (out of service).

6. In the Options section, select the options appropriate for this status. You can select more than one option.

   The list of options changes depending on the category you choose, but always includes the following:

   - Require odometer
   - Unit is recommendable
   - Unit is exchangeable

- Unit is available for dispatch (selected by default)
- Comment Required
- Unit in Station
- Additional ARL dispatch response time: ____ min ____ sec

  This is a time value that will be added to the response time of a unit in this status.

- Unit must be assigned to an incident.

  This check box only appears for the following categories: Acknowledged, Assigned, At Scene, At Other, Enroute, Other Activity, or To Other. For the Acknowledged category, the default state for the check box is selected and the check box is always disabled. For the other categories, the default state of the check box is unselected and the check box is enabled.

The following fields may also display, depending on the selection:

- Out of Vehicle Status
- To other location description
- Cross-staffed unit still available
- At other location description
- Display status as blank

Adding Unit Status Code Timeout Information

Add timeout information for each priority of a unit status code after you add the properties information. You can also configure the timeout information any time the unit is not on an incident. In addition, you can set a new status to take affect after the timeout.

Before adding unit status code timeout information, you must complete the steps in “Adding Unit Status Code Properties Information” on page 10-11.

To add unit status code timeout information:

1. Access the form for new unit status codes. For instructions, see “Adding Unit Status Codes” on page 10-11.

   The Unit Status Codes form appears with the Properties tab in focus (see Figure 10-7). A list of existing status codes and their descriptions displays on the left side of the form.

2. From the Unit Status Codes list on the left, select a status code.

3. Select the Timeouts tab.

4. Click **View/Modify**.

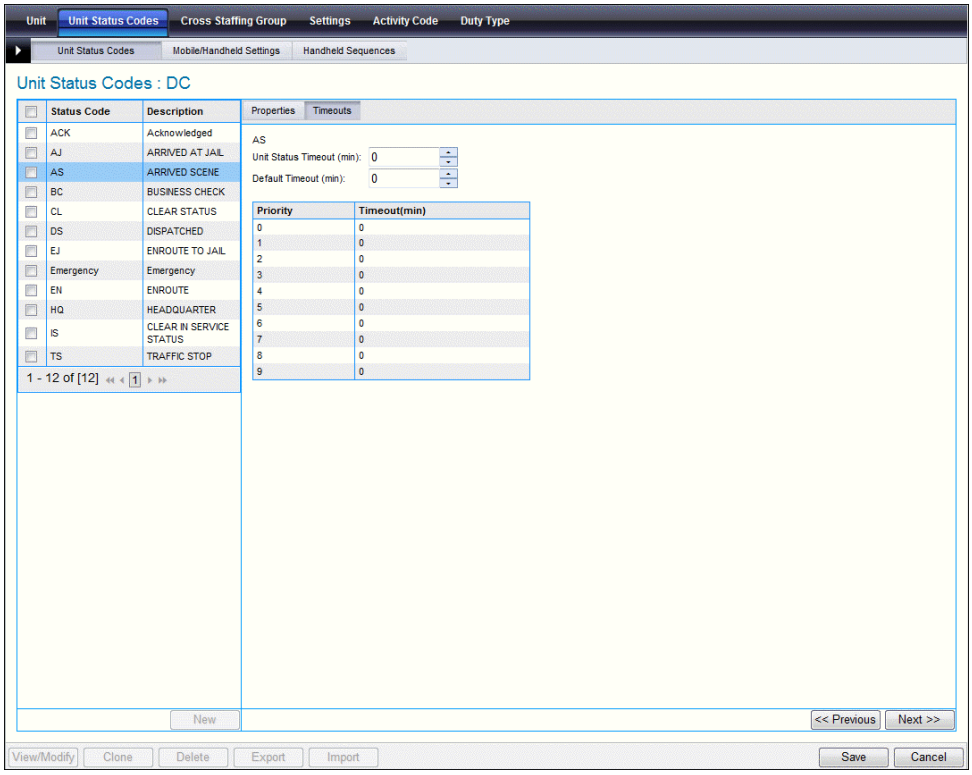


Figure 10-8 Unit Status Codes – Timeout Settings

5. From the Unit Status Timeout (min) list, select a timeout value in minutes for the unit status. This field is a timeout for when the unit in this status is *not* assigned to an incident.

6. From the Default Timeout (min) list, select a default timeout for the unit status. This field acts as a timeout when the unit in this status *is* assigned to an incident.

NOTE

If you do not want a status to timeout, leave timers set to zero.

---

7. In the table, select a priority timeout. Click in the field to change the timeout value.

8. Repeat this step for each priority.

   A priority timeout value is the amount of time a unit can be in this status for each of the priorities before being flagged as being timed out. If the value is zero, the time in the Default Timeout field applies.

9. Click **Save**.

Adding Mobile/Handheld Status Codes

Use the Unit Status Code Mobile/Handheld Settings tab when you want to set or change the display order of status codes in the Mobile or Handheld client. From this screen you can also set the status options upon Mobile/Handheld logoff; for example, if you want an officer to remain on duty in the CAD system while in court, or for a fire crew to remain on duty while in the station.

To add Mobile/Handheld status codes:

1. From the navigation panel, select **Unit Management**, then select **Unit Status Codes.**

2. Select **Mobile/Handheld Settings**.

   The Mobile/Handheld Settings form appears.

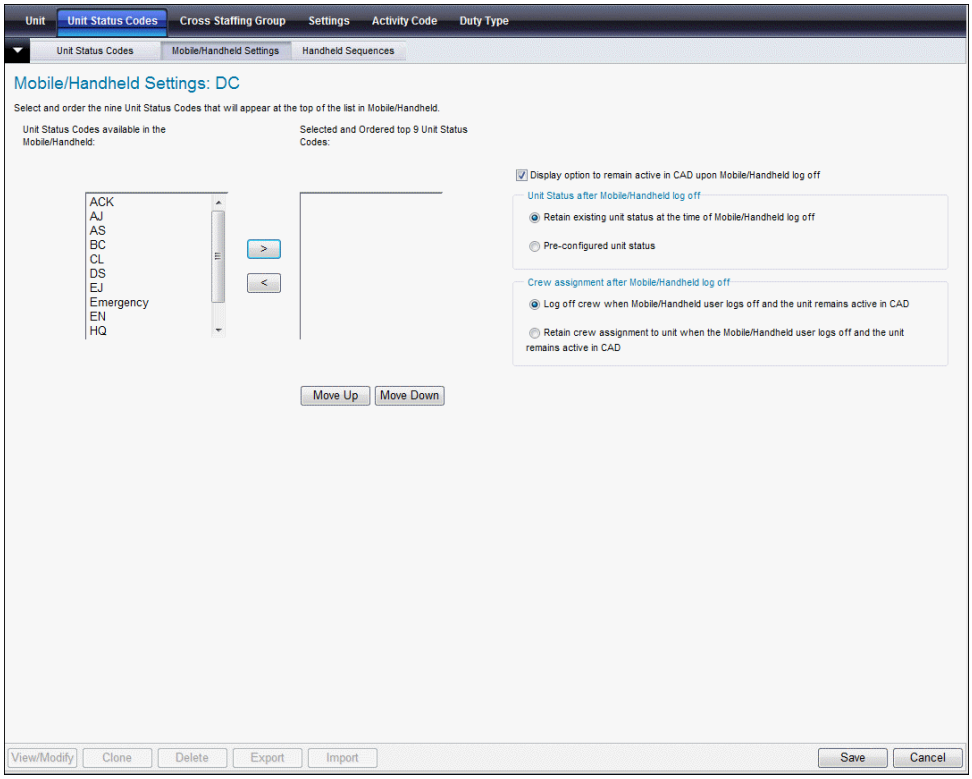


Figure 10-9 Unit Status Codes – Mobile/Handheld Settings Form

3. Click **View/Modify**.

4. From the Unit Status Codes Available in the Mobile/Handheld list on the left, select up to nine unit status codes that you want to appear at the top of the Unit Status Codes list in the Mobile or Handheld client. If fewer than nine status codes are entered here, the client will display other system status codes to complete the list.

NOTES

Motorola Solutions recommends that you always provision the **Emergency** status code to be in the first position in this list, so that it will appear at the top of the Unit Status Codes list in the Mobile or Handheld client.

5. Click the right arrow to move your selected unit status codes to the Selected and Ordered top 9 Unit Status Codes list on the right.

6. To change the order of the status codes in the Selected and Ordered top 9 Unit Status Codes list, do the following:

   a. Select a status code you want to move.

   b. To move that status code up or down in the list, click **Move Up** or **Move Down**.

   c. Repeat for each unit status code you want to move.

   This is the order in which the codes will display in the Mobile/Handheld unit.

7. If you want Mobile users to have the ability to stay active in CAD when they log off, select the **Display option to remain active in CAD upon Mobile/Handheld log off** check box.

8. Do one of the following to set the unit status of the Mobile/Handheld unit when it is logged off:

   - Retain the existing unit status at the time of log off. This is the default.
   - Use a pre-configured unit status. If you select this option, a selection list appears.

9. If there is a crew involved, set the Crew assignments for the log off.

   - Log off crew when Mobile/Handheld user logs off and the unit remains active in CAD
   - Retain crew assignment to unit when the Mobile/Handheld user logs off and the unit remains active in CAD.

10. Click **Save**.

Configuring Handheld Status Code Sequences

PremierOne Handheld users need an easy way to update their unit status from the current status. For instance, if a unit is dispatched with one “Accident” call, then the most likely status flow would be *Dispatched > Enroute > At Scene > Clear.* So if the unit is in “Dispatched” Status, then the client provides a single-click option to change the status from “Dispatched” to “Enroute” rather than requiring the officer to display all unit statuses and select the “Enroute” status from the list.

The Handheld client also provides a way to select one of the available unit statuses (selecting one of the statuses from the list) if the provisioned sequence is not appropriate to the Handheld user. Because different agencies use different status flows, PremierOne provides the option to provision the unit status sequence at the agency level.

PremierOne provides the option to select the Unit statuses (Mobile Unit statuses) and provide the way to sequence the selected unit statuses (Ex: “DS”->”EN”->”AS”->”CL”). The administrator can also provide the option to view the existing sequence flows and provide the option to update the sequence. After the system is provisioned with required sequencing, then it sends this sequencing along with all provisioned Mobile unit statuses to Handheld client.

To modify the Handheld status code sequence:

1. From the navigation panel, select **Unit Management**, then select **Unit Status Codes.**

2. Select **Handheld Sequences.**

The Handheld Sequences form appears.

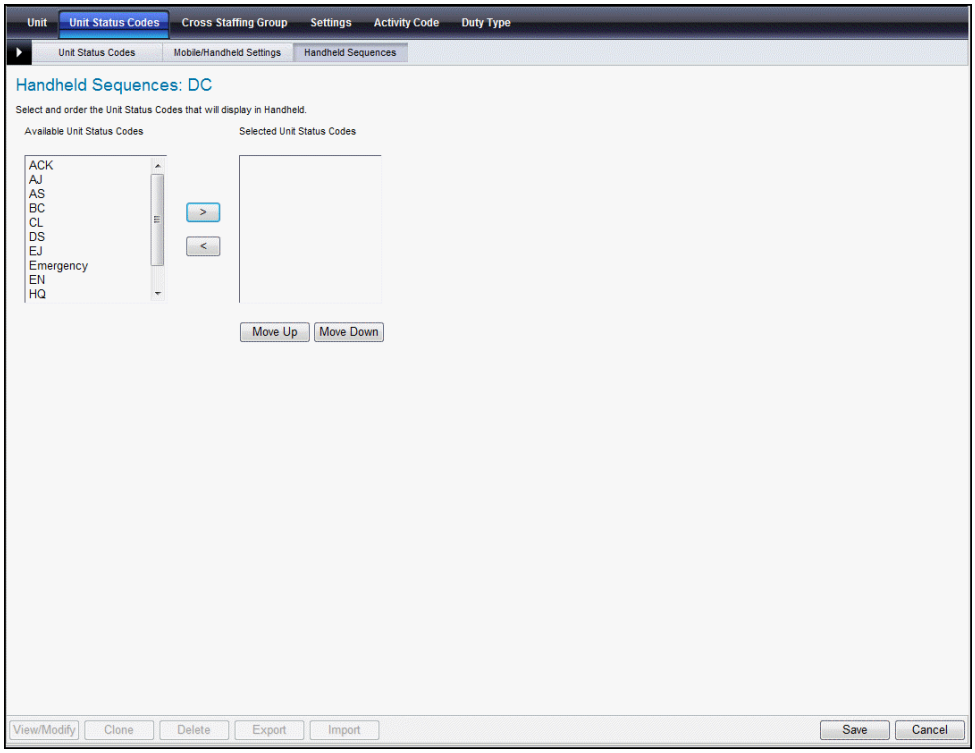


Figure 10-10 Unit Status Codes – Handheld Sequences Screen

3. Click **View/Modify**.

4. From the Available Unit Status Codes list on the left, select the status codes that you want to appear at the top of the list in Handheld.

5. Click the right arrow to move your selected unit status codes to the Selected Unit Status Codes list on the right.

6. To change the order of the status codes in the Selected Unit Status Codes list on the right, do the following:

   a. Select a status code you want to move.

   b. To move that status code up or down in the list, click **Move Up** or **Move Down**.

   c. Repeat for each unit status code you want to move.

   This is the order in which the codes will display in the Handheld unit.

Configuring Cross Staffing Groups

A cross staffing group is a set of units with a group name. With cross staffing, you can apply special availability rules to a single crew that staffs multiple units. When any of the units in a cross staffing group is assigned to an incident or becomes unavailable for any other reason, PremierOne CAD places all of the other units in the cross-staffing group in a configured unavailable status.

Use the Unit Management Cross Staffing Group configuration item to assign names to cross staffing groups and to assign units to the groups.

Understanding Cross Staffing and Unit Status

In most circumstances, when a crew leaves with a unit that is cross staffed, all other units in that cross staff group become unavailable. However, if one of the other units is already in an administrative status, such as OOS (Out of Service), this unit would remain in its current status.

Dependency: Status = Unavailable to Cross Staffing (For more information, see “Configuring Unit Status Transaction” on page 10-24.)

PremierOne updates each unit individually based on the following table:

Table 10-1 Cross-Staffing and Status

Action Against One Unit Within a Cross-Staffing Group	Affect On Other Units Within the Cross-Staffing Group	
	If the Current Status Is	Then the Resulting Status Would Be
Unit is dispatched onto an incident.	Clear	Status provisioned as: Unavailable Due to Cross Staffing
	Any Other Status	Current Status (No Change)
Unit is placed into a Clear Status	Status provisioned as: Unavailable Due to Cross Staffing	Clear
	Any Other Status	Current Status (No Change)
Unit is placed into any of the following: Acknowledged, Assigned, At Other, At Scene, Enroute, To Other	Clear	Status provisioned as: Unavailable Due to Cross Staffing
	Any Other Status	Current Status (No Change)
Unit is placed into an Admin or Other Activity status code that is provisioned as: Cross-Staffed Units Still Available = Yes	Any Status	Current Status (No Change)

Table 10-1 Cross-Staffing and Status

Action Against One Unit Within a Cross-Staffing Group	Affect On Other Units Within the Cross-Staffing Group	
	If the Current Status Is	Then the Resulting Status Would Be
Unit is placed into any status code that is provisioned as: Cross-Staffed Units Still Available = No This includes all status codes belonging to any other category outside of admin or Other Activity.	Clear	Status provisioned as: Unavailable Due to Cross Staffing
	Any Other Status	Current Status (No Change)

Adding Cross Staffing Groups

Cross staffing groups consist of the group name and the unit IDs of the units belong to the group.

To add a cross staffing group:

1. From the navigation panel, select **Unit Management**, and then select **Cross Staffing Group**.

   The Cross Staffing Group form appears.

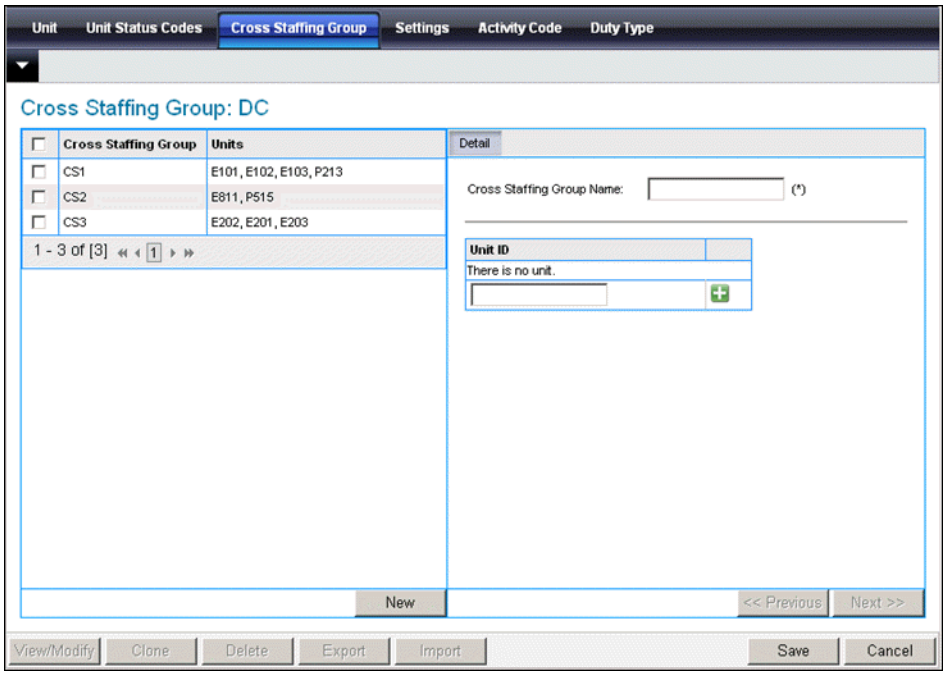


Figure 10-11 Cross Staffing Group Form

2. Click the **New** button on the left below the list of cross staffing groups.

3. In the Cross Staffing Group Name field, type a name for your new group. The name must be unique within your agency.

4. In the Unit ID field, type the ID for the unit to add to this group, and then press **Enter** or click the plus symbol at the end of the row.

> **CAUTION**
> If you do not click the plus symbol or press **Enter**, PremierOne does not save the cross staffing information, even after you click Save.

5. Continue adding Unit IDs and pressing **Enter** or clicking the plus symbol until you have listed all the units for this group. When you have added all of the units to this staffing group, you should have a blank row at the end.

6. Click **Save**.

Configuring Unit Management Settings

Use the Unit Management Settings configuration item to do the following:

- Command Line – Set what the number specified on the command line represents: the incident number or the unit's call sign.
- Shift ID Codes – Change or delete the shift ID code, description, or the activation time.
- Transactions – Change the association between a transaction and its default unit status.

Configuring Command Line Numbers

Configure command line information when you need to change what a number entered on the command line represents: the incident number or the unit's call sign. By default, numbers are assumed to be the unit's call sign and incidents are referenced as `#incnum`.

To configure command line numbers:

1. From the navigation panel, select **Unit Management**, then select **Settings**, and then select **Command Line**.

   The Command Line form appears.

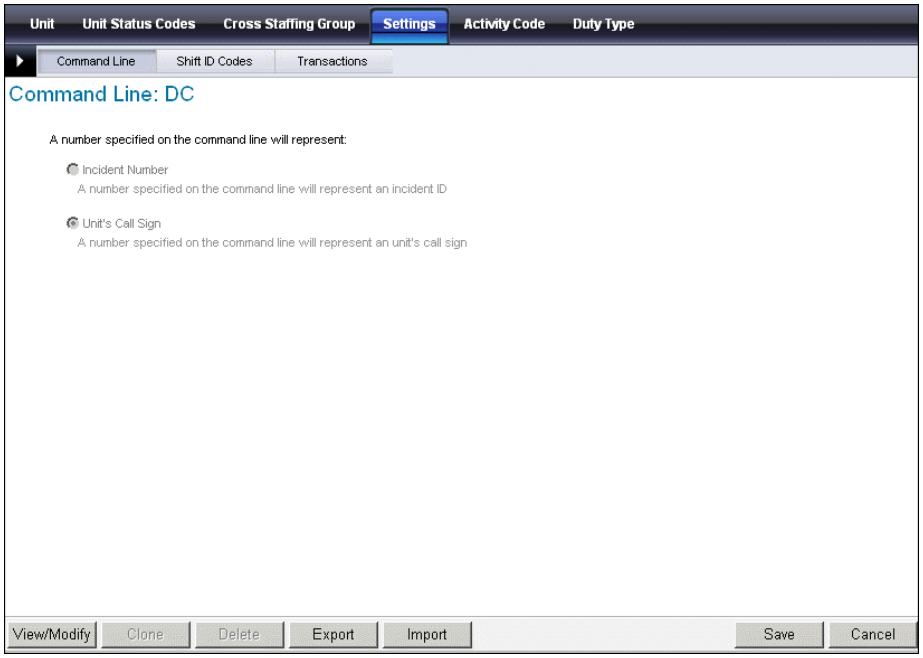


Figure 10-12 Command Line Form

2. Click **View/Modify**.

3. Select whether you want the incident number or the unit call sign to take precedence on the command line.

   If you select **Incident Number**, when a user types a unit ID in a command line that calls for incident number or unit ID, the user will need to precede the unit ID with the # symbol.

   If you select **Unit's Call Sign**, when a user types an incident number in a command line that calls for incident number or unit ID, the user will need to precede the incident number with the # symbol.

4. Click **Save**.

Configuring Shift ID Code Information

Shift ID code controls the Shift ID that is used and the activation time.

To configure shift ID code information:

1. From the navigation panel, select **Unit Management**, then select **Settings**, and then select **Shift ID Codes**.

   The Shift ID Codes form appears.

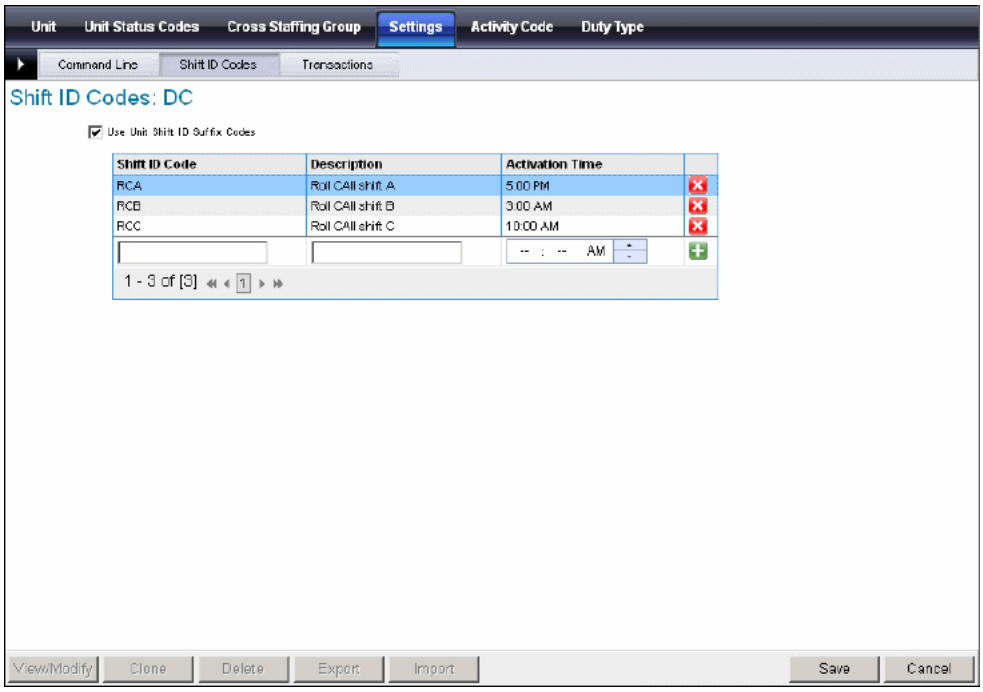


Figure 10-13 Shift ID Codes Form

2. Click **View/Modify**.
3. Select whether your agency will use unit shift ID suffix codes.

   Example:

   If the unit ID is 1A12 and the shift ID is C, with a unit shift ID suffix code, the unit ID would appear as 1A12C.

4. In the blank Shift ID Code field, type the name of the new code.
5. In the blank Description field, type a short description for the code.
6. In the blank Activation Time field, select the time the shift will be activated.

7. Click the plus symbol at the end of the row or press **Enter** to save the shift ID information and add another row.

> **CAUTION**
> If you do not click the plus symbol or press **Enter**, PremierOne does not save the shift ID information, even after you click Save.

8. Click **Save**.

Configuring Unit Status Transaction

The unit transaction indicates the status to use for a unit when a specific unit transaction occurs. Transaction information can also include additional related properties, such as whether status changes are confirmed, whether odometer readings are required, requirements for emergency status, and so on.

You configure the actual unit statuses in the Unit Status Codes configuration item. When you create unit statuses, you must assign them to a specific category. Categories consist of the following:

- Acknowledged
- Administrative
- Assigned
- At Other
- At Scene
- Clear
- Enroute
- Other Activity
- To other

For additional details, see “Configuring Unit Status Codes” on page 10-11.

With the exception of the First Pass of Two Pass Traffic Stop, each unit transaction has only the unit statuses in one category available to it.

To configure transaction information:

1. From the navigation panel, select **Unit Management**, then select **Settings**, and then select **Transactions**.

   The Transaction form appears.

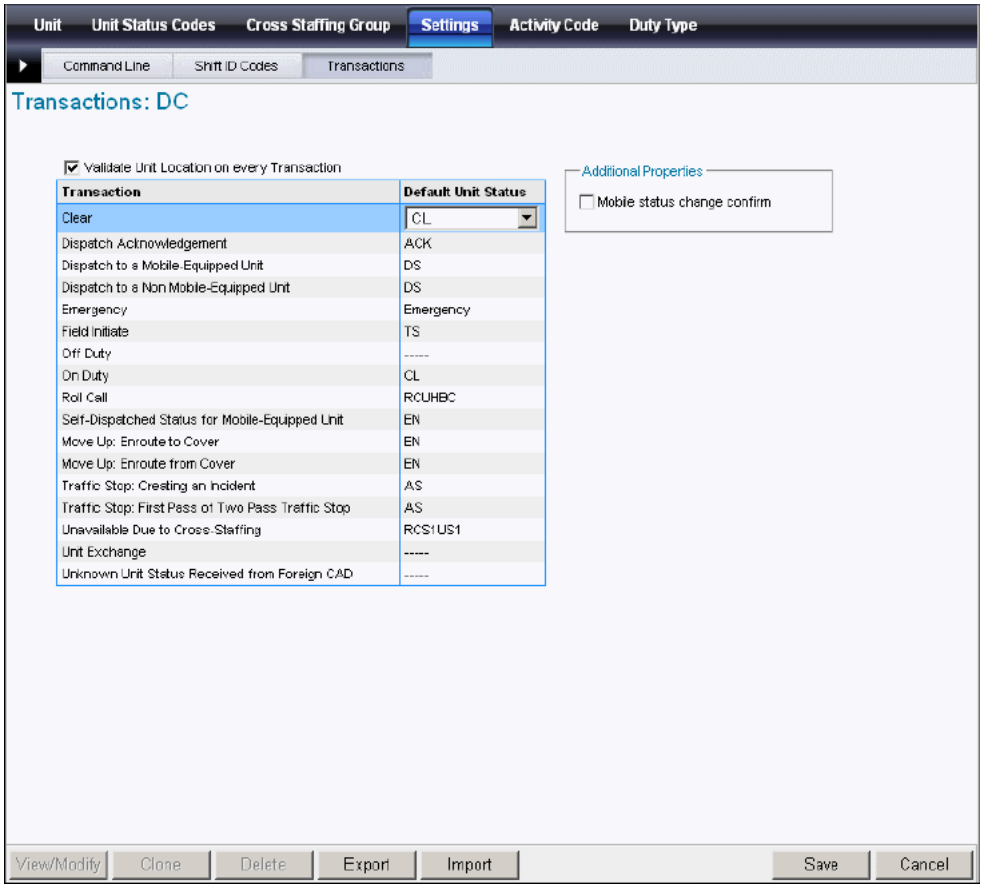


Figure 10-14 Transactions Form

2. Click **View/Modify**.

3. Select the **Validate Unit Location on Every Transaction** check box to require that unit status commands that include a location are verified in a separate step when the command is submitted.

4. From the Clear row, select the status for a unit in a clear status. Available statuses in this list belong to the Clear category of unit statuses.

   The Additional Property, Mobile Status Change Confirm, is reserved for future functionality.

5. From the Dispatch Acknowledgment row, select the status for a unit that acknowledges a dispatch. Available statuses in this list belong to the Acknowledgement category of unit statuses.

6. From the Mobile-Equipped Unit row, select the status for a unit that is equipped with a mobile computer and dispatched to an incident. Available statuses in this list belong to the Assigned category of unit statuses.

7. From the Dispatch to a Non Mobile-Equipped Unit row, select the status for a unit that is not equipped with a mobile computer and is dispatched to an incident. Available statuses in this list belongs to the Assigned or Enroute category of unit statuses.

8. From the Emergency row, select the status for a unit in emergency status. Available statuses in this list belong to the Other Activity category of unit statuses.

   The additional properties are not yet functional.

   - Mobile Status Change confirm
   - Emergency Confirm Type
   - Emergency alert nearby units
   - Emergency - must create an incident
   - Emergency silent signal
   - Emergency fake cancellation
   - Send emergency notification
   - Emergency broadcast time
   - Emergency notification distance

9. From the Field Initiate row, select the status for a unit assigned to a field-initiated incident. Available statuses in this list belong to the Arrived Scene category of unit statuses.

10. From the Off Duty row, select the status unit status for an off duty unity. or a unit assigned to a field-initiated incident. Available statuses in this list belong to the Arrived Scene category of unit statuses.

    Select any of the following additional properties:

    - Require odometer reading – Require an odometer reading when the unit is placed on duty.
    - Validate odometer – Validate the odometer reading when the unit is taken off duty.

      The Validate odometer field is available only when the Require odometer check box is selected.

- Deferred off duty allowed – Allow a unit to be placed in a deferred off duty status while it assigned to an incident. Once the unit clears from the incident, it is automatically taken off duty.

NOTE

A local agency can provision a unit status code at the agency level to be sent to all external systems provisioned to receive unit status updates whenever the local agency's unit is placed off duty. To provision the update, see "Configuring Local Agency Settings" on page 22-24.

- Mobile Status Change Confirm– Reserved for future functionality.

11. From the On Duty row, select the status for a unit that is placed on duty. Available statuses in this list belong Clear category of unit statuses.

    Additional properties include the following:

    - Mobile Status Change Confirm – Reserved for future functionality.
    - Require personnel – Require personnel to place the unit on duty.
    - Require odometer – Require an odometer reading when the unit is placed on duty.
    - Validate odometer – Validate the odometer reading when the unit is placed on duty.

      The Validate odometer field is available only when the Require odometer check box is selected.
    - Validate unit ID – Validate the unit ID when the unit is placed on duty.

      NOTE

      If you select Yes for validate unit ID, only preconfigured units can be placed on duty (see "Adding Unit IDs" on page 10-2).

    - Include names in unit history – Include the personnel names in the unit history.

12. From the Roll Call row, select the status for a unit that is in an activated roll call. Available statuses in this list belong to the Administrative category of unit statuses.

    The Additional Property, Mobile Status Change Confirm, is reserved for future functionality.

13. From the Self-Dispatched Status for a Mobile-Equipped Unit, select a status for mobile-equipped unit that has dispatched themselves to an incident. Available statuses in this list belong to the Enroute category of unit statuses.

    The Additional Property, Mobile Status Change Confirm, is reserved for future functionality.

14. From the Move Up: Enroute to Cover row, select the status for a unit that is enroute to cover another station or area. Available statuses in this list belong to the Enroute category of unit statuses.

    For more information on move ups, see "Configuring Move Ups" on page 10-32.

15. From the Move Up: Enroute From Uncover row, select the status for a unit that is enroute from covering another station or area. Available statuses in this list belong to the Enroute category of unit statuses.

16. From the Traffic stop: Creating an incident row, select the status for a a unit assigned to a traffic stop.Available statuses in this list belong to the Arrived Scene category of unit statuses.

    This status is used when an incident is created on the first pass *or* second pass of a traffic stop.

    The Additional Property, Mobile Status Change Confirm, is reserved for future functionality.

17. From the Traffic stop: First Pass of Two Pass Traffic Stop row, select the status for a unit that is assigned to the first pass of a two-pass traffic stop. Available statuses in this list belong belongs to the Assigned or At Scene category of unit statuses.

    An incident is not created in this situation, but the unit is placed into this unit status code.

    The Additional Property, Mobile Status Change Confirm, is reserved for future functionality.

18. From the Unavailable due to Cross-Staffing row, select the status for a unit that is unavailable due to cross-staffing. Available statuses in this list belong to the Administrative category of unit statuses.

    The Additional Property, Mobile Status Change Confirm, is reserved for future functionality.

    For details on cross staffing, see "Configuring Cross Staffing Groups" on page 10-19.

19. From the Unit exchange properties, select any of the following properties:

    - Comment – Require the dispatcher to enter a comment when issuing the UX command.
    - Mobile Status Change Confirm – Reserved for future functionality.

20. From the Unknown Unit Status Received from Foreign CAD row, select the default unit status to use when receiving an unknown unit status update from a foreign CAD system.

Configuring Activity Codes

Use the Unit Management Activity Code configuration item to manage the activity codes for units. Activity codes are codes that are used to categorize activity and time spent by units other than the time tracked by unit status codes, such as special DUI patrols.

You can add, modify, export, import, and delete activity codes. For details on modifying, exporting, importing, and deleting codes, see "Working With Configuration Items" on page 2-9.

Adding Activity Codes

Add codes when the activity codes you already have do not meet your needs. You cannot modify an activity code. To change an activity code, you must delete and then re-add the record.

To add an activity code:

1. From the navigation panel, select **Unit Management**, and then select **Activity Code**.

   The Activity Code form appears.

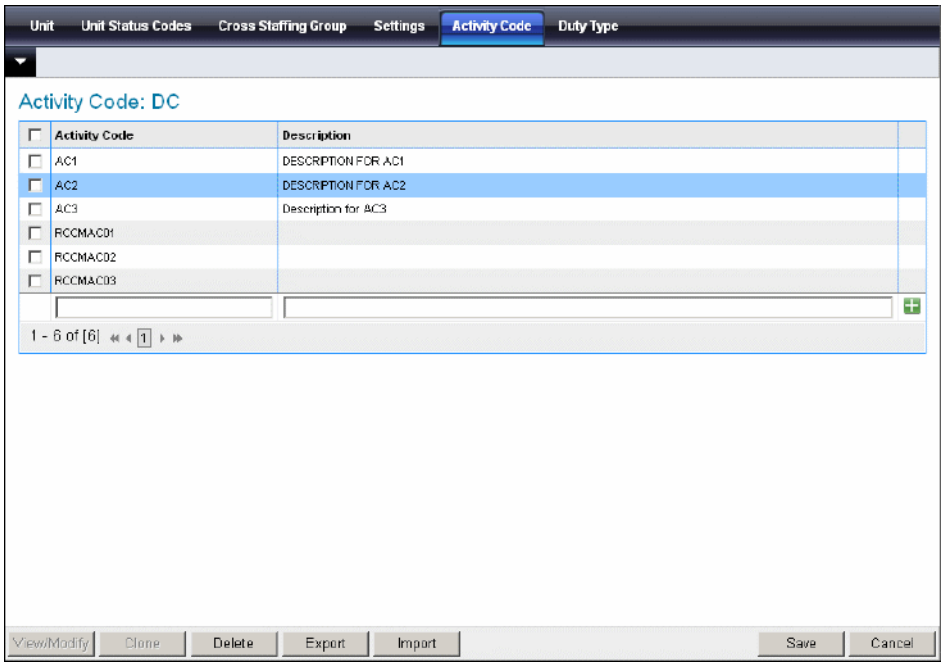


Figure 10-15 Activity Code Form

2. Click **View Modify**.

3. In the blank Activity Code field, type a new code.

   Activity codes must be unique within an agency but do not have to be unique between agencies.

4. In the blank Description field, type a short description for the code.

5. Click the plus symbol at the end of the row or press **Enter** to temporarily save the code and description and add another row.

   The new code and description display in blue to indication that they have not been permanently saved.

6. Click **Save**.

   The new codes and descriptions now display in black to indicate that they have been saved.

Configuring Duty Types

Use the Duty Type configuration item to manage duty types for units at the agency level.

Duty types allow an agency to categorize the units into their assigned equipment and purpose or the typical use of the unit. This is especially valuable for fire agencies, because fire agencies have many categories for their units.

Examples:

Duty types for fire agencies:

ENGINE could be assigned to basic fire fighting units that respond to all types of rescues, fires, and medical calls.

RESCUE could be assigned to units that respond to all hazardous material calls, rescue alarms, and structure fires where the crew is utilized for command staff support.

Duty types for medical agencies:

MEDIC could be used for ALS units with patient transport capability.

SQUAD could be used for ALS units without patient transport capability.

Duty types for law agencies:

PATROL could be used for all normal response (Patrol) units.

K9 could be used for units with a dog.

DET could be used for units with a detective.

CS could be used for crime scene units.

You can add, modify, export, import, and delete duty types. For details on modifying, exporting, importing, and deleting codes, see “Working With Configuration Items” on page 2-9.

Adding Duty Types

Add a duty type when the existing duty type codes do not meet your needs.

To add a duty type:

1. From the navigation panel, select **Unit Management**, and then select **Duty Type**.

   The Duty Type form appears. A list of existing records displays on the left side of the form.

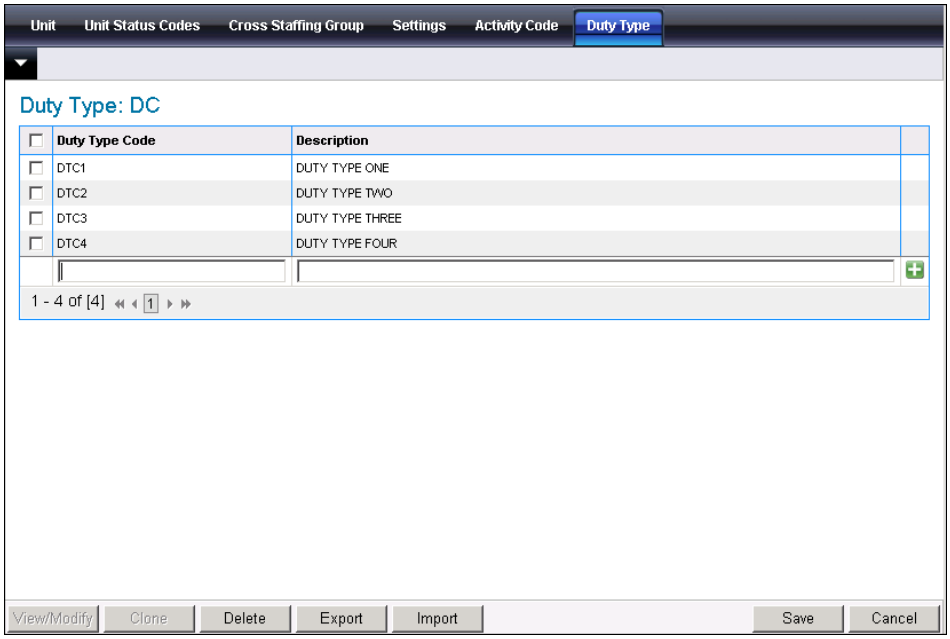


Figure 10-16 Duty Type Form

2. Click **View/Modify**.

3. In the blank Duty Type Code field at the bottom of the list, type your new duty type code.

4. In the blank Description field, type a description for your new duty type code.

5. Press **Enter** or click the plus icon at the end of the row to temporarily save your new duty type code and description.

6. Continue adding codes and descriptions.

7. Click **Save** to permanently save your codes and descriptions.

Configuring Move Ups

The Move Up command (MU) allows dispatchers to replenish stations or areas that have been depleted of resources (for example, a station that sends all of its units to fight a fire). Dispatchers can “move up” one or more units to temporarily replace the resources that are away from a station or area. During the time a unit is assigned to a temporary station or area through the use of the MU command, the system treats the unit as though its “home” assignment is the temporary station or area assigned by the move up.

An agency must be provisioned to use either stations or areas for the recommendation assignments of the agency’s units. A single agency cannot mix the assignments of stations and areas. Depending on how an agency is provisioned, the MU command specifies coverage of the same entity provisioned for that agency (stations or areas).

No specific provisioning is required for a dispatcher to use the MU command to move up a unit successfully. However, for tracking purposes, you can configure PremierOne to create an incident when the MU command is executed. If you choose this option, you must provision an incident type that will be assigned to move ups, a default modifying circumstance for the move up incident type, a default disposition for move up incidents, and the status a unit will be placed in when enroute to or from a move up incident. You can also configure PremierOne to automatically send paging, toning, tear and run, and printing agency alerts when a move up occurs.

A move up incident is created as a closed incident with the unit(s) specified in the MU command associated to the incident. The provisioned disposition is assigned to the closed incident. The incident does not require any action by the dispatcher to be closed.

If you are working in a multi-agency environment, you must provision incident creation for each agency. By doing so, when a move up occurs, an incident is created for each agency owning units that are being moved up.

To configure incident creation and auto-alerting for the Move Up command:

1. If an appropriate incident type for move up incidents does not already exist, create a new incident type for move ups.

   For details, see “Adding Incident Type Codes” on page 13-4.

2. If an appropriate modifying circumstance for move up incidents does not already exist, create a new modifying circumstance for move up incidents.

   For details, see "Adding Modifying Circumstances Codes" on page 13-8.

3. If appropriate unit status codes for Move Up – Enroute to Cover and Move Up – Enroute from Cover transactions do not already exist, create new unit status codes for these transactions.

   For details, see "Adding Unit Status Codes" on page 10-11.

> **NOTE**
> You can provision an icon indicating the unit's moved-up status to display on the Unit Status Monitor and on the Status tab of the Unit Summary screen. For details, see "Configuring CAD Status Monitor Icons" on page 32-3.

4. Configure the creation of an incident when a move up is executed.

   a. From the navigation panel, select **Incident Management**, and then select **Service Settings**.

      The Service Settings form appears with the Service Defaults tab in focus.

   b. Select the Initiation Defaults tab.

      The Initiation Defaults form appears (Figure 10-17).

   c. Click **View/Modify**.

   d. In the Initiation Defaults form, scroll to the Move Up Incidents section.

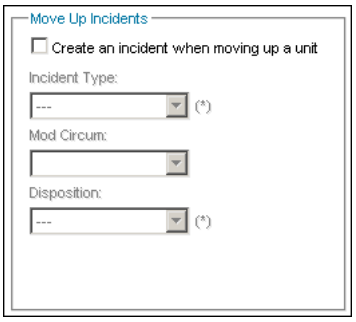


Figure 10-17 Initiation Defaults Form – Move Up Incidents Section

   e. In the Move Up Incidents section, select the **Create an incident when moving up a unit** check box.

      The Move Up Incident Type, Move Up Modifying Circ., and Move Up Disposition list boxes become enabled.

   f. From the Move Up Incident Type list, select the incident type that will be associated by default with move up incidents.

g. From the Move Up Modifying Circ. list, select the modifying circumstance that will be associated by default with the move up incident type.

h. From the Move Up Disposition list, select the disposition that will be associated by default with move up incidents.

i. Click **Save**.

5. Provision the status a unit will be placed in when enroute to or from a move up incident.

   a. From the navigation panel, select **Unit Management**, then select **Settings**, and then select **Transactions**.

      The Transactions form appears with a list of transactions and the default unit status associated with each.

   b. Click **View/Modify**.

   c. Select the **Move Up: Enroute to Cover** transaction.

   d. From the Default Unit Status list, select the unit status that will be assigned by default to the **Move Up: Enroute to Cover** transaction.

   e. Select the **Move Up: Enroute from Cover** transaction.

   f. From the Default Unit Status list, select the unit status that will be assigned by default to the **Move Up: Enroute from Cover** transaction.

NOTE

An icon may be configured by your agency to display on the Unit Status Monitor when a unit is in moved-up status. This icon also appears on the Status tab of the Unit Status screen. For details, see “Configuring CAD Status Monitor Icons” on page 32-3.

6. Provision whether paging, toning, tear and run, and printing agency alerts will be automatically sent when a move up occurs.

NOTES

Agencies must be configured to use stations for move up alerting to work.

A unit must be in station and in dispatchable status to be toned.

a. From the navigation panel, select **Interfaces**, then select **Alerting**, and then select **Settings**.

The Settings tab appears.

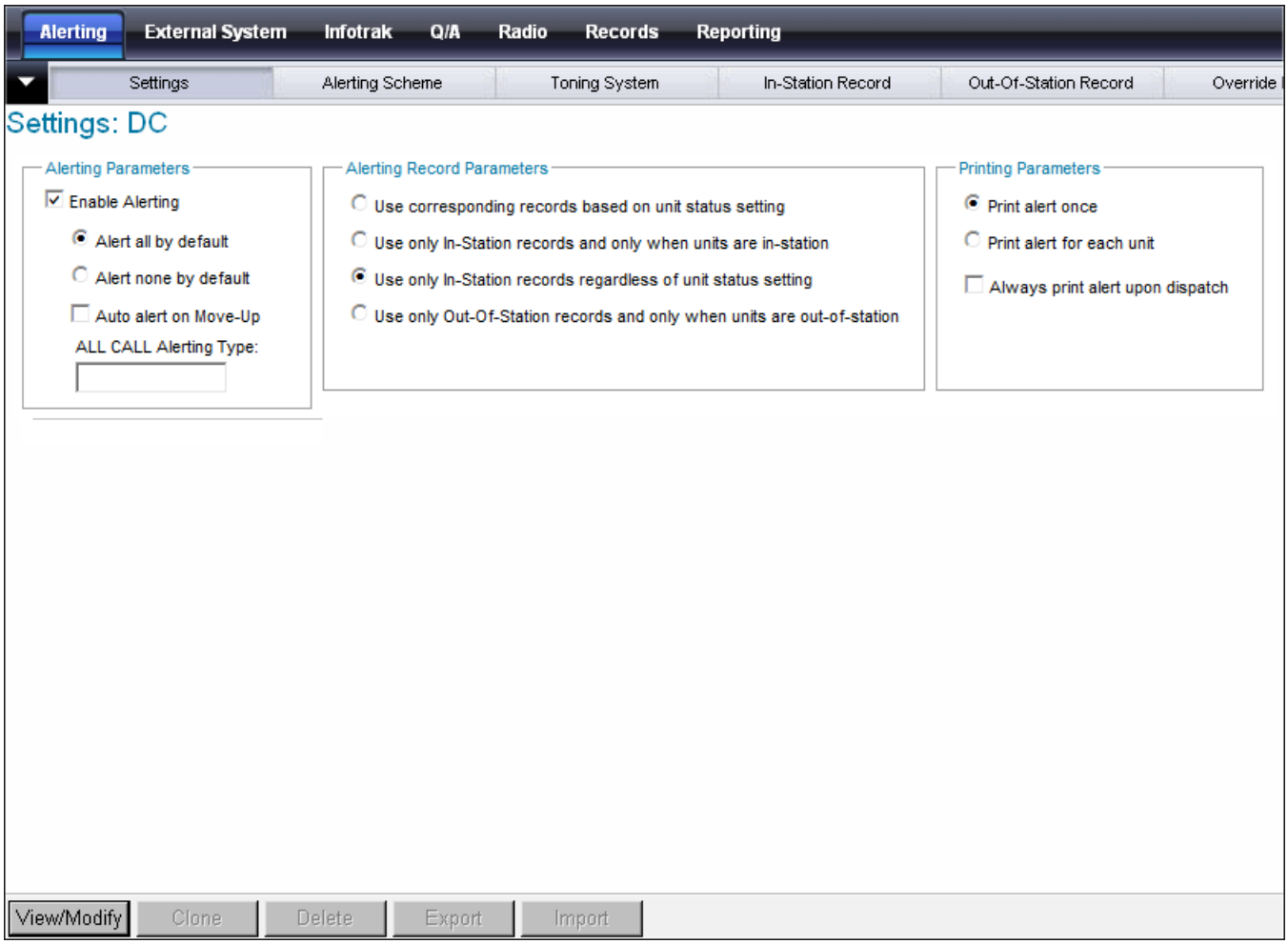


Figure 10-18 Settings Tab

b. Click **View/Modify**.

c. In the Alerting Parameters section, select the Auto alert on Move-Up check box.

NOTES

An agency must be configured to use stations for move up alerting to work.

A CAD user can override the Auto Alert setting when entering the Move Up command. For more information, see “Reassigning Units With the Move Up Command (MU)” in the PremierOne *CAD User Guide*.

d. To set how to handle the printing of alerts for move ups, in the Printing Parameters section, do the following:

Select one of the following:

- Print Alert Once

  Send one copy of the incident information to each configured printer.

- Print alert for each unit

  Send one copy of the incident information for each unit to each configured printer if the unit is in the station.

Additionally, select the following, if required.

- Always print alert upon dispatch

7. Click **Save**.

CHAPTER 11

Configuring Resources

The Resources configuration item contains the following items:

- Capability Group – Where you define common sets of capabilities for the various types of units that exist within your agency. For details, see “Configuring Capability Groups” on page 11-2.
- Capability/Skill – Where you define the capabilities and personnel skills to be assigned for units. For details, see “Configuring Capabilities/Skills” on page 11-4.
- Personnel – Where you set the details, contact information, roles, authorizations, and resource assignments for personnel. For details, see “Configuring Personnel” on page 11-7.
- Vehicle – Where you define vehicle type, description, capabilities and equipment. For details, see “Configuring Vehicles” on page 11-20.
- Device Profile – Where you create profiles for a device that control the maximum size of transactions or messages, whether two-Factor Authentication is used during signon, BOLO settings, messaging settings, incident information that is sent, hot hit notification that is sent, query responses that are sent, and whether emergency messages are sent to radios outside of the vehicle. For details, see “Configuring Device Profiles” on page 11-22.
- Device Types – Where you set general, login, printing, and permissions information for device types, such as an ASTRO radio, workstation, mobile unit, pager, radio, or PDA. For details, see “Configuring Device Types” on page 11-34.
- Devices – Where you configure individual devices, such as MDTs, workstations, and handheld devices. For details, see “Configuring Devices” on page 11-43.
- Systems – Where you add new 9-1-1, TDD, or other systems. For details, see “Configuring Systems” on page 11-67.

Configuring Capability Groups

Use the Capability Group configuration item to define common sets of capabilities for the various types of units that exist within your agency.

Example:

You define a capability group of 10 capabilities and then assign this group to multiple units. A change is required to the capabilities assigned to this group. You only have to perform that change on a single record.

You can add, modify, delete, import, and export capability groups. You are adding, modifying, deleting, exporting, or importing the entire capability group record rather than any portion such as deleting a selected capability. For information on modifying, exporting, importing, and deleting, see "Working With Configuration Items" on page 2-9.

When you import a capability group, you import the entire group including all of the capability codes associated with it. Therefore, if you are going to import *both* capability groups and capabilities/skills, you must do one of the following:

Remove the list of capability *codes* and all the other information except the column titles from the second tab of the spreadsheet before you import *Capability Groups*.

OR

Remove the list of capability *groups* and all of the other information except the column titles from the second tab of the spreadsheet except the column titles before you import *Capability Codes*.

You also must change the Agency ID(s) on the first tab, to match the agency ID of the agency to which you are importing the data.

If you do not change the Agency ID, you will receive a message stating "Capability group <name> already exists. File was not imported," or "Capability <name> already exists. File was not imported."

If you change the agency ID but do not remove the list of capability codes from the spreadsheet, you will receive a message stating "Import error on row 2 of the CapabilityGroupAssignment tab: <name> is not a valid value for CapabilityGroupCode." File was not imported," or "Import error on row 2 of the CapabilityAssignment tab: <name> is not a valid value for CapabilityCode." File was not imported."

Adding Capability Groups

Add capability groups when the capability groups you already have do not meet your needs.

To add a capability group:

1. From the navigation panel, select **Resources**, and then select **Capability Group**.

   The Capability Group form appears (Figure 11-1). A list of existing capability groups appears on the left side of the form and a list of all of your agency's provisioned capabilities appears in the Available Capabilities box in alphabetical order.

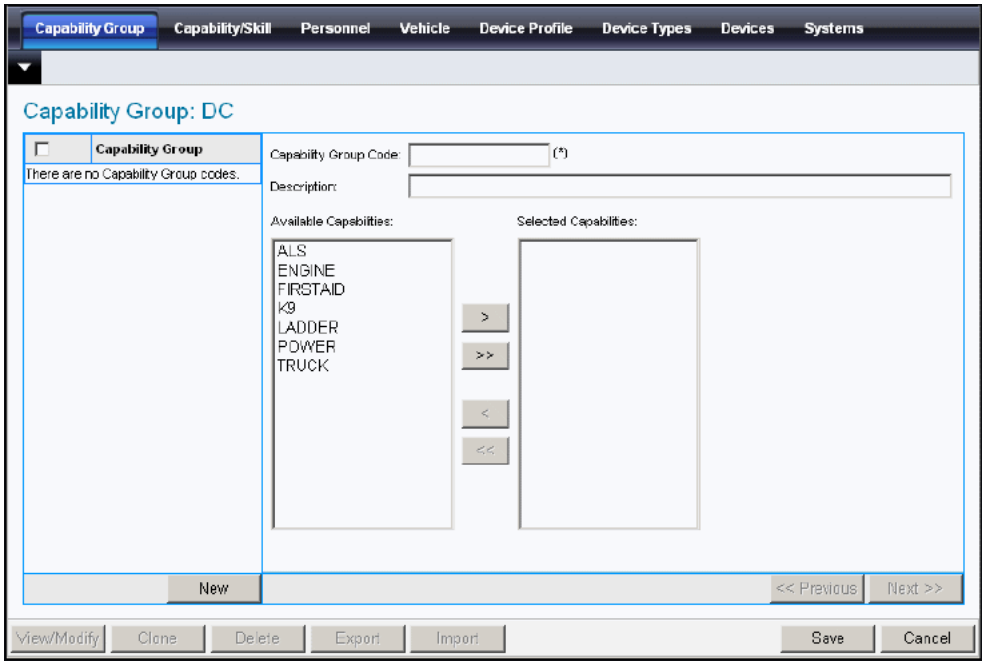


Figure 11-1 Capability Group Form

2. At the bottom of the Capability Groups list, click the **New** button.

3. In the Capability Group Code field, type the code for your new capability group. You can use a maximum of 10 characters.

4. In the Description field, type a description for the capability group.

5. From the Available Capabilities box, select the capabilities that you want associated with this capability group. Click the arrow to move your selected capabilities to the Selected Capabilities box.

6. Click **Save**.

Configuring Capabilities/Skills

Use the Capability/Skill configuration item to define the capabilities and personnel skills to be assigned for units.

Unit capabilities define all of the different characteristics that can be assigned to the unit based on the unit's ability to respond to different situations. This includes defining the type of vehicle that is assigned to the unit, such as an Engine, the equipment that is available on the vehicle, such as a Hurst tool, and the skills associated with the crew, such as negotiating skills.

You can add, modify, and delete capabilities. For details on modifying and deleting capabilities, see "Working With Configuration Items" on page 2-9.

NOTE

When you import a capability group, you import the entire group including all of the capability codes associated with it. Therefore, if you are going to import *both* capability groups and capabilities/skills, you must do one of the following:

Remove the list of capability *codes* and all the other information except the column titles from the second tab of the spreadsheet before you import *Capability Groups*.

OR

Remove the list of capability *groups* and all of the other information except the column titles from the second tab of the spreadsheet before you import *Capability Codes*.

You also must change the Agency ID(s) on the first tab, to match the agency ID of the agency to which you are importing the data.

If you do not change the Agency ID, you will receive a message stating "Capability group <name> already exists. File was not imported," or "Capability <name> already exists. File was not imported."

If you change the agency ID but do not remove the list of capability codes from the spreadsheet, you will receive a message stating "Import error on row 2 of the CapabilityGroupAssignment tab: <name> is not a valid value for CapabilityGroupCode." File was not imported," or "Import error on row 2 of the CapabilityAssignment tab: <name> is not a valid value for CapabilityCode." File was not imported."

You cannot change the capability code. If you want to change the capability code name, you must delete and re-add the record.

Capabilities Overview

Not every unit is capable of responding to all situations. Some units are able to respond to very basic situations based on their equipment or personnel, while others are more specialized.

Each unit that PremierOne can recommend must be provisioned with a complete set of capabilities. Users can manage these capabilities by selecting them or removing them. Each time a police unit goes on and off duty, the provisioned capabilities are refreshed.

Fire and medical units rarely go off duty, however their personnel assignments change and personnel have different skills. A skill is a personnel capability that is brought to a unit. Fire and medical units can break down causing those units to be temporarily unable to respond for a specific capability.

Provisioning Capabilities

Provisioning capabilities requires multiple steps. See the following list and the references to the sections that describe the steps in detail.

To provision capabilities:

1. Provision response categories. See “Adding Response Categories” on page 14-36.

   Response categories allow an agency to group similar unit capabilities together.

2. Provision capabilities. See “Adding Capabilities/Skills” on page 11-6.

   Capabilities include abilities, such as Advanced Life Support; equipment, such as a Hurst tool; and skills, such as fluency with a foreign language.

   When you provision capabilities, you assign a response category code to each capability. Each capability can have only one response category; however a response category may have multiple capabilities.

3. Return to response categories if you want to verify that your capabilities now appear in the Capabilities box. See “Adding Response Categories” on page 14-36.

4. Provision capability groups. See “Adding Capability Groups” on page 11-3.

   A capability group allows your agency to define a common set of capabilities for the various types of units that exist within your agency. This reduces the redundancy and maintenance of provisioning the same capabilities to each unit that may share these capabilities.

5. Provision duty types. See “Adding Duty Types” on page 10-31.

   Duty types are used to categorize units into their assigned purpose, such as rescue, engine, K9, or patrol.

6. Provision the Duty Type field on the Vehicle tab in Unit Preassignments. See “Configuring Unit Preassignments” on page 10-4.

   A unit can have only one duty type.

7. Provision capability groups on the Unit Capabilities tab in Unit Preassignments. See “Configuring Unit Preassignments” on page 10-4.

You can assign a group and/or individual capabilities.

A capability group may be assigned to more than one unit.

Adding Capabilities/Skills

Capabilities and skills are defined by a code and a response category. You can additionally designate a skill as a personnel skill and select capability groups to associate with the capability or skill.

To add a capability/skill:

1. From the navigation panel, select **Resources**, and then select **Capability/Skill**.

   The Capability/Skill form appears with a list of existing activity codes.

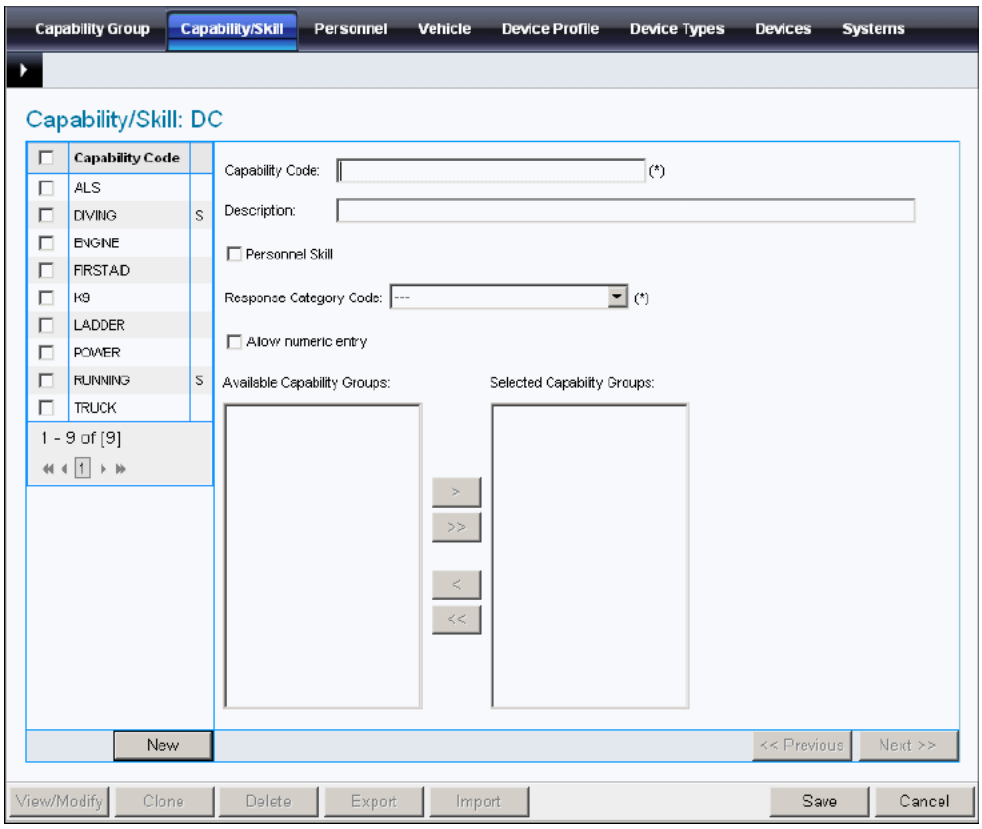


Figure 11-2 Capability/Skill Form

2. At the bottom of the Capability Code list, click the **New** button.
3. In the Capability Code field, type the new code.
4. In the Description field, type a short description for the code.

5. If the capability is a personnel skill, such as fluency in another language (SPANISH) or negotiation (NEGOT), rather than a vehicle or equipment capability such as 4X4 or HURST tool, select the Personnel Skill check box.

   If you check this field, PremierOne populates the Response Category Code field with the value SKILL and disables that field. PremierOne also disables the rest of the fields on the form because they are not applicable to personnel skills.

6. From the Response Category Code list, select the response category for this capability code.

   Response categories allow an agency to group similar unit capabilities together. Grouping capabilities together makes reviewing and maintaining a unit's capabilities much easier. For more information about response categories, see If you

7. In the Allow numeric entry field, indicate whether you want to accept numeric entry for the capability.

   The default for this field is unchecked or No.

   Example:

   An example of a numeric entry capability code would be Number of Paramedics.

8. From the Available Capability Groups box, select one or more capability groups to be associated with the capability. Click the arrow to move your selected groups to the Selected Capability Groups box.

   If you are configuring capabilities for the first time and have not yet configured capability groups, you will need to complete these steps, add your capability groups (see "Adding Capability Groups" on page 11-3), and then return to this step to add the capabilities.

9. Click **Save**.

Configuring Personnel

Use the personnel configuration item to manage personnel in your agency. Personnel information is contained in five tabs: Details, Contact Info, Roles, Authorization, and Resource Assignments.

You can add, modify, delete, and clone personnel records. For details on modifying, deleting, and cloning, see "Working With Configuration Items" on page 2-9.

Adding Personnel Records

When you add a personnel record, you enter information on the following tabs of the Personnel form:

- Details – Where you add or modify information about the person's name, user ID, user name, date of birth, ethnicity, sex, height, weight, blood type, supervisor, badge, rank, personnel ID, radio call sign, Social Security number, driver's license number, expiration date, and state of issue, account status, radio ID, and capabilities.
- Contact Info – Where you add or modify information about the person's email addresses, physical address, phone numbers, emergency contact, and any keywords.
- Roles – Where you select roles to assign to the person, such as call taker, dispatcher, or supervisor.
- Authorization – Where you control the person's login authorizations, login restrictions, and password.
- Resource Assignments – Where you assign equipment and vehicles.
- Preassignments – Where you make preassigned jurisdictional assignments for officers assigned to jurisdictions, not fixed Unit IDs, when they go on duty.

Adding Personnel Detail Information

Personnel detail information includes the person's name, User ID, skills, date of birth, rank, radio call sign, and other identifying information.

To add personnel detail information:

You access the Personnel form from the navigation panel. You can use the filter to enter the name of the person and the User ID. If you are unsure of the spelling of the name, type your best guess, and click Sound Alike to use the Soundex feature to find close matches. For details on using the filter display, see "Using Filters" on page 2-7.

You can also use the following wildcard characters in searches:

% any string of zero or more characters

_ any single character

[ ] any single character within the specified range

[^] any single character not within the specified range

1. From the navigation panel, select **Resources**, and then select **Personnel**.

The Personnel form appears. A list of existing records displays on the left side of the form.

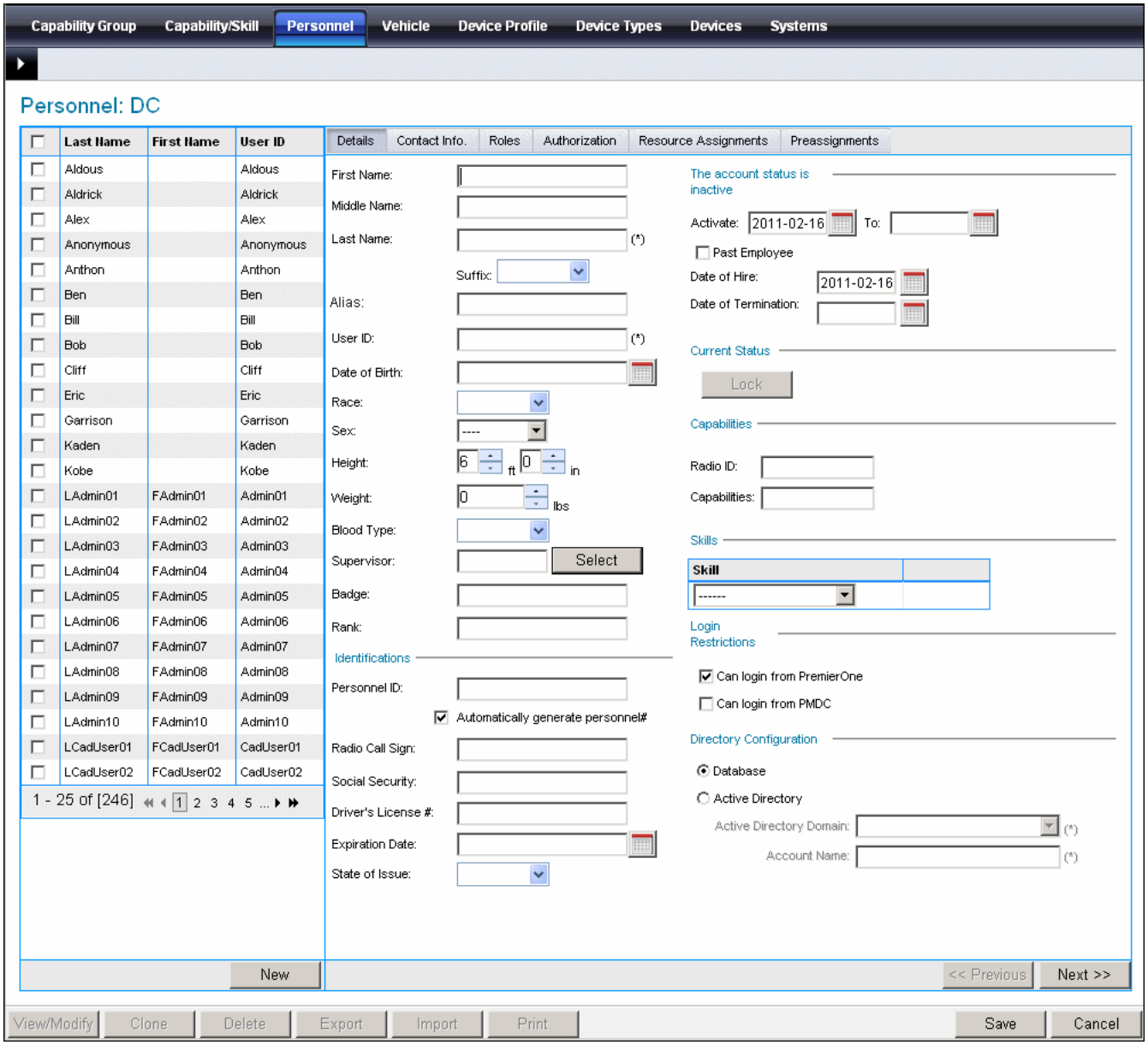


Figure 11-3 Personnel Form – Details Tab

2. At the bottom of the personnel record list, click the **New** button.

   The Personnel tab appears.

3. Enter as much personnel information as possible in the Details tab.

   The User ID and User Name fields are required. The User ID is the ID the person will use when he or she logs on.

The Alias field is the alias that can be used in messaging. You can also enter aliases in Address Books. If a person has multiple aliases, the alias is first used from the personal address book, then the global address book, and then the shared address book.

NOTE

An alias is automatically created in the Address Book based upon Radio alias value when the radio is added to in PremierOne. Any time the alias is changed in the Radio configuration, the alias is not updated in the Address Book; you must manually update the alias. The alias in the Address Book and Radio configuration do not have to match.

Messages uses the alias in the Address Book to route notification/mail messages.

Following are fields that may need some clarification:

- Current Status – Indicates whether the user is logged in. You can lock a user out by clicking the Lock button. A dialog box displays prompting you for confirmation and asking for the time period in which the user should be logged out. Either enter the amount of time in minutes or hours, or select the Until button, and then select the date.

  When a user's account becomes locked due to invalid login attempts, you can use this dialog box to unlock the account.

Figure 11-4 Locked Dialog Box

- Active – Indicates the dates of employment for the person. When the end date is reached, the employee is deactivated.
- Past Employee – Indicates the user is no longer employed (this field does not interact with the Active fields).
- Date of Termination – The last day the person was employed.
- Radio ID – How the user wants to be addressed on the radio (such as 1 adam 4). This does not relate to radio the employee's radio assignment.
- Capabilities – Free text field listing any capabilities associated with the personnel record. This field has no effect on the capabilities assigned to a unit (when the person is assigned to a unit).

  When a personnel record has skills assigned and then that person is assigned to a unit, those skills become capabilities that the unit possesses.

- Skills – Skills that the person has, such as language skills or negotiator skills. A person can have multiple skills.

  The skill codes must be set up before you can select the skills. For information on setting up Personnel Skill codes, see “Provisioning Capabilities” on page 11-5. Skills are used in recommendations.

- Radio call sign – The radio call sign associated with the personnel record. This field does not affect any unit preassignments for a person.

- Login Restrictions – Select whether the user will be logging in from PremierOne CAD and Mobile and/or PMDC.

- Directory Configuration – If your agency is using Active Directory (AD) authentication, select the **Active Directory** button. Then select the **Active Directory Domain** and enter the **Account Name** for the user. This method can be used when you are already using AD to control your user accounts.

  Active Directory Domains must be configured in List and Statute Management. For details, see “Configuring Active Directory for Authentication” on page 6-9.

  The Premier One user ID does not have to be same with external active directory account name. For example, the PremierOne user ID `NUser1` can link to the external active directory user account `MSmith` of external domain `R2-HA`.

Adding Personnel Contact Information

Personnel contact information includes the person’s email addresses, physical address, phone numbers, and any keywords.

To add personnel contact information:

1. Open the Personnel window.

   For details, see “Adding Personnel Detail Information” on page 11-8.

2. Select the Contact Info tab in the Personnel window.

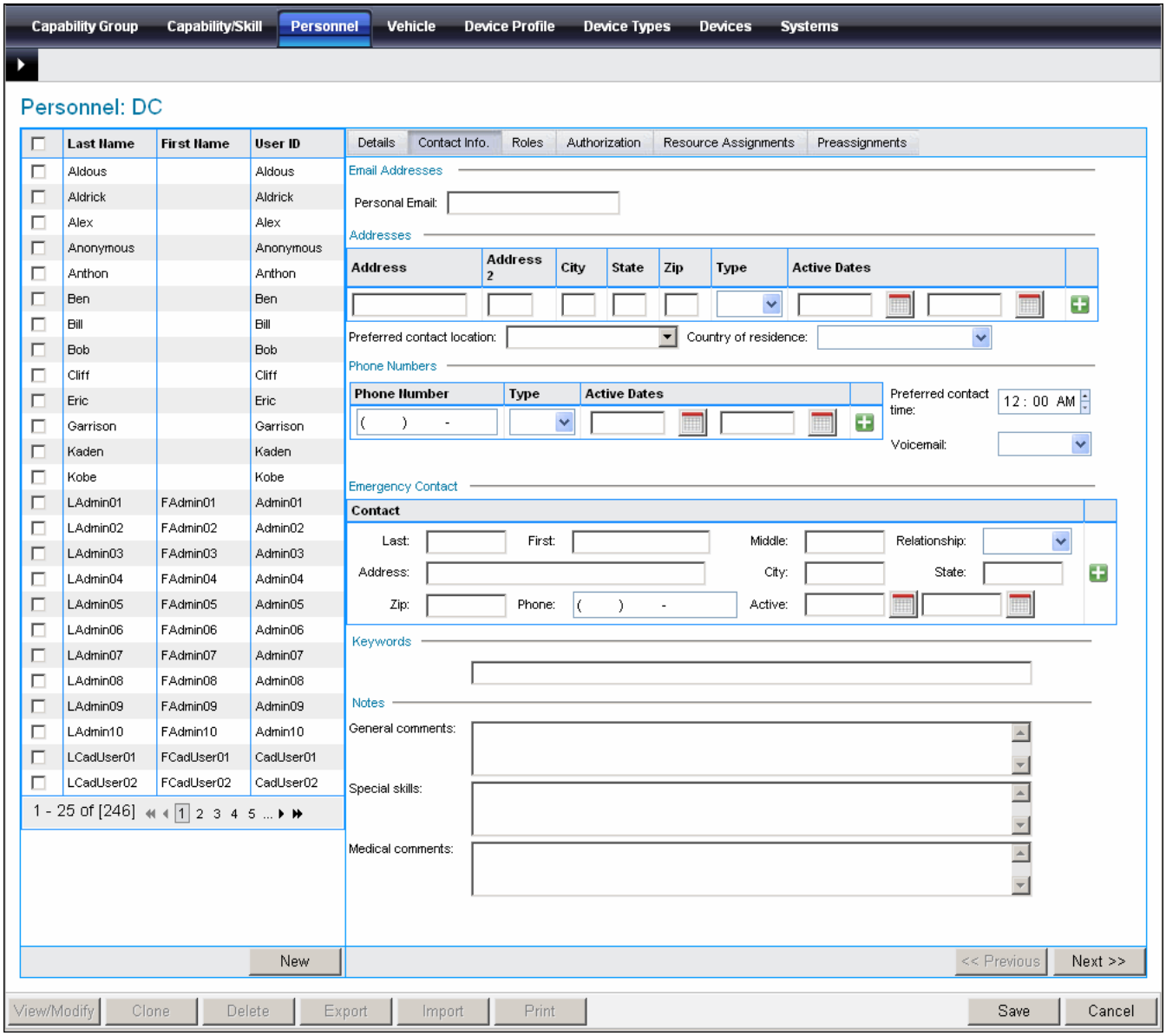


Figure 11-5 Personnel Form – Contact Info Tab

3. In the Email Addresses section, type the primary and secondary email addresses for this contact.

4. In the Addresses section, type the addresses. Also enter a preferred contact location and the county of residence.

   Type up to 32 characters in the address fields.

   Use the Address 2 field for an apartment number, unit number or other information.

Click the plus symbol to the right of the address line to save the address and add another address row.

CAUTION

If you do not click the plus symbol to the right of the address, PremierOne does not save the address information, even after you click Save.

5. In the Phone Numbers section, type the phone number, including the area code. Also enter the type of phone (cell, home, or pager) and the active dates for the phone number. Enter the preferred contact time and voice mail information.

   Click the plus symbol to the right of the phone to save the phone information and add another phone number row.

6. In the Emergency Contact section, type the information for the person's emergency contact.

   Click the plus symbol to the right of the emergency contact information to save the information and add another set of contact fields.

7. In the Keywords section, type any unique words that can be used to search for this person.

   Keywords can be searched for in the Address Book.

8. In the Notes section, enter any general comments, special skills, or medical comments that apply to this person.

9. Click **Save**.

Adding Personnel Roles Information

Personnel roles information includes the roles you assign to the person, such as call taker, dispatcher, or supervisor. Roles control the access that a user has to the different services, Address Books, Groups, Messaging, Print, and Provisioning and specific instances of address books, dynamic groups, query types, and printers. For additional details on roles, see "Adding Role Permissions" on page 8-5.

You can also assign permissions to resources based on device types; for details, see "Adding Device Type Permissions" on page 11-39. If permissions are provisioned in both places, the most restrictive will apply.

To add personnel roles information:

1. Open the Personnel window.

   For details, see "Adding Personnel Detail Information" on page 11-8.

2. Select the Roles tab in the Personnel window.

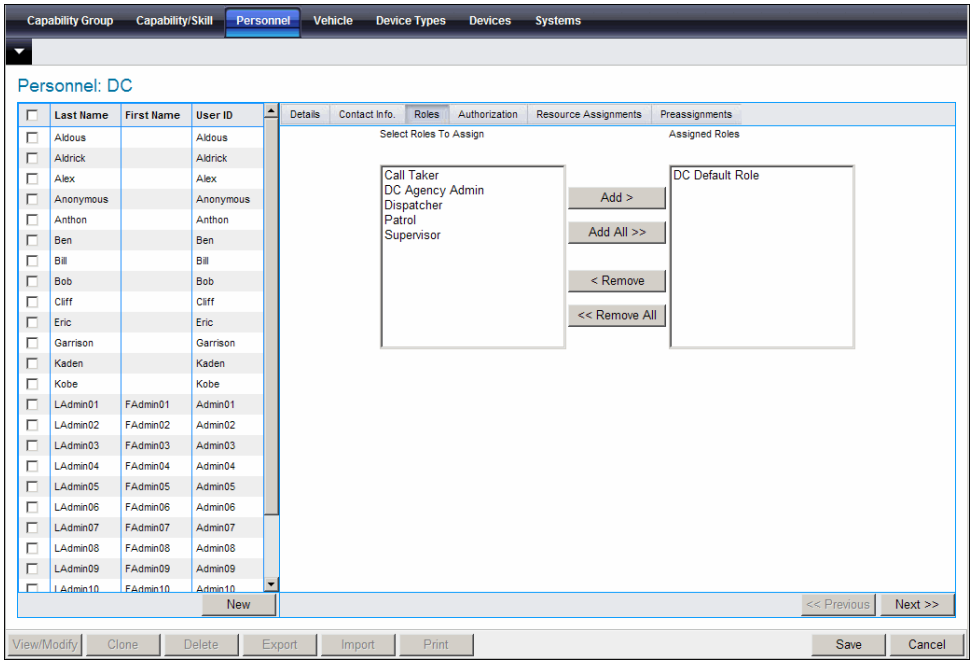


Figure 11-6 Personnel Form – Roles Tab

3. From the Select Roles to Assign box, select one or more role and click the **Add** arrow.

4. Click **Save**.

Adding Personnel Authorization Information

Personnel authorization information is where you control the person's login authorizations, login restrictions, and password.

To add personnel authorization information:

1. Open the Personnel window.

   For details, see "Adding Personnel Detail Information" on page 11-8.

2. Select the Authorization tab in the Personnel window.

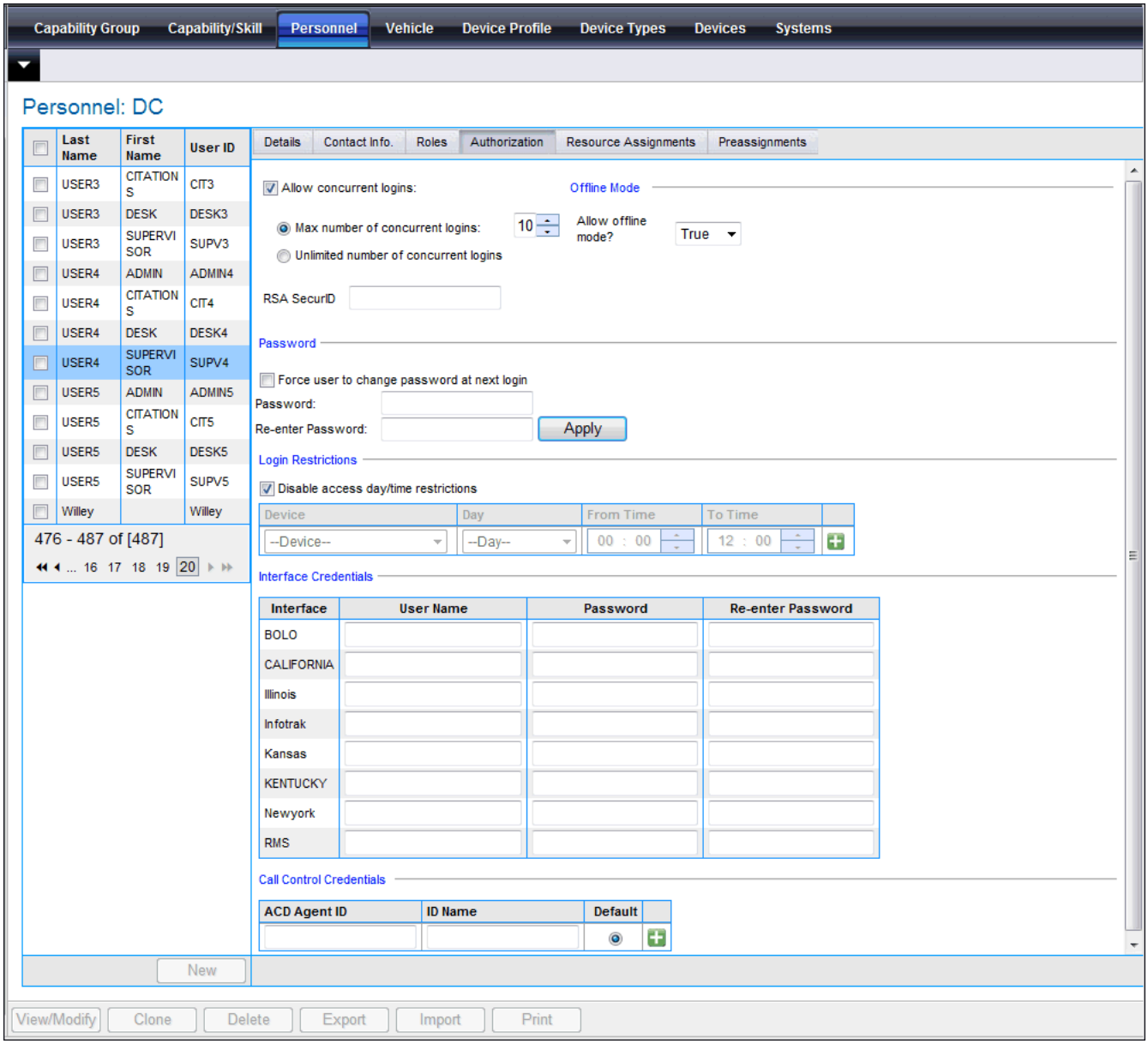


Figure 11-7 Personnel Form – Authorization Tab

3. In the top section, select how to handle concurrent logons for this person.

   Concurrent logins allow users to log in to more than one device at a time. Concurrent logins can be set for a device type in the Resources-Personnel configuration item, for an agency in the Authentication configuration item, and for a workstation in the Devices-Workstation item.

If a setting in more than one of these places, all of the concurrent limitations are validated during login process. The most restrictive value will apply.

NOTE

If a call taker is using NG9-1-1 Call Control functionality, Motorola strongly recommends that the user is NOT allowed concurrent logins. NG9-1-1 Call Control requires that the same user ID only be active within the Call Control module one session at a time. If a user is active in two call control sessions simultaneously, statistics regarding 9-1-1 call handling would be incorrect. The SMS Text messaging gateway between citizen cell phones would also be affected and the call control could potentially misdirect messages.

4. In the Offline Mode section, select whether to allow offline mode.
5. In the Password section, select whether to force the person to change his or her password at the next login and type the initial password.
6. In the Login Restrictions section, select whether there are any times or days when access will be disabled.
7. In the Interface credentials section, enter the user name and password for the appropriate interface. Re-enter the password.

   This data is passed to CommSys for verification.
8. If your agency is using an integrated telephony system, enter the credentials for the 9-1-1 Call Control position in the Call Control Credentials section, and click the plus (+) sign.

   Use the associated ACD Agent ID and VIPER password. Users can be assigned multiple Agent IDs.
9. Click **Save**.

Adding Personnel Resource Assignment Information

Personnel resource assignment is where you assign equipment, including radios, pagers, and vehicles.

To add personnel resource assignment information:

1. Open the Personnel window.

   For details, see “Adding Personnel Detail Information” on page 11-8.

2. Select the Resource Assignments tab in the Personnel window.

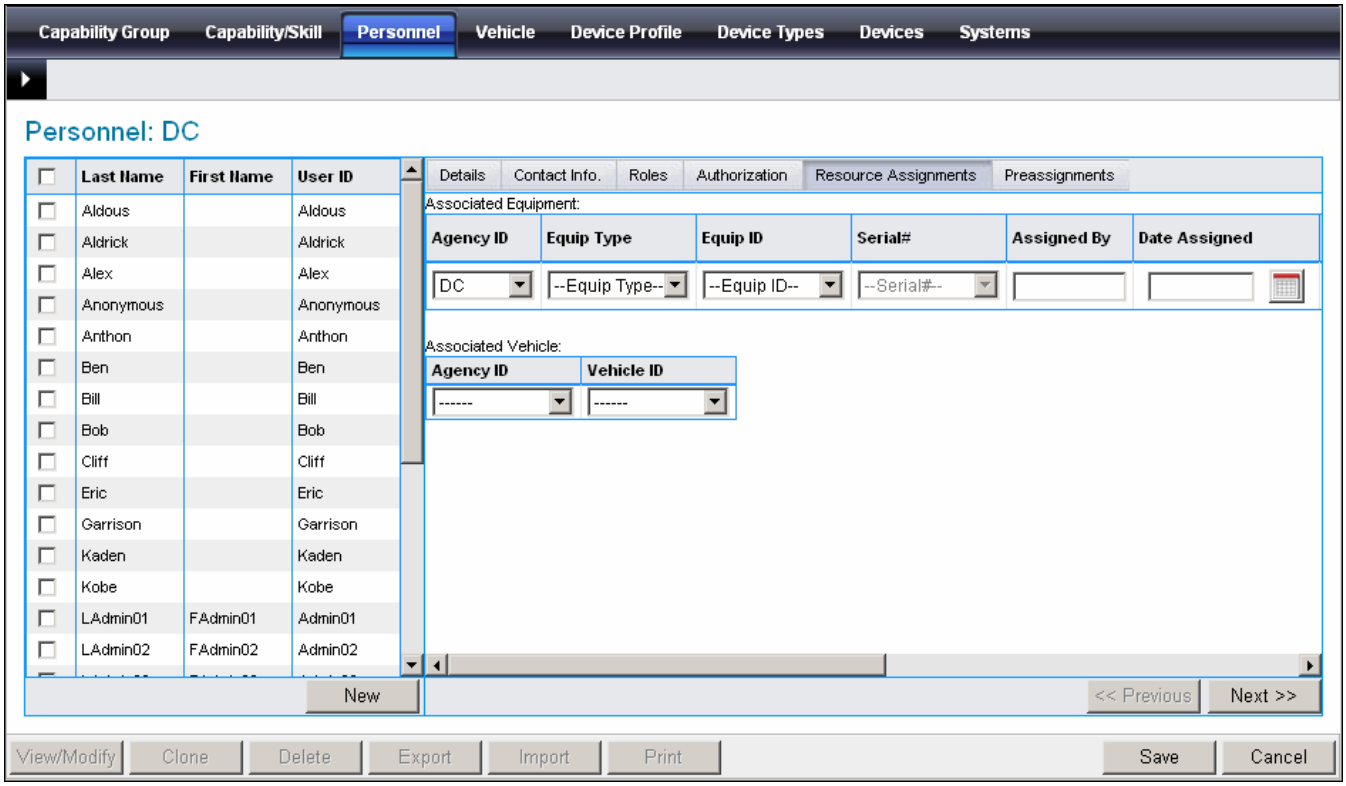


Figure 11-8 Personnel Form – Resource Assignments Tab

3. In the Associated Equipment section, do the following:

   a. In the Equip Type field, select the equipment type you are assigning to this person.

   b. In the Equip ID field, select the equipment ID for the equipment you are assigning to this person.

   c. In the Serial # field, select the serial number for the equipment you are assigning to this person.

   d. In the Assigned By field, type or select the name of the person who assigned the equipment.

   e. In the Date Assigned field, type or select the date on which the equipment was assigned.

   f. In the Time Assigned field, select the time the equipment was assigned.

   g. In the Condition Assigned field, select the condition the equipment was in when it was assigned.

   h. In the Date Returned field, type or select the date on which the equipment was returned, if applicable.

i. In the Time Returned field, select the time the equipment was returned, if applicable

j. In the Condition Returned field, select the condition the equipment was in when it was returned, if applicable.

To add more equipment, click the plus symbol to the right of the equipment row. Equipment can include one or more radios, MDTs, pagers, and so on.

4. In the Associated Vehicle section, do the following:

a. In the Agency ID field, select the Agency ID for the assigned vehicle for this person.

b. In the Vehicle ID field, select the ID of the vehicle for this person.

5. Repeat the procedure for any other personnel records you want to add.

6. Click **Save**.

Adding Personnel Preassignments

You can add personnel preassignments for officers who are assigned to the same jurisdictions and do not have fixed Unit IDs. This is useful, for example, for supervisors who are assigned to the same jurisdictions whenever they go on duty. Once provisioned, officers can go on duty using the preassignments regardless of the specified unit ID. Values entered here override any jurisdictional unit assignments. For details on unit assignments, see “Configuring Unit Preassignments” on page 10-4.

Currently users can load the jurisdictional assignments provisioned against a unit into the On Duty form. However, users are not allowed to load the jurisdictional assignments provisioned against a Personnel record into the On Duty form.

The following rules apply to jurisdictional assignments:

- Users cannot modify any of the jurisdictional assignments that are provisioned against the Personnel record during an On Duty transaction. Therefore, whenever the user indicates that the Personnel’s jurisdictional assignments are to be used for an On Duty transaction, all manually specified jurisdictional assignments are ignored for the transaction.

- If more than one officer is assigned to the unit, the On Duty transaction only considers the jurisdictional assignments that are provisioned against the first officer specified for with transaction. If the first officer specified does not have a provisioned Area/Station value, an error displays.

To add personnel preassignments:

1. Open the Personnel form.

For details, see “Adding Personnel Detail Information” on page 11-8.

2. Select the Preassignments subtab.

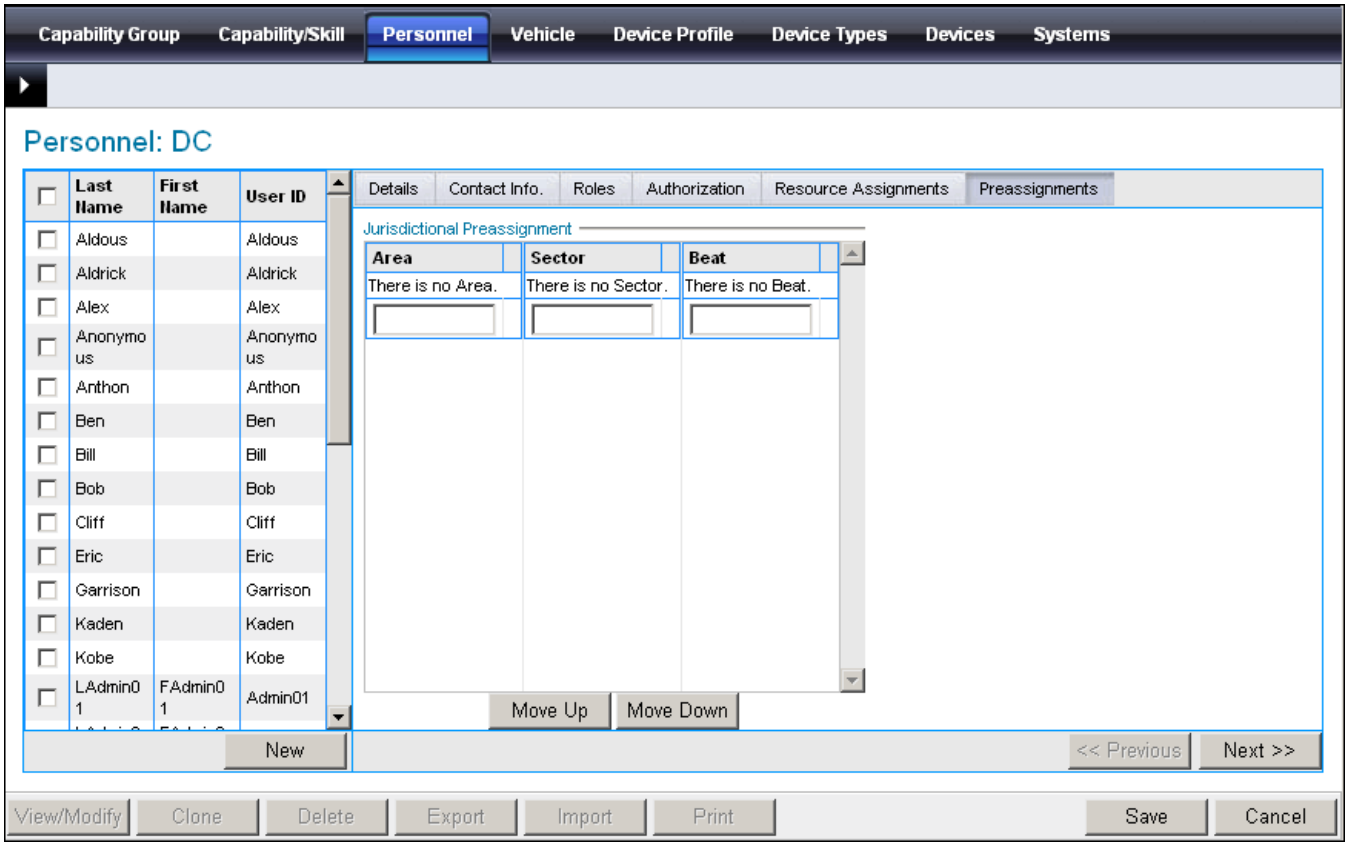


Figure 11-9 Personnel Form – Preassignments Settings Subtab

3. Enter the Area/Sector/Beat combinations for the assignment.

   The order of the assignments are used for recommendations based on jurisdictional assignments. Assignments at the top of the list are considered first. To change the order, select the area, sector, or beat that you want to move, and then click **Move Up** or **Move Down**.

4. Click **Save**.

Configuring Vehicles

When you add a vehicle, you enter information on the Vehicles form. Before adding vehicle records, you must complete the following prerequisites:

- Create vehicle lists in Lists and Statute Management. For instructions, see “Adding Lists and Codes” on page 6-6.
- Configure capabilities in Unit Management. For instructions, see “Adding Capabilities/Skills” on page 11-6.
- Configure equipment in Resources. For instructions, see “Configuring Workstation/MDT/Handheld Devices” on page 11-43.
- Configure equipment types in Resources. For instructions, see “Adding Device Type General Information” on page 11-35.

To add a vehicle:

1. From the navigation pane, select **Resources**, and then select **Vehicle**.

   The Vehicle form appears. A list of existing records displays on the left side of the form.

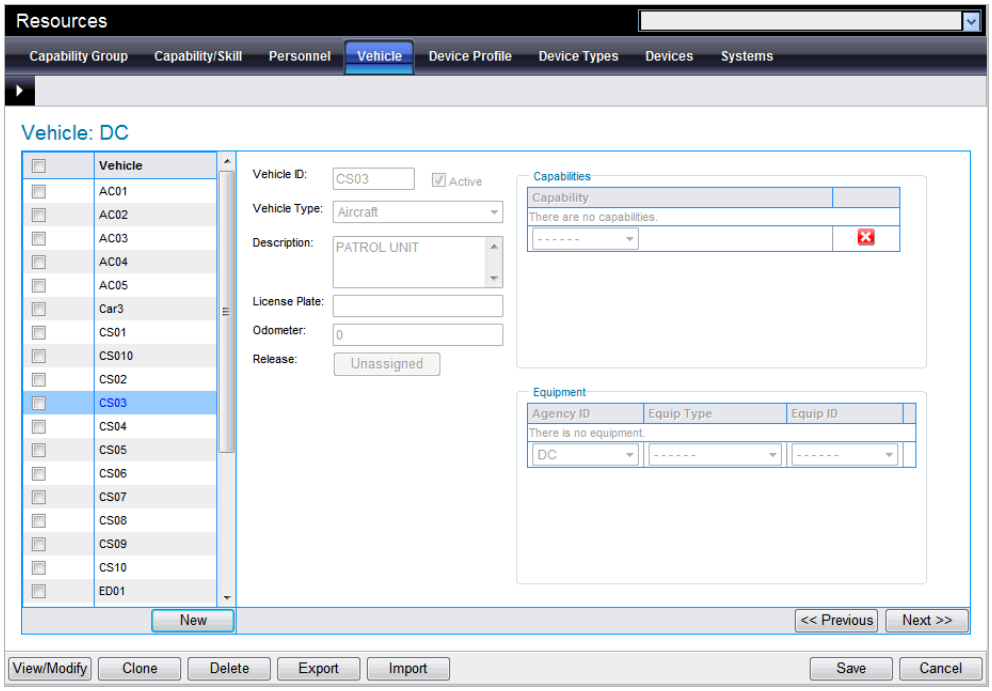


Figure 11-10 Vehicles Form – Add New

2. At the bottom of the vehicle record list, click the **New** button.
3. Enter the Vehicle ID, type, description, license plate, and odometer.

4. If the vehicle is active, select the **Active** check box.

5. In the License Plate field, enter the license plate number for the vehicle.

6. In the Odometer field, enter the odometer reading.

   To unassign a vehicle for a unit, click **View/Modify** and then click the Release button. Currently, you cannot identify the unit the vehicle is assigned to from this window.

7. From the Capabilities list, select a capability if the vehicle has one. Capabilities refer to the function or equipment on a vehicle, such as fire engine, truck, or K9 unit.

   When you select a capability, PremierOne saves the capability you added and adds another row to the table.

   The options for the Capability list are configured on the Capability form. For more information, see "Adding Capabilities/Skills" on page 11-6.

8. From the Equipment list, select the equipment and equipment ID that is included with this vehicle. Equipment can include one or more radios, MDTs, pagers, GPS and Trimble Direct GPS devices, and so on.

   When you select the equipment ID, PremierOne saves the equipment information and adds another row for additional more equipment.

9. Repeat the procedure for any other vehicle records.

   Each unsaved vehicle record appears in the Vehicle list in blue text.

> **NOTE**
> If you have a large number of vehicles to configure, you can import the information from an spreadsheet. For details, see "Importing Configuration Items" on page 2-13.

10. Click **Save**.

Configuring Device Profiles

Use the Device Profile configuration item to configure options for different radio systems. Device profiles can be created for multiple radio types. Device profiles are used in radio configuration. For details, see “Adding Radios” on page 11-55.

You can add, modify, export, import, and delete device profiles. For details, see “Working With Configuration Items” on page 2-9. You cannot change the Device Profile name. If you want to change the name, you must delete and re-add the record.

When you configure a device profile, you add information on the following tabs:

- General – Where you set the name for the profile, configure the maximum number of characters supported in messages, and whether two-factor authentication is used.
- BOLO Content – Where you configure the priority of BOLO messages that are sent to the radio, the maximum number of pages in the BOLO text, and the fields and the order of the fields that are sent.
- Emergency Content – Where you set whether emergency notifications are automatically sent to the radio when the officer is out of the vehicle.
- Incident Content – Where you set whether dispatch and updates are sent to the officer’s radio when the responder is out of the vehicle.
- Message Content – Where you configure the priority of messages sent to the radio, whether messages are sent when the responder is out of the vehicle, the maximum number of pages in messages, and the fields and the order of the fields that are sent.
- Notification Content – Where you configure whether hot notifications are sent to responders when they are out of the vehicle, the information that is sent, and the order of the information that is sent.
- Query Content – Where you configure whether query responses are sent to a radio when the responder is out of the vehicle, whether hot hit notifications are sent to the radio regardless of whether the responder is out of the vehicle, and the priorities of hot hit notifications to send when the responder is out of the vehicle.

Configuring Device Profiles General Information

Device profile information sets limits on the maximum number of characters that are supported in messages and whether two-factor authentication is used during signon.

To configure general information:

1. From the navigation panel, select **Resources.**
2. Select **Device Profile**.

The Device Profile form appears with a list of existing profiles on the left side of the form.

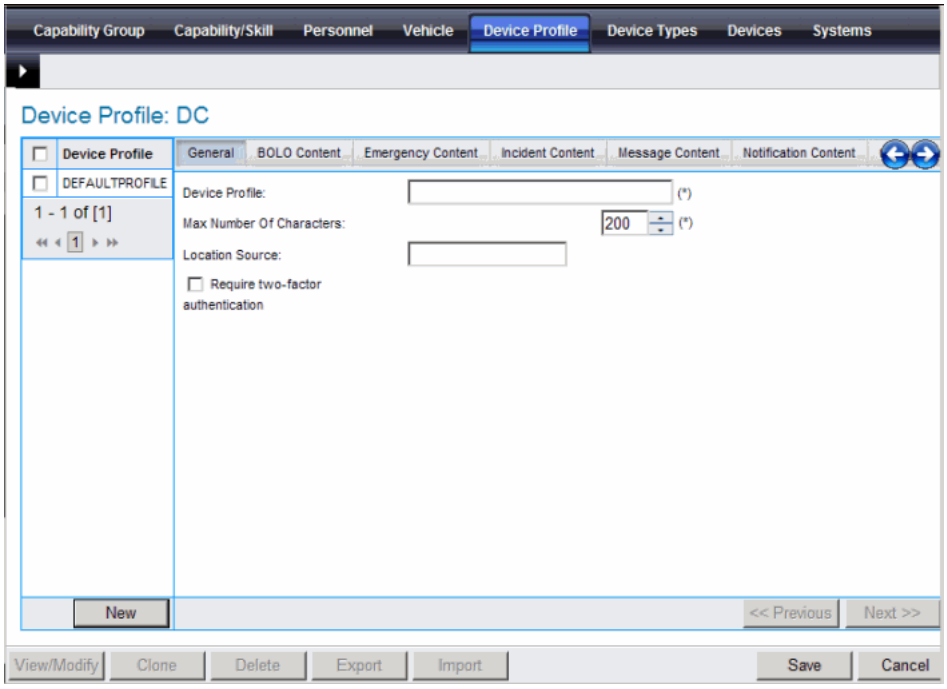


Figure 11-11 Device Profile Form – General Tab

3. At the bottom of the device profile list, click the **New** button.

4. In the Device Profile field, enter an identifying name for the profile.

5. From the Max. Number of Characters list, select the maximum number of characters allowed in a message to the radio system.

   Any excess text is truncated. The message will have an indicator that it was truncated. The maximum value is 200.

6. In the Location Source field, enter the MUPS (Motorola Universal Processing Server) information.

   For an XTS radio using the 7.11 ASTRO API, the value would be `MUPS_XTS_7.11`. Only XTS, APX, and XTL radios are supported.

   This information is used when a request is made for an on demand update for a person or unit with a radio. Otherwise, the information defaults to PremierOne mobile.

7. To use two-factor authentication in sign on, select the **2-Factor Authentication** check box.

   Two-factor authentication is required for access to NCIC and other similar databases. One-factor authentication is acceptable for some agencies to connect only to their state databases.

Two-factor authentication associates the user to a device with an additional level of security so the user can run queries.

If you do not select the check box, then either device login authentication (identifies the device such as a portable radio or mobile unit) or one-factor authentication (associates a user to a device with a user ID and password) is used. Which option is used When you are finished, click **Save**.

Configuring Device Profiles BOLO Content

Device profile BOLO content controls the priority of BOLO messages that are sent to the radio, the maximum number of pages in the BOLO text, and the fields and the order of the fields that are sent.

NOTE
ASTRO limits individual message sizes to 225 characters.

To configure BOLO content:

1. Access the form for device profiles.

   For instructions, see “Configuring Device Profiles General Information” on page 11-22.

2. Select the BOLO Content tab.

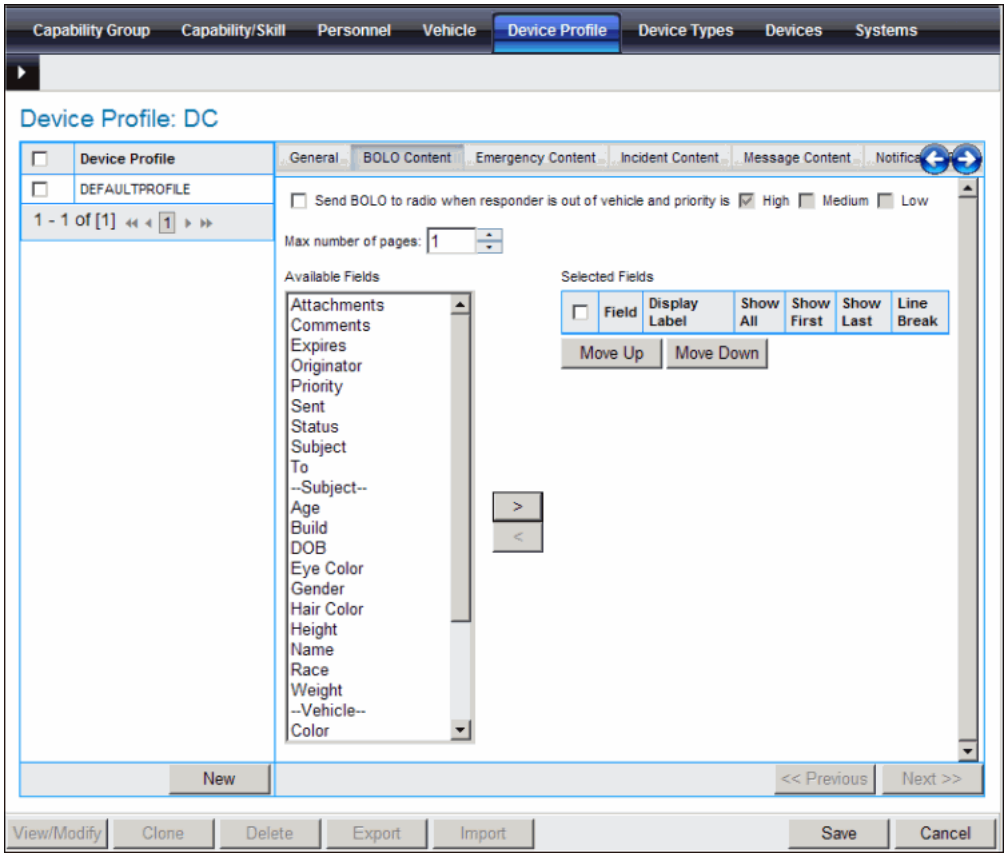


Figure 11-12 Device Profile Form – BOLO Content Tab

3. To send BOLOs to responders when they are out of their vehicles, select the **Send BOLO to radio when out of vehicle** check box.

4. Select the check boxes for the priorities for which to send BOLO messages.

5. From the Max number of pages list, select the maximum number of pages of information to send to the radio with the BOLO message.

6. From the Available Fields box, select the fields you want to display and click the left-facing arrow to add them to the Selected Fields box.

   - To reorder the fields, select the field to move and then click the **Move Up** and **Move Down** buttons.
   - For each field, select whether you want to show all of the field, the first ten characters, or the last ten characters.
   - To add a line break after the field, select the **Line Break** check box.

7. Click **Save**.

Configuring Device Profiles Emergency Content

Device Profile emergency content controls whether emergency notifications are automatically sent to a radio when the “primary” officer is out of the vehicle. The entire content of the notification is sent.

To configure emergency content:

1. Access the form for device profiles.

   For instructions, see “Configuring Device Profiles General Information” on page 11-22.

2. Select the Emergency Content tab.

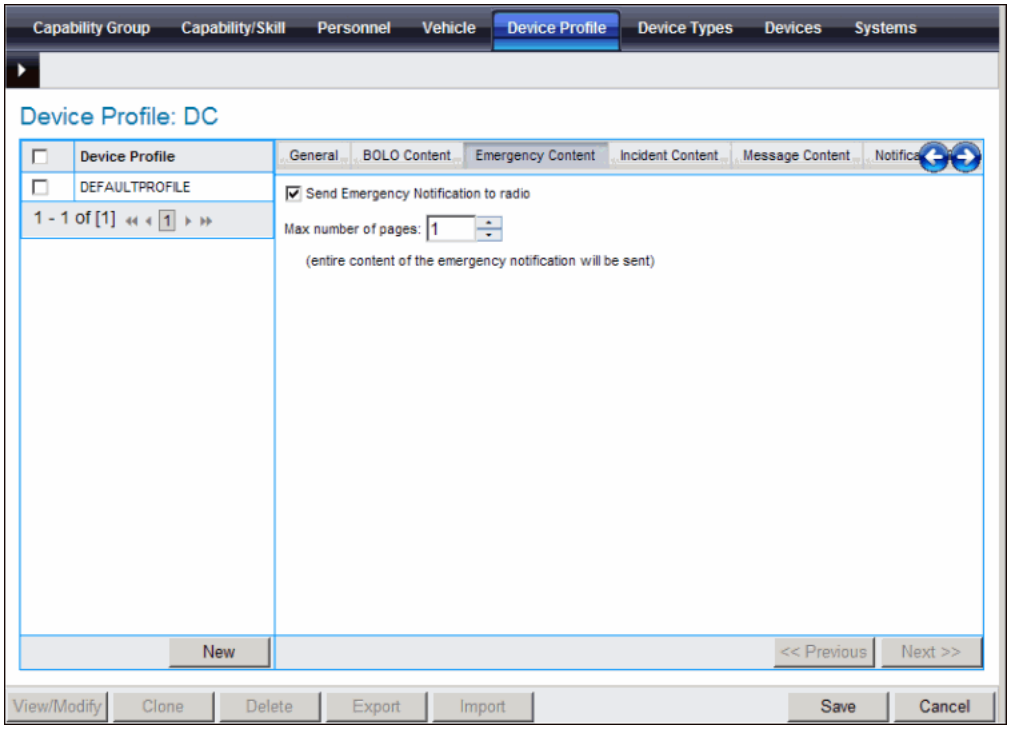


Figure 11-13 Device Profile Form – Emergency Content Tab

3. Select the **Send Emergency Notification to radio when out of vehicle** check box.

4. Click **Save**.

Configuring Device Profile Incident Content

The incident content controls whether incident dispatches and updates are sent to an officer's radio when an officer is out of the vehicle, the fields that are sent, and the maximum number of pages that are sent.

NOTE
ASTRO limits individual message sizes to 225 characters.

To configure incident content:

1. Access the form for device profiles.

   For instructions, see "Configuring Device Profiles General Information" on page 11-22.

2. Select the Incident Content tab.

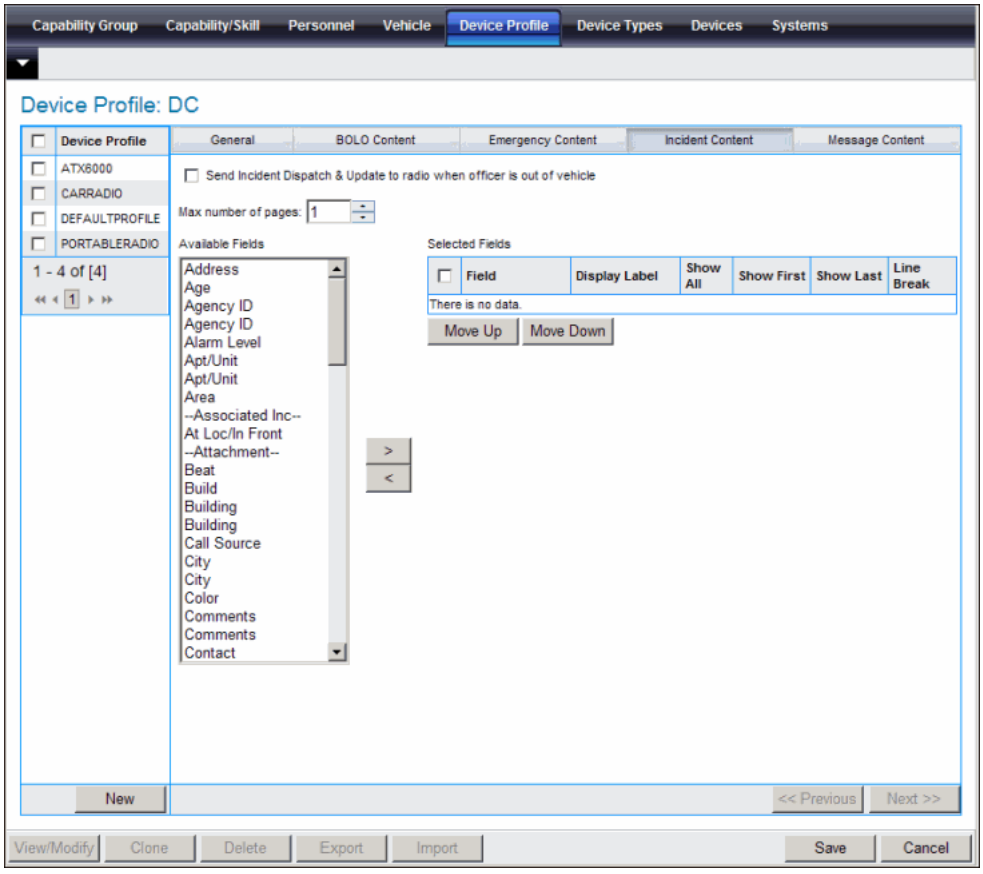


Figure 11-14 Device Profile Form – Incident Content Tab

3. To send incident content to responders when they are out of their vehicle, select the **Send Incident Dispatch and Update to radio when officer is out of vehicle** check box.

4. From the Available Fields box, select the fields you want to display and click the left-facing arrow to add them to the Selected Fields box.

   - To reorder the fields, select the field to move and then click the **Move Up** and **Move Down** buttons.
   - For each field, select whether you want to show all of the field, the first ten characters, or the last ten characters.
   - To add a line break after the field, select the **Line Break** check box.

5. Click **Save**.

Configuring Device Profile Message Content

The message content controls the fields that are sent to a radio, the order of the fields, the maximum number of pages that are sent to the radio, and whether the message is sent when the responder is out of the vehicle.

NOTE
ASTRO limits individual message sizes to 225 characters.

To configure message content:

1. Access the form for device profiles.

   For instructions, see "Configuring Device Profiles General Information" on page 11-22.

2. Select the Message Content tab.

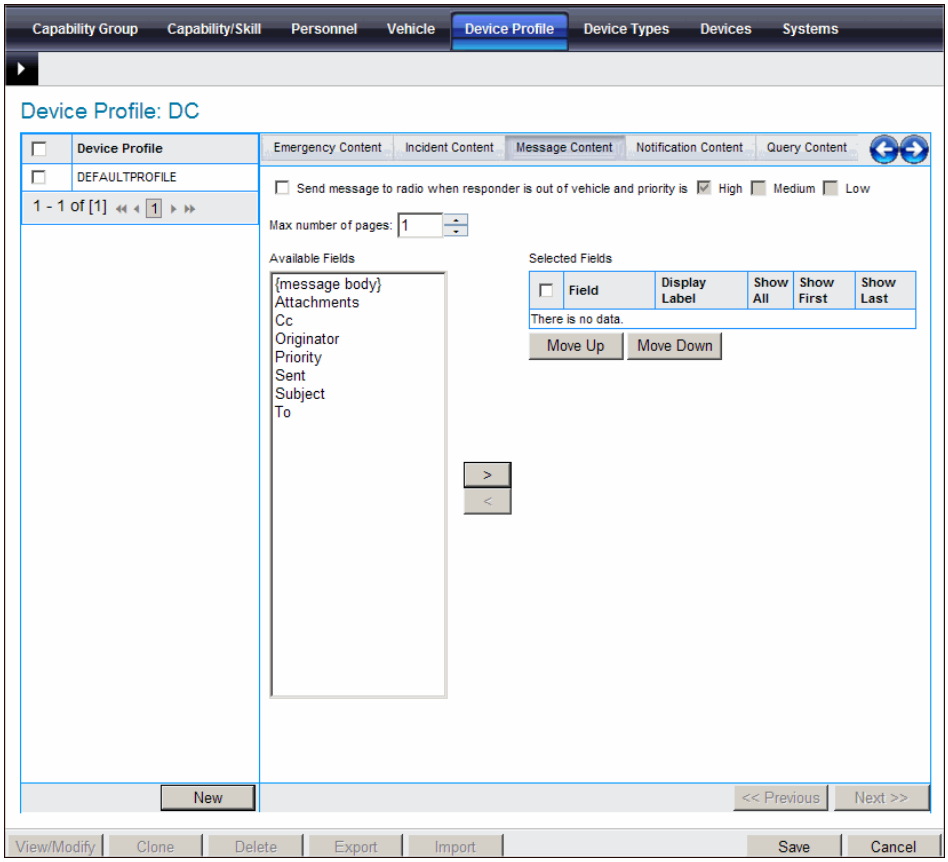


Figure 11-15 Device Profile Form – Message Content Tab

3. To send messages when the responder is out of the vehicle, select the **Send message to radio when responder is out of vehicle** check box.

4. Select the check boxes for the message priorities you want sent to the responder when the responder is out of the vehicle. You can select multiple priorities.

5. From the Max number of pages list, select the maximum number of pages of information to send to the radio with the message information.

6. From the Available Fields box, select the fields you want to display and click the right-facing arrow to add them to the Selected Fields box.

   - To reorder the fields, select the field to move and then click the **Move Up** and **Move Down** buttons.
   - For each field, select whether you want to show all of the field, the first ten characters, or the last ten characters.
   - To add a line break after the field, select the **Line Break** check box.

7. Click **Save**.

Configuring Device Profile Hot Hit Notification Content

Notifications can be configured to display for hot hits. Hot Hits are keywords that occur in a query response, such as WANTED. Notification content controls the fields that are sent to a radio, the order of the fields, the maximum number of pages that are sent to the radio, and whether notifications are sent when the responder is out of the vehicle.

To configure hot hit notification content:

1. Access the form for device profiles.

   For instructions, see "Configuring Device Profiles General Information" on page 11-22.

2. Select the Notification Content tab.

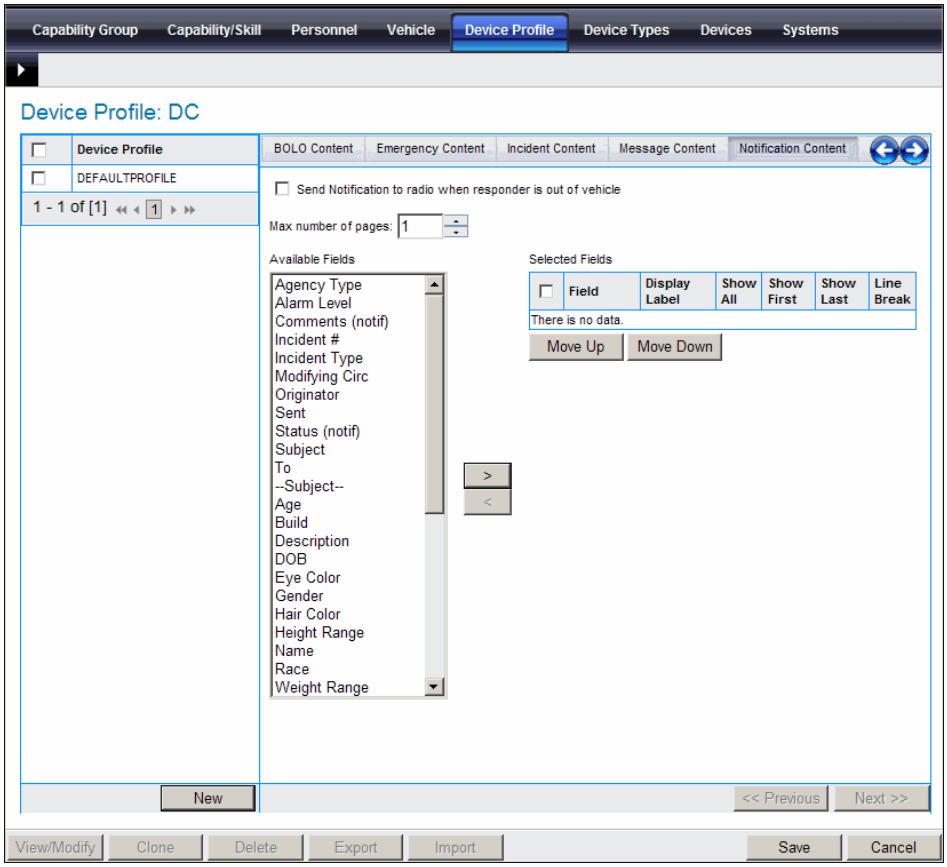


Figure 11-16 Device Profile Form – Notification Content Tab

3. To send notifications when the responder is out of the vehicle, select the **Send Notification to radio when out of vehicle** check box.

4. From the Max number of pages list, select the maximum number of pages of information to send to the radio with the message.

5. From the Available Fields box, select the fields you want to display and click the right-facing arrow to add them to the Selected Fields box.

- To reorder the fields, select the field to move and then click the **Move Up** and **Move Down** buttons.
- For each field, select whether you want to show all of the field, the first ten characters, or the last ten characters.
- To add a line break after the field, select the **Line Break** check box.

6. Click **Save**.

Configuring Device Profile Query Content

Query content controls whether query responses are sent to a radio when the responder is out of the vehicle, whether hot hit notifications are sent to the radio regardless of whether the responder out of the vehicle, and the priorities of query responses to send when the responder is out of the vehicle.

To configure query content:

1. Access the form for device profiles.

   For instructions, see "Configuring Device Profiles General Information" on page 11-22.

2. Select the Query Content tab.

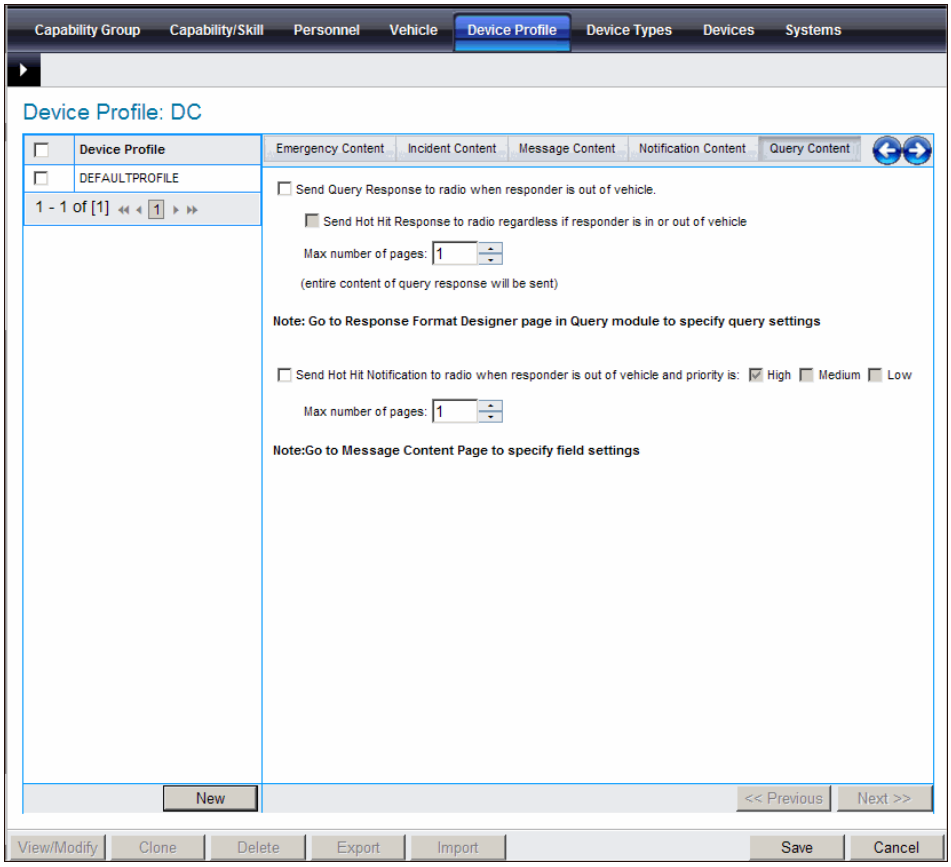


Figure 11-17 Device Profile Form – Query Content Tab

3. To send query responses to a radio when the responder is out of the vehicle, select the **Send Query Response to radio when responder is out of vehicle** check box.

4. To send query responses regardless of whether the responder is out of the vehicle, select the **Send Hot Hit Responses to radio regardless if responder is in or out of vehicle** check box.

   You must select the check box in the previous step to enable this check box.

5. From the Max number of pages list, select the maximum number of pages to send to the radio for query responses. The entire content of query responses is always sent.

6. To Send hot hit notifications when the responder is out of the vehicle, select the **Send Hot Hit Notification to radio when responder is out of vehicle and priority is** check box. Then select the priority of messages that you want to send. You can select multiple priorities.

   The fields that are sent are configured on the Message Content tab. For details, see “Configuring Device Profile Message Content” on page 11-28.

7. From the Max number of pages list, select the maximum number of pages to send to the radio for notification messages.

8. Click **Save**.

Configuring System Address Message Type Indicators

You can configure the message type indicator for the ASTRO radios. This includes incident dispatch, incident update, emergency, query returns, hot hits, and hot hit notification messages.

To configure system address type indicators:

1. Log on to the PremierOne Admin Console.

2. Click the **Configuration** icon.

3. Click the Edit tab.

4. Navigate to and select the `msAdmin > mobile server` item.

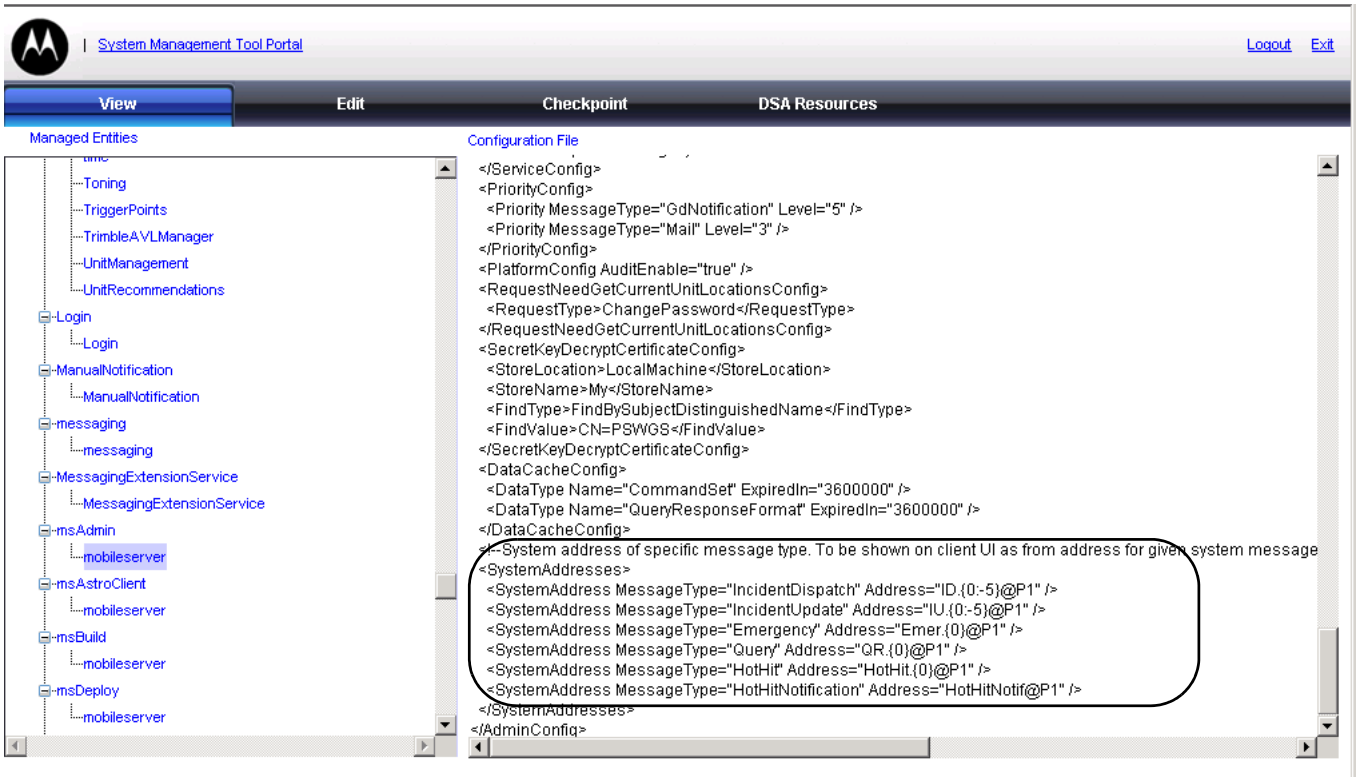


Figure 11-18 System Address Message Type Settings

5. In the System Addresses section, edit the text for the message type display.

   As examples, this is what would display as the message type in the ASTRO radio:

QR.DMV@P1 License CO1234
HotHitNotif@P1 Red motorcycle

6. Click **Save**.

Configuring Device Types

Use the Device Types configuration item to configure properties of device types. Properties include general settings, login settings and permissions to services.

Device types consists of workstations, ASTRO radios, and mobile units. Devices are actual physical entities capable of executing CAD and mobile client software including workstation/mobile units, radios, 2-Tone Radio Groups, pagers, pager groups, printers, and GPS. Devices can be assigned to personnel, vehicles, or units and have some sort of device ID.

- Provision the *device type* when you want to configure settings for the entire group of workstations, radios, or mobile units.
- Provision the actual *device* when you want to configure settings for a specific instance of a device; for example, a specific workstation, a specific mobile unit, or a specific pager. For details on provisioning devices, see “Configuring Devices” on page 11-43.

Modifying Device Types

When you modify a device type, you modify information on four tabs:

- General – Where you add or modify information about the type of device, the device name, description, addressability, make, model, serial number, position, FBR path, OS version, unique address, associated radio ID, and account status.
- Login – Where you add or modify information about automatic login, concurrent logins, failed logins, login retries, the inactive timer, day or time restrictions, printing access, and offline mode for the device.
- Printing – Where you select printers that are available to the device type (disabled for ASTRO radios).
- Permissions – Where you select the services to assign to the device, and then select the features to allow for the selected service or services (disabled for ASTRO radios).

Adding Device Type General Information

General device type information consists of identifying information such as name, description, and timers, offline mode settings, and message routing settings (ASTRO radios only).

To add device type general information:

1. From the navigation panel, select **Resources** and then select **Device Types**.

   The Device Type form appears (see Figure 11-19).

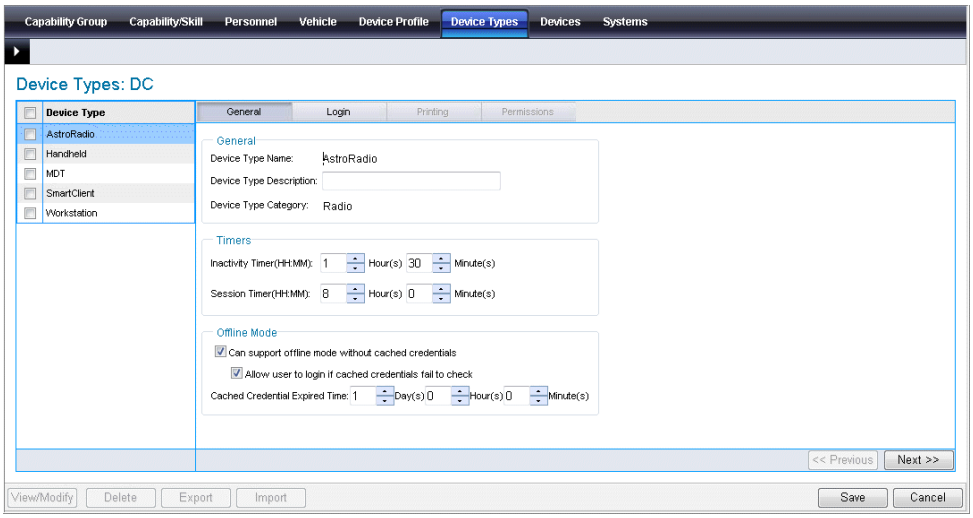


Figure 11-19 Device Types Form – General Tab

2. Select the device type you want to modify.
3. Click **View/Modify**.

   You can now edit the fields on the tabs. Not all the fields can be edited.

4. In the Device Type Description field, enter a description of the device.
5. In the Timers section do the following:

   - From the Inactivity Timer fields, select the amount of time that can pass before the device type is considered inactive. Depending on the device type, the device type may be locked.
   - From the Session Timer field, select the amount of time that can pass in a session.

   Radio session user's may need to follow CJIS (Criminal Justice Information System) rules for session and inactivity timers.

6. To allow offline mode when network connection is lost, select the **Can support offline mode without cached credentials** check box. Then optionally set the following:

- To allow a user to still log in if the cached credentials do not agree with the login that is used, select the **Allow user to login if cached credentials fail to check** box.
- From the **Cached Credential Expired Time** lists, select the time after which the cached credentials will expire.

7. In the Message Routing section (ASTRO radios only), select the message priorities that are sent to the radio when the officer is out of the vehicle.
8. Click **Save**.

Adding Device Type Login Information

Device type login information consists of settings for concurrent logins, failed logins, day/time restrictions for login access, and emergency settings.

To add device type login information:

1. Access the form for device types. For instructions, see "Adding Device Type General Information" on page 11-35.

   The Device Types form appears with the General tab in focus (see Figure 11-19). A list of existing devices types displays on the left side of the form.

2. Select the Login tab.

Fields for login information display.

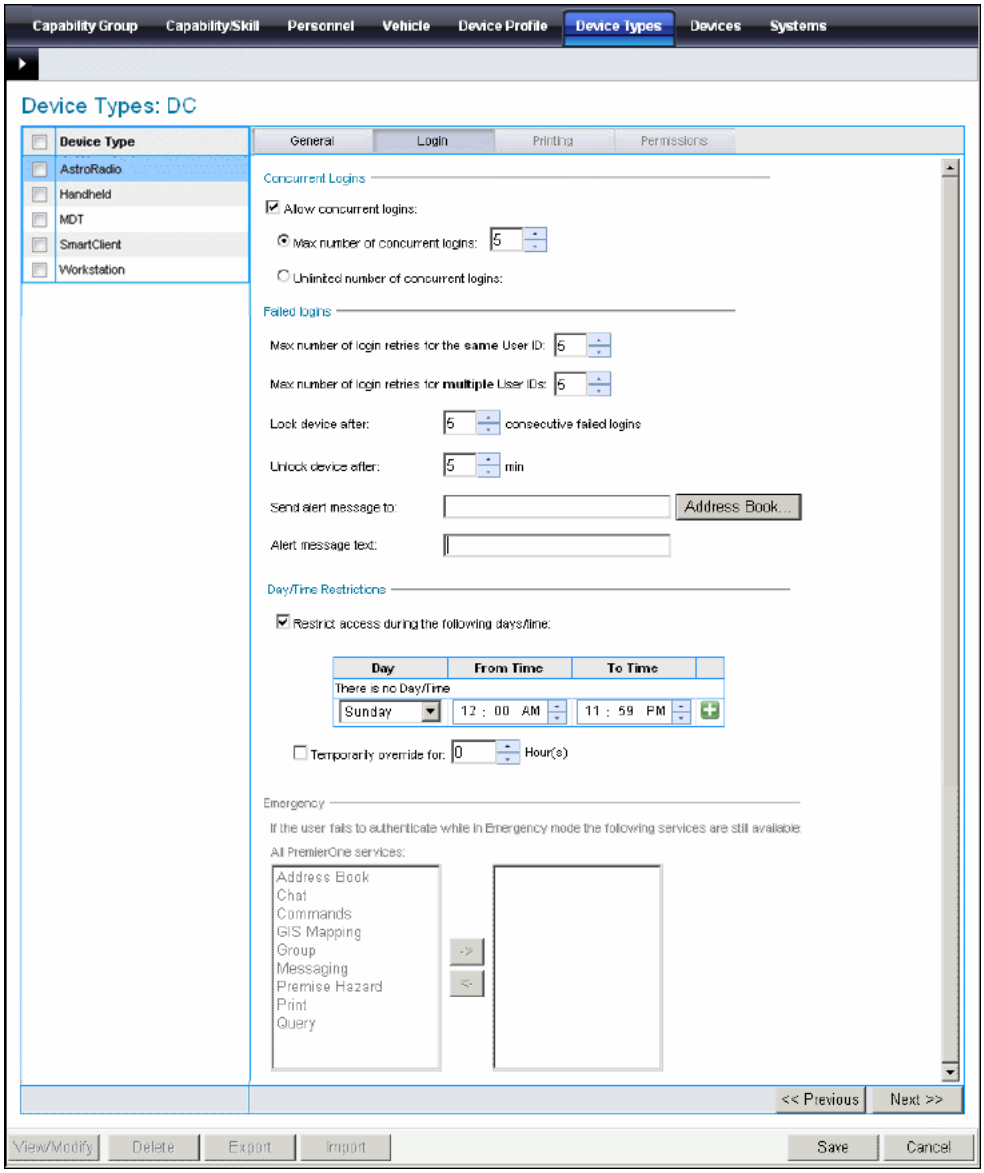


Figure 11-20 Device Type Form – Login Tab

3. In the Concurrent logins section, set whether concurrent logins are allowed, and the maximum number.

   Concurrent logins allow users to log in to more than one device at a time. Concurrent logins can be set for a device type in the Resources-Personnel configuration item, for an agency in the Authentication configuration item, and for a workstation in the Devices-Workstation item.

   If a setting in more than one of these places, all of the concurrent limitations are validated during login process. The most restrictive value will apply.

4. In the Failed Login section, set the maximum number of login retries, and when to lock and unlock the device. You can also select the users to send an alert message to when the maximum number of login retries is used and enter the alert message to deliver.

5. In the Day/Time Restrictions section, set any times to restrict access.

   Select the **Temporary Override** check box and enter the number of hours for a potential override. This allows you to grant temporary access to the device type in case of emergency.

6. In the Emergency section, select the services that can be accessed when the agency is placed in Emergency Mode (Authentication–Agency Setting–Emergency Mode) and the user cannot have the user's logon authenticated.

Adding Device Type Printers

Printer information consists of the list of printers available to the device type. This tab is disabled for ASTRO radios.

To add device type printer information:

1. Access the form for device types. For instructions, see "Adding Device Type General Information" on page 11-35.

   The Device Types form appears with the General tab in focus (see Figure 11-19). A list of existing devices types displays on the left side of the form.

2. Select the Printing tab.

A list of all existing and selected printers displays.

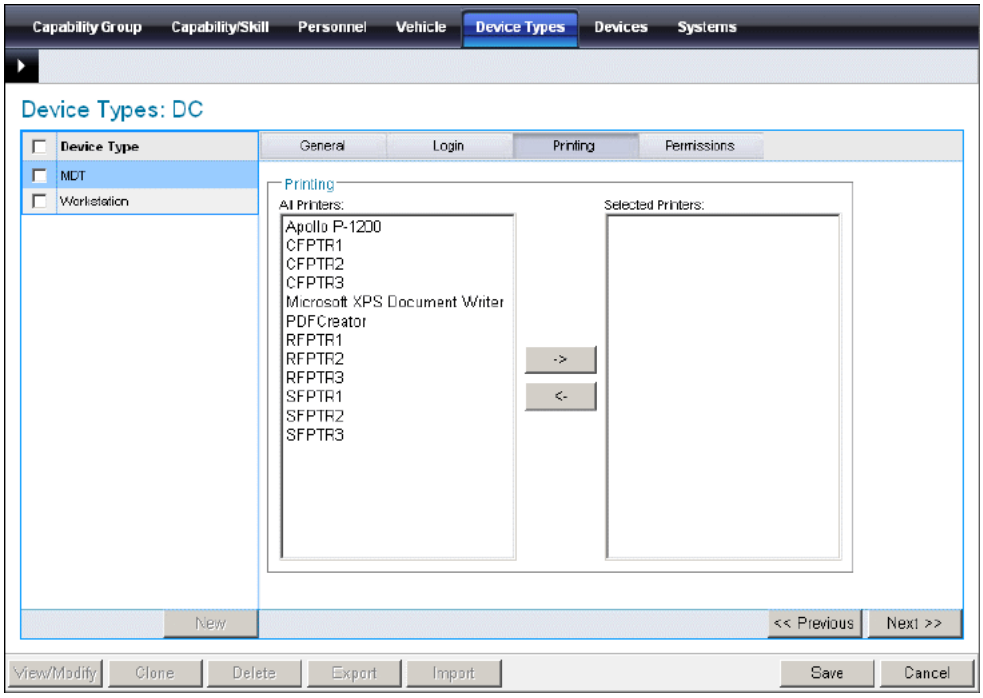


Figure 11-21 Device Type Form – Printing Tab

3. Select any printers you want made available to the device type and add them to the Selected Printers list.

Adding Device Type Permissions

Permission information consists of the services and features available to device types. This tab is disabled for ASTRO radios.

You can also assign permissions to resources based on resource roles; for details, see “Adding Personnel Roles Information” on page 11-13. If permissions are provisioned in both places, the most restrictive will apply.

NOTE

When a device's permissions are changed, the user must exit the client and relaunch for the changes to take effect.

To add device type permissions:

1. Access the form for device types. For instructions, see “Adding Device Type General Information” on page 11-35.

   The Device Types form appears with the General tab in focus (see Figure 11-19). A list of existing devices types displays on the left side of the form.

2. Select the Permissions tab.

The Services and Features subtabs display.

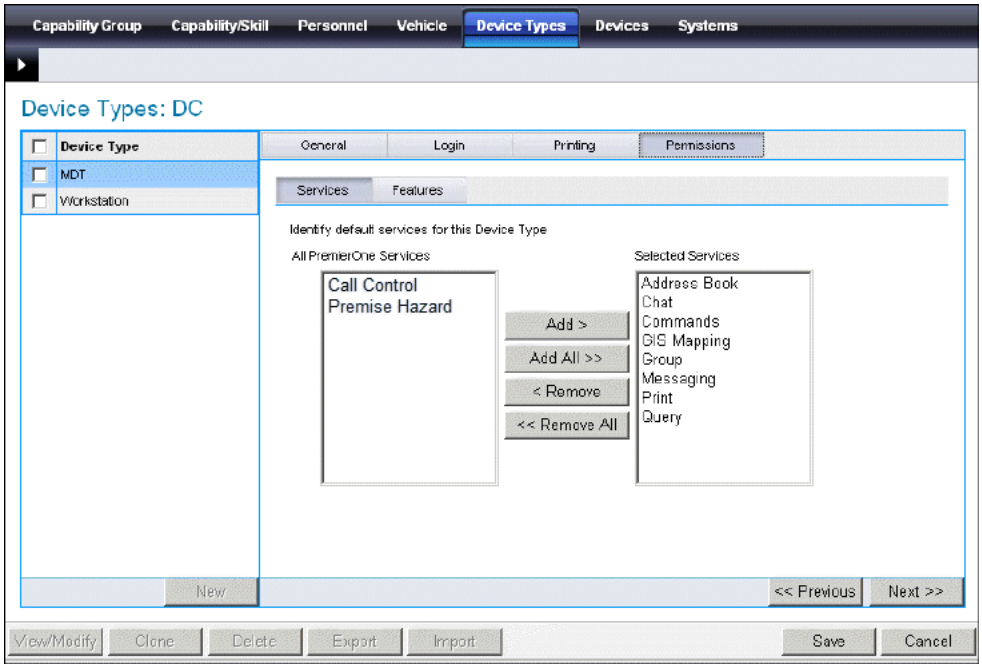


Figure 11-22 Device Type Form – Permissions Tab, Services Subtab

3. Select the services you want available to the device type and add them to the Selected Services list.

   For additional information on services, see “Adding Role Permissions” on page 8-5.

4. Click the Features subtab.

The selected services are listed on the left side and the features for that service are listed on the right side.

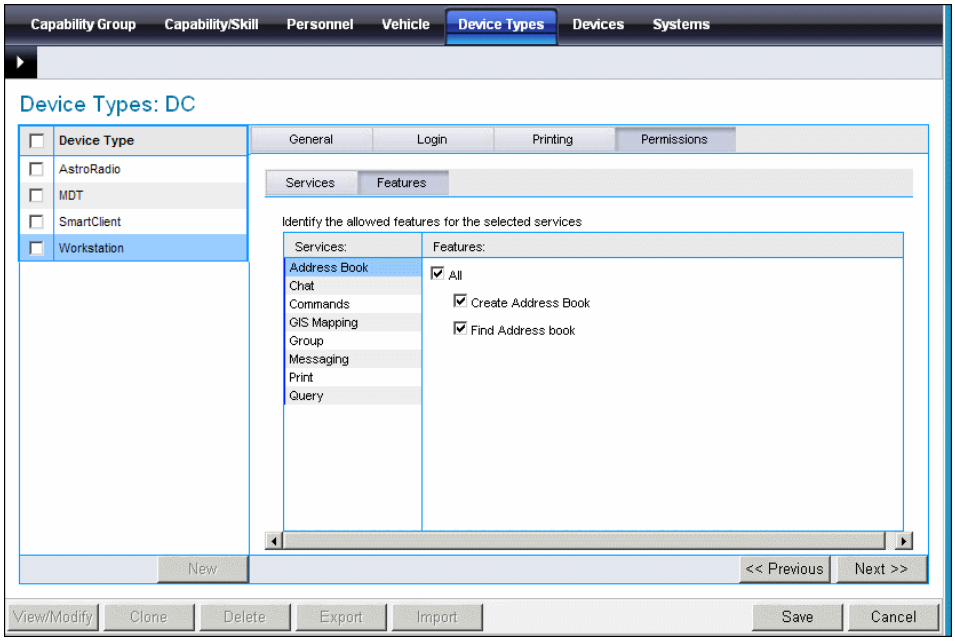


Figure 11-23 Device Types Form – Permissions Tab, Features Subtab

a. Select a service from the Services list on the Features subtab.

b. Select the associated features that you want available to all devices of this type.

c. Continue selecting services and features until you have associated features with all services for this device type.

For additional details on features, see “Adding Role Permissions” on page 8-5.

NOTE
If you also configure permissions for roles, the most restrictive permissions apply.

5. Click **Save**.

Adding Equipment

In addition to device types, you can add equipment types that may be needed by your agency. Equipment types can be assigned to personnel, vehicles, and units. Equipment type properties consist of a name and description.

To add equipment types:

1. From the navigation panel, select **Resources** and then select **Device Types**.

The Device Type form appears (see Figure 11-19).

2. Click the filter arrow.
3. Select **Add New**, then **Equipment Type**.
4. Click **OK**.

   The Equipment window appears.

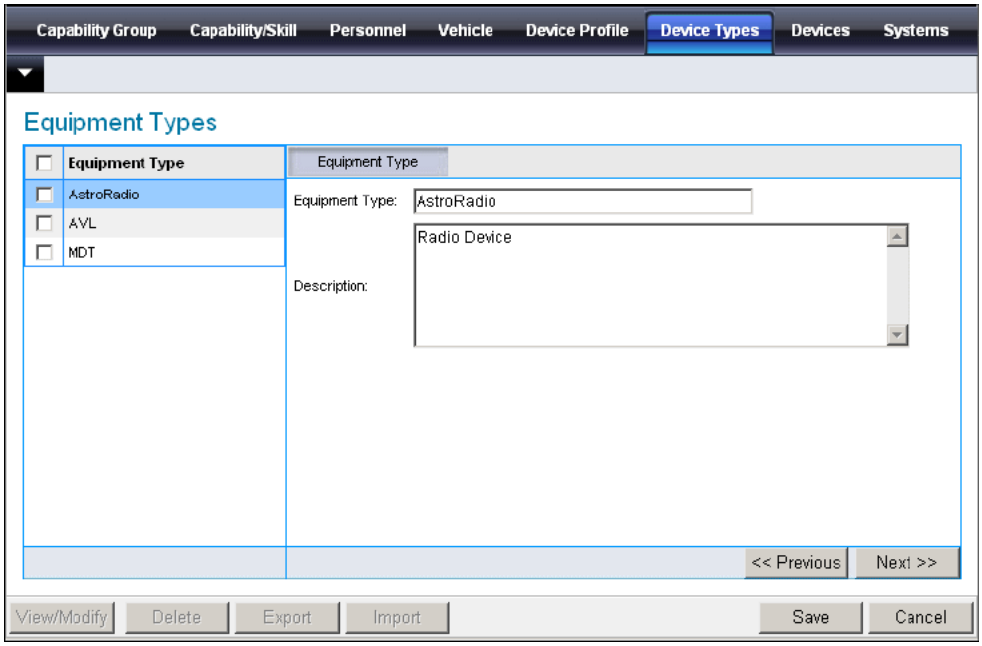


Figure 11-24 Device Types Window – Equipment Type Tab

5. Click **New**.
6. In the Equipment Type field, enter a name for the equipment type.
7. In the Description field, enter a description.
8. Click **Save**.

Configuring Devices

Use the Devices configuration item to configure properties of device types. Properties include general settings, login settings and permissions to services.

Devices are actual physical entities capable of executing CAD and mobile client software including workstation/mobile units, radios, 2-Tone Radio Groups, pagers, pager groups, printers, and GPS. Devices can be assigned to personnel, vehicles, or units and have some sort of device ID.

- Provision the *device type* when you want to configure settings for the entire group of workstations or mobile units.
- Provision the actual *device* when you want to configure settings for a specific instance of a device; for example, a specific workstation, a specific mobile unit, or a specific pager. For details on provisioning devices, see "Configuring Device Types" on page 11-34.

You can add, clone, modify, export, import, and delete devices. For information on cloning, exporting, importing, and deleting, "Working With Configuration Items" on page 2-9.

Configuring Workstation/MDT/Handheld Devices

Use the Workstation/MDT/Handheld configuration item to manage your agency's workstations, MDTs, Handheld, and Smart Client devices, and some interface settings.

When you add a workstation, MDT, handheld, smart client, or other equipment, you enter information on four tabs:

- General – Where you add or modify information about the type of device, the device name, description, addressability, make, model, serial number, position, FBR path, OS version, unique address, associated radio ID, and account status. You can also modify your CAD client screen size on this tab.
- Login Settings – Where you add or modify information about automatic login, concurrent logins, failed logins, login retries, the inactive timer, day or time restrictions, printing access, and offline mode for the device.
- Permissions – Where you select the services to assign to the device, and then select the features to allow for the selected service or services.
- Interface Settings – Where you provision the information for the CryWolf chronic false alarm interface and the Zetron 3030 Telecommunications Device for the Deaf (TDD).

You can add, modify, clone, import, and export and delete workstation/MDT/handheld devices and other equipment. For details on cloning, modifying, importing, exporting, and deleting workstations and MDTs, see “Working With Configuration Items” on page 2-9.

NOTE

For integration with radios, the user identities in PremierOne must match the user identities provisioned in UNS. The two systems are not kept in synchronization automatically. If the two lists of users do not match, users may not be able to send and receive messages.

Device identities are not provisioned in UNS, so administration of device identities in PremierOne controls only device messaging abilities. An unprovisioned device in PremierOne will not receive or send text messages successfully.

Radio devices can also be locked from a PremierOne the provisioning console. Locked devices cannot send and receive messages.

Adding Workstation/MDT/Handheld General Information

General information includes information about the type of device, the device name, description, addressability, make, model, serial number, position, FBR path, OS version, unique address, associated radio ID, and account status.

NOTE

Depending on the device type you select, different fields appear on the form.

To add devices general information:

1. From the navigation panel, select **Resources**.

   The Workstations/MDT/Handheld Devices form appears with the General tab in focus. A list of existing workstations/MDTs/handheld devices displays on the left side of the form.

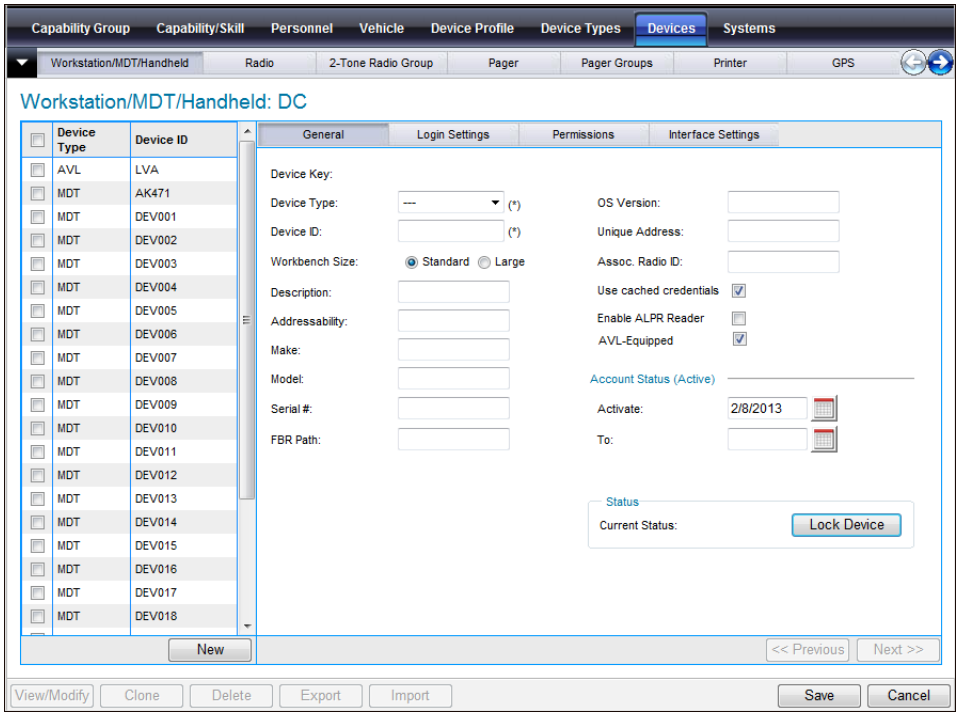


Figure 11-25 Workstation/MDT/Handheld – Add New

2. Click **New**.

3. From the Device Type list, select the device type and enter information appropriate to the device you are adding.

   The Device Type list includes any equipment that you may have added under the Device Types configuration item.

> **NOTE**
> Do not use the characters > or < in the Device ID field.

4. In the Workbench Size field, select **Large** to set your CAD client screen to a larger size that accommodates lengthy forms that otherwise require extensive scrolling in the default Standard screen size.

5. For the CAD signon screen to keep the default information of Agency, Role, and Coverage Groups select the **Use cached credentials** check box.

6. To enable Automatic License Plate Recognition (ALPR) for a mobile unit, select the **Enable ALPR Reader** check box.

> **NOTES**
> The Enable ALPR Reader field appears only for device type MDT.
> To set up automatic queries on ALPR hits, use the Query configuration item to select a query type to run and map the query type field to run the query on. For details, see “Configuring ALPR Automatic Queries” on page 31-54.

7. If the MDT is has AVL, make sure the **AVL-Equipped** check box is selected.

   This allows for reporting when the unit stops reporting its location. For details, see "Configuring GPS Cadence" on page 25-22.

8. In the Telephony section, do the following:

   NOTE
   The Telephony section appears only for device type Workstation.

   - If your system is only using TDD, select the **TDD Workstation** check box (selecting 911 Workstation automatically will automatically include TDD).
   - From the System list, select the 9-1-1 System that is being used.
   - In the Position ID field, enter the position ID for the workstation.
   - From the Intercom Lines list, select the intercom line for the workstation. You can add multiple lines.

     Intercom lines are added in "Configuring Incoming Line Types and Lines" on page 12-4.

9. In the Account Status (Active) section, select a date to activate the device account, and if appropriate, a date to deactivate the account.

10. You can lock a device by selecting the **Lock Device** button in the Status section.

11. Click **Save**.

Adding Login Settings Information

Login settings includes information about automatic login, concurrent logins, failed logins, login retries, the inactive timer, day or time restrictions, printing access, and offline mode for the device.

To add login settings information:

1. Access the form for a new workstation/MDT/handheld device. For instructions, see "Configuring Workstation/MDT/Handheld Devices" on page 11-43.

   The Workstations/MDT /Handheld form appears with the General tab in focus (see Figure 11-25). A list of existing devices displays on the left side of the form.

2. Select the Login Settings tab.

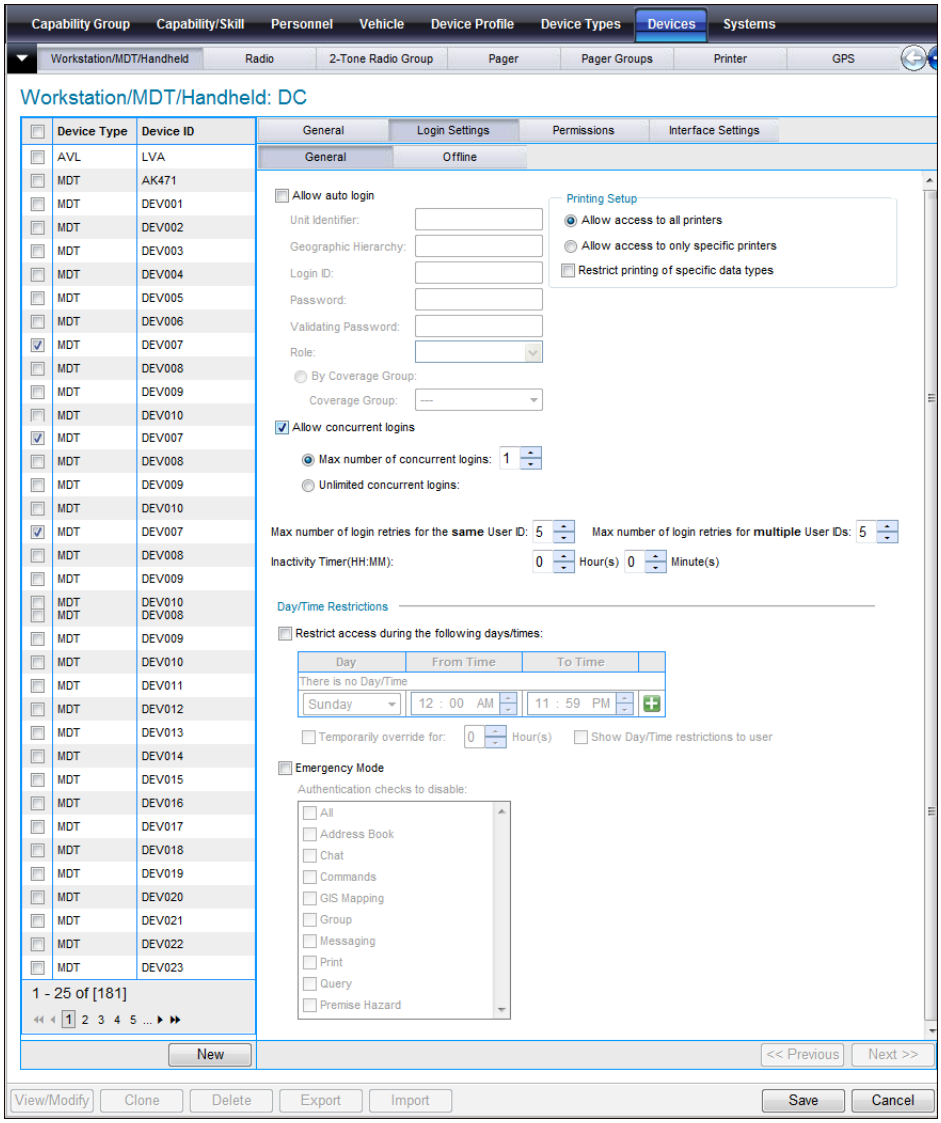


Figure 11-26 Workstation/MDT/Handheld – Login Settings Tab, General Subtab

3. On the General subtab, do the following:

   a. Select whether to allow auto login for the device. This feature is intended for fire units that want to be automatically logged in indefinitely.

      If you enable auto login, enter information for the fields below the Allow auto login field. The Geographic hierarchy is the area, sector, and beat or other geographic designation.

   b. Select whether to allow concurrent logins for this device.

      Concurrent logins allow users to login to more than one device at a time. Concurrent logins can be set for a device type in the Resources-Personnel configuration item, for an agency in the Authentication configuration item, and for a workstation in the Devices-Workstation item.

If a setting is in more than one of these places, all of the concurrent limitations are validated during login process. The most restrictive value will apply.

NOTE
Concurrent logons are not allowed for CAD workstations. The fields are disabled for workstations.

4. If you allow concurrent logins, select the appropriate field below the Allow auto login field.

   a. Enter the maximum number of failed logins and maximum number of login retries by multiple users for this device.

   b. Set the hour and minute settings for the inactive timer for this device.

   c. In the Printing Setup section, select the printing settings for this device.

   d. In the Day/Time Restrictions section, select any restrictions for this device.

      Select the **Temporary Override** check box and enter the number of hours for a potential override. This allows you to grant temporary access to the device in case of emergency.

5. In the Emergency section, select the services that can be accessed when the agency is placed in Emergency Mode (Authentication–Agency Setting–Emergency Mode) and the user cannot have the user's logon authenticated.

6. To allow offline mode, select the Offline sub tab.

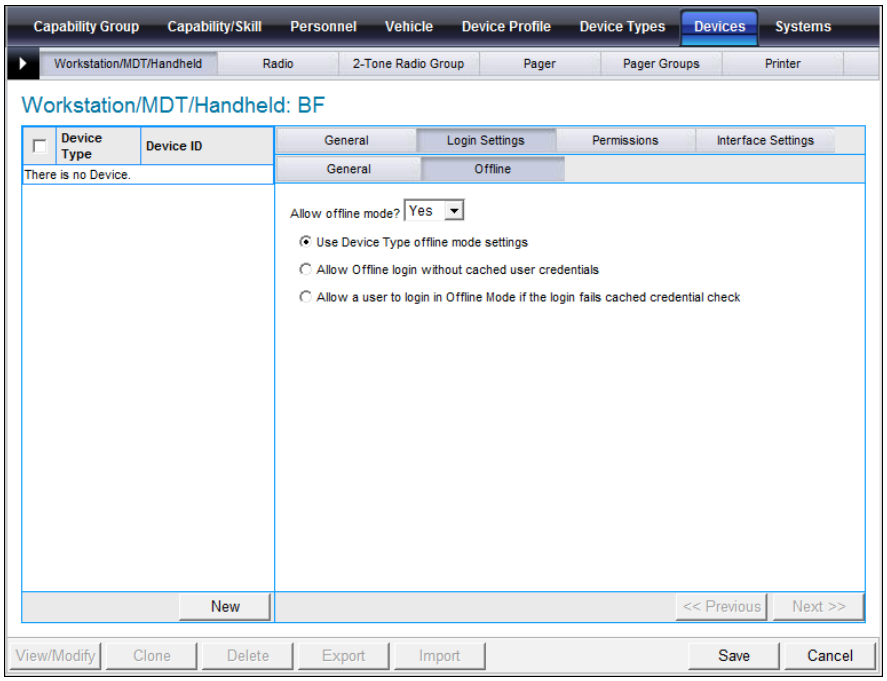


Figure 11-27 Workstation/MDT/Handheld – Login Settings Tab, General Subtab

7. From the Allow offline mode list, select **Yes**.

8. Select one of the following:

   - To use the device type offline mode settings, select the **Use Device Type offline mode settings** button.

     For details on the settings, see "Configuring Device Types" on page 11-34.

   - To allow offline login without cached user credentials, select the **Allow Offline login without cached user credentials** button.

   - To allow a user to login if the login credentials don't match cached credentials, select the **Allow a user to login in Offline Mode if the login fails cached credentials** button

9. Click **Save**.

Adding Permissions Information

Permissions is where you select the services to assign to the Workstation/MDT/Handheld device, and select the features to allow for the selected service or services.

To add permissions information:

1. Access the form for a new Workstation/MDT/Handheld device. For instructions, see "Configuring Workstation/MDT/Handheld Devices" on page 11-43.

   The Workstation/MDT/Handheld form appears with the General tab in focus (see Figure 11-25). A list of existing devices displays on the left side of the form.

2. On the Devices form, select the Permissions tab.

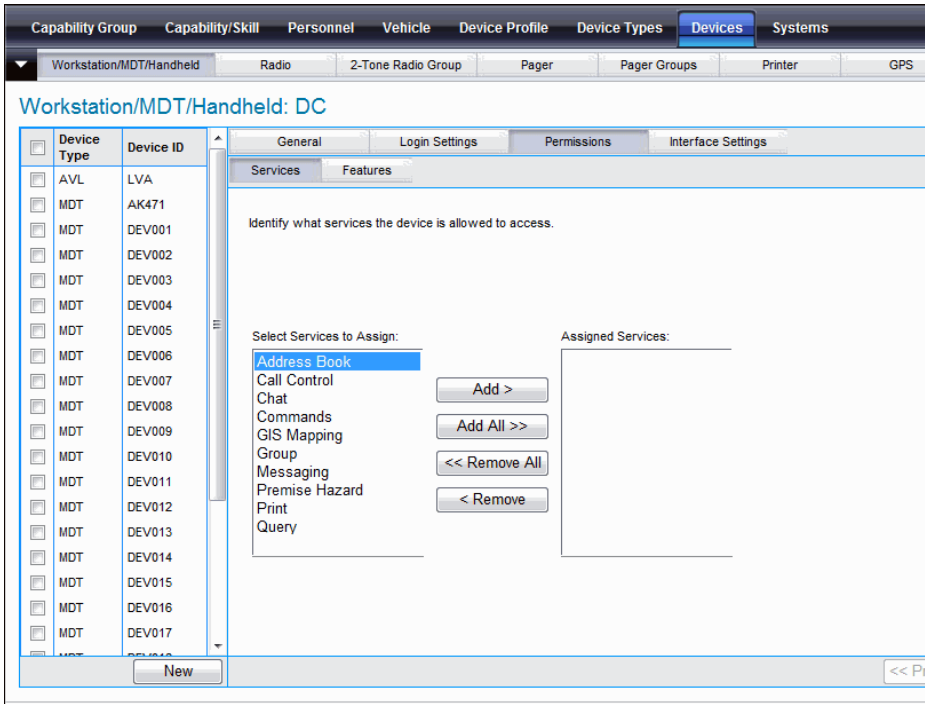


Figure 11-28 Workstation/MDT/Handheld – Permissions Tab, Services Subtab

3. On the Services subtab, select one or more services to assign to this device in the Select Services to Assign box and click the **Add** button to add the services to the Assigned Services list.

   For additional details on services, see “Adding Role Permissions” on page 8-5.

4. Click the Features subtab.

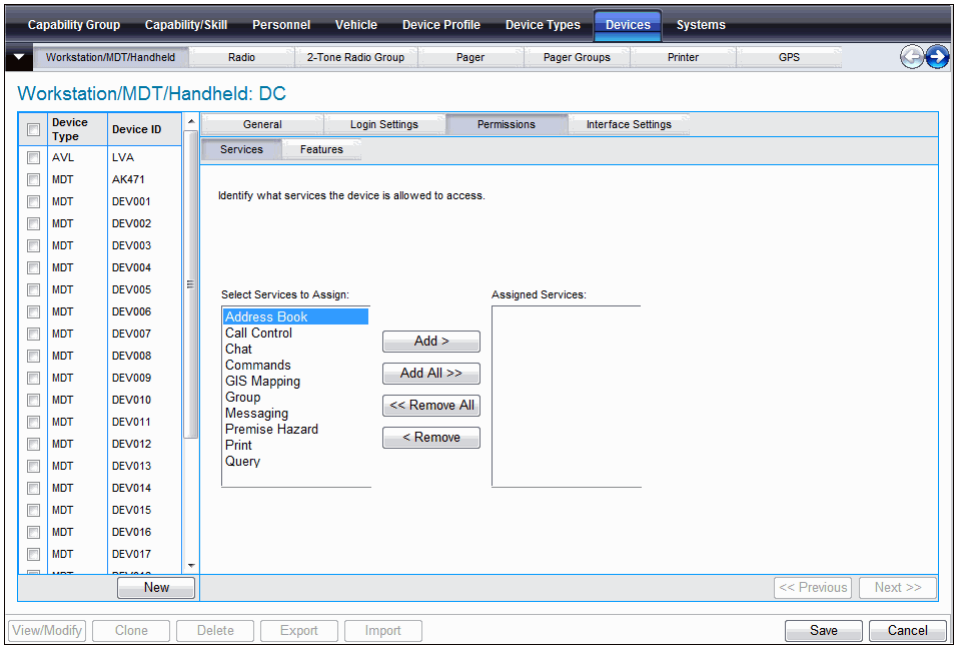


Figure 11-29 Workstation/MDT/Handheld – Permissions Tab, Features Subtab

5. On the Features subtab, do the following:

   a. Select a service from the Services list.

   b. Select the associated features that you want available to this device.

   c. Repeat for all services assigned to this device.

      For Call Control, the following options are available:

      - To allow a supervisor to listen to other calls without the call taker knowing that the call is being monitored, select **Call Control: Listen & Join**. The supervisor can join the call by selecting Join in the Call list.

      - To allow a user to type in a phone number and receive the ALI information, select **Call Control – Manual ALI query**.

      - To allow CAD and Mobile users (workstations and MDTs) that are not at a call taking workstation to view SMS and TDD transcripts, select **View SMS/ TDD Transcripts**.

   For details on features, see “Adding Role Permissions” on page 8-5.

6. Click **Save**.

Adding Interface Settings

Interface Settings is where you provision the information for the CryWolf false alarm interface and the Zetron 3030 Telecommunications Device for the Deaf (TDD).

The CryWolf® False Alarm Reduction application, by Public Safety Corporation, is a false alarm tracking system. PremierOne interfaces with CryWolf to gauge the appropriate response to an incoming Alarm incident reported to the call taker or dispatcher by an alarm monitoring company. If an incoming alarm is not identified as a chronic false alarm, an Alarm incident is created and the appropriate response occurs. However, if PremierOne identifies an incoming alarm as having generated a predetermined number of false alarms over a predetermined time period (for example, 3 false alarms in the last 12 months), then this particular alarm response may be handled with a different level of urgency. If a chronic alarm proves to be yet another false alarm, then your agency may bill the owner of the property for the response cost.

The Zetron® model 3030 provides a client-side TTY (text telephone)/TDD interface that passively monitors each emergency telephone call to detect if TDD modulation/demodulation is required. In the event that the Zetron 3030 detects a TDD calling tone, the Zetron unit answers the data call and notifies the call taker at his or her workstation that a TDD call is being received. The caller and call taker then converse via the keyboard and the conversation is displayed on the screen. The call taker can move to other windows and perform other tasks while the conversation is still in progress.

To provision CryWolf and Zetron 3030 interface information:

1. Access the form for a new Workstation/MDT/Handheld device. For instructions, see "Configuring Workstation/MDT/Handheld Devices" on page 11-43.

   The Workstation/MDT/Handheld form appears with the General tab in focus (see Figure 11-25). A list of existing devices displays on the left side of the form.

2. Select the Interface Settings tab.

   The CryWolf/Zetron 3030 form appears.

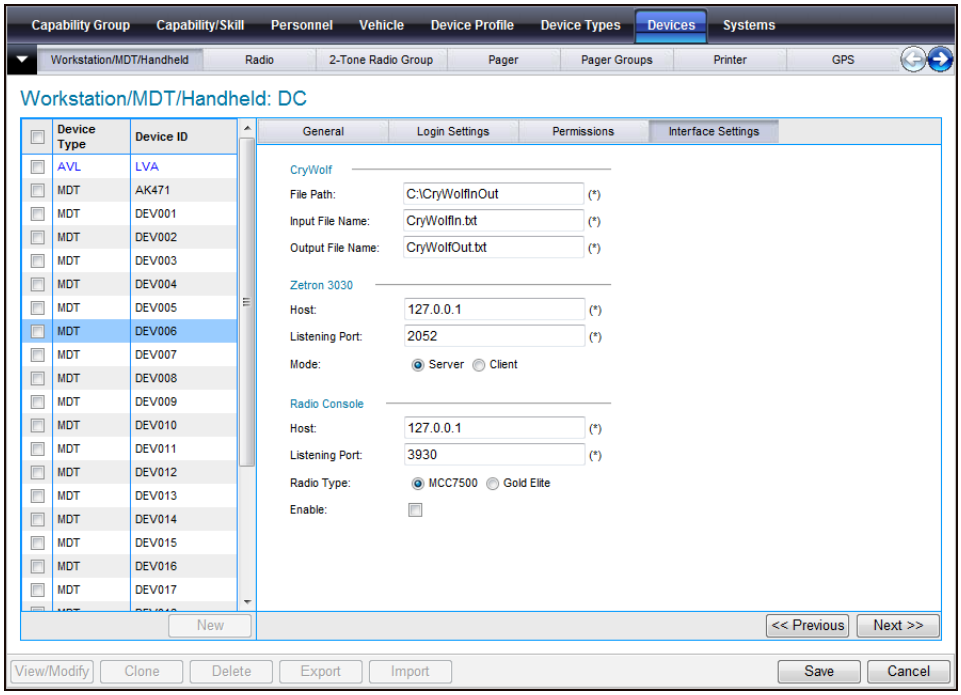


Figure 11-30 Workstation/MDT/Handheld – Interface Settings Tab

3. Click **View/Modify**.

4. To set up the CryWolf interface, do the following:

   a. In the File Path field, type the path to the location where you want the CryWolf documents to be stored when CryWolf reads and writes files; for example, `C:\CryWolf_InOut`.

   b. In the Input File Name field, type the name of the input file for CryWolf to use when it reads alarm details.

   c. In the Output File Name field, type the name of the output file for CryWolf to use when it writes a file for the specified address with an Alarm ID.

5. To set up the Zetron 3030 interface, do the following:

   a. In the Host field, type `127.0.0.1`.

      The Host field is the internal address of the CAD workstation used for the CAD client to communicate with the Premier TDD application. Always use `127.0.0.1` unless told otherwise by Motorola.

   b. In the Listening Port field, type `2052`.

      The Listening port is the port that is used for the CAD client to Premier TDD communication. Always use `2052` unless told otherwise by Motorola.

c. In the Mode field, select **Server**.

Server mode is the normal mode for the Zetron 3030 interface and is how the CAD client listens for information sent from TDD.

Client mode is a supported mode by the CAD client for general TCP/IP configuration and support. You should not need to use this setting for Zetron 3030.

6. To set up the Radio Console interface, do the following:

a. In the Radio Type field, select the type of radio you are using.

b. In the Enable field, check the box to enable the radio.

c. Do not change the following default values:

In the Host field, do not change the default value of `127.0.0.1`. The Host field is the internal address of the CAD workstation used for the CAD client to communicate with the radio interface. Always use `127.0.0.1` unless told otherwise by Motorola.

In the Listening Port field, do not change the default value of `3930`. The Listening port is the port that is used for the CAD client to radio console communication. Always use 3930 unless told otherwise by Motorola.

7. Click **Save**.

Refreshing PremierOne from CryWolf

When PremierOne receives a Refresh file from CryWolf, all records are deleted from the database and only the address-validated records in the Refresh file are added to the refreshed database. If a database is used across multiple agencies where some user-defined Alarm records exist, PremierOne deletes those records.

Using the CryWolf Configuration File

In addition to the provisioning of CryWolf you have done here, you also need to be aware of the settings available in the Configuration module in the System Management Tool Portal. For more information, see the Configuration chapter in the *PremierOne System Administrator Guide*.

Configuring Radios

Radio information is contained on one tab and consists of basic identification settings and the radio assignment. Radio devices are provisioned to associate them with a unit and a radio channel.

You can use the Filter to search for radios by agency, alias, ID, or RIN.

You can add, modify, export, import, clone, and delete radios. For details on modifying, importing, exporting, deleting and cloning radios, see "Working With Configuration Items" on page 2-9.

Adding Radios

Information for radios consists of general identification information, description, device profile, make and model, activation dates, any radio assignment information, and the status of the radio. Depending on the system, either the device ID or unit ID will display for the logged in status.

To add a radio:

1. From the navigation panel, select **Resources**.
2. Select **Devices**, and then select **Radio**.

   The Radios form appears. A list of existing radios displays on the left side of the form.

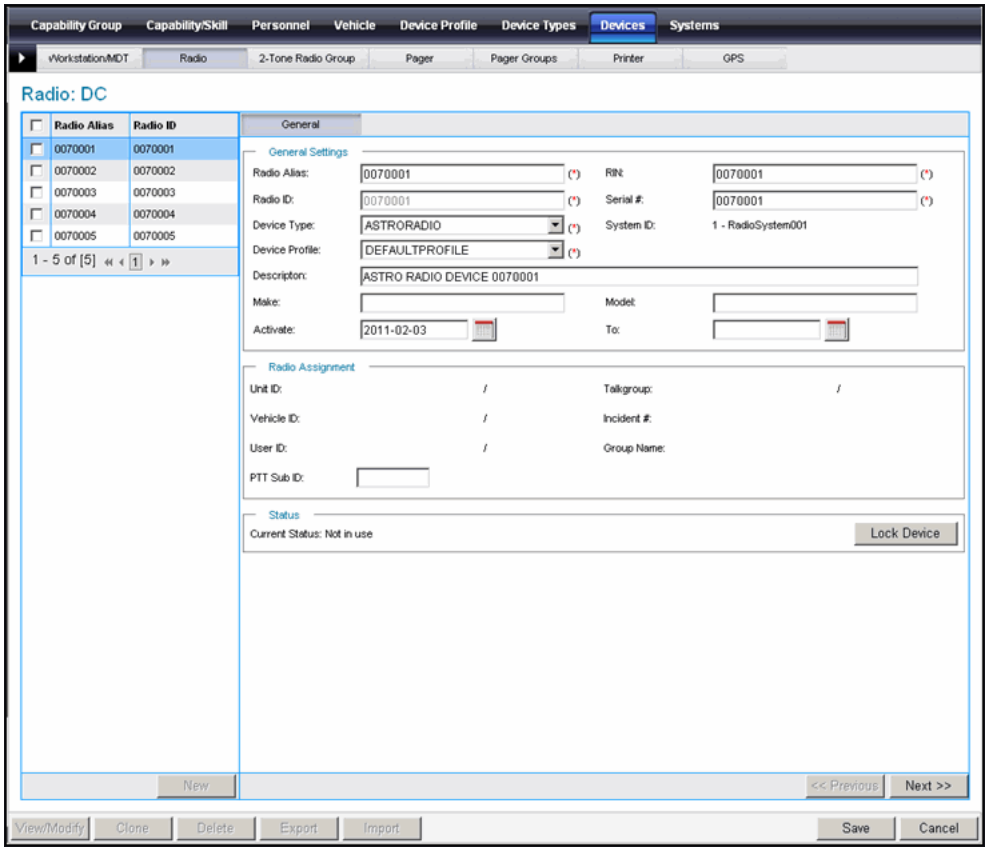


Figure 11-31 Radio Form

3. At the bottom of the radios list, click the **New** button.
4. In the Radio Alias field, enter an alias for the radio.

5. In the RIN field enter the Radio Identification Number (RIN) for the radio.

   This ID is usually an inventory ID that is used to internally track the equipment and can also be the label on the radio when appropriate.

6. In the Radio ID field, enter the Electronic ID code that allows the radio system to recognize the radio.

   This value is how the radio will be referenced.

7. In the Serial # field enter the serial number for the radio.

8. From the Device Type list, select the device type.

9. From the Device Profile list, select the device profile.

   Device profiles are defined in the Resources–Device Profile configuration item. For details, see “Configuring Device Profiles” on page 11-22.

10. In the Description field, type a description for the radio.

11. In the Make and Model fields, enter the make and models for the radio.

12. In the Activate and To fields enter the beginning and ending activation dates for the radio.

    The current radio assignment displays below the Activate fields and is read-only. The Talkgroup ID is an assignment made in the Radio system and the Group ID is the Radio Talkgroup ID in CAD.

    Radio assignments can be made here, or in the Resources–Personnel, Resources–Vehicle, Resources–Unit items or in CAD when you place a unit on duty.

13. Click **Save**.

> **NOTE**
> You can lock/unlock a device by selecting the Lock Device/Unlock Device button in the Status section.

Configuring Two-Tone Radio Groups

Use the Two-Tone Radio Group configuration item to add two-tone radio and pager groups.

You can add, modify, export, import, clone, and delete pager groups. For details on modifying, importing, exporting, deleting, and cloning pagers, see “Working With Configuration Items” on page 2-9.

To configure two-tone pager groups:

1. From the Navigation panel, select **Resources**.
2. Select **Devices**, and then select **Two-Tone Radio Group**.

   The Two-Tone Radio Group form appears with a list of any existing two-tone radio groups on the left side of the form.

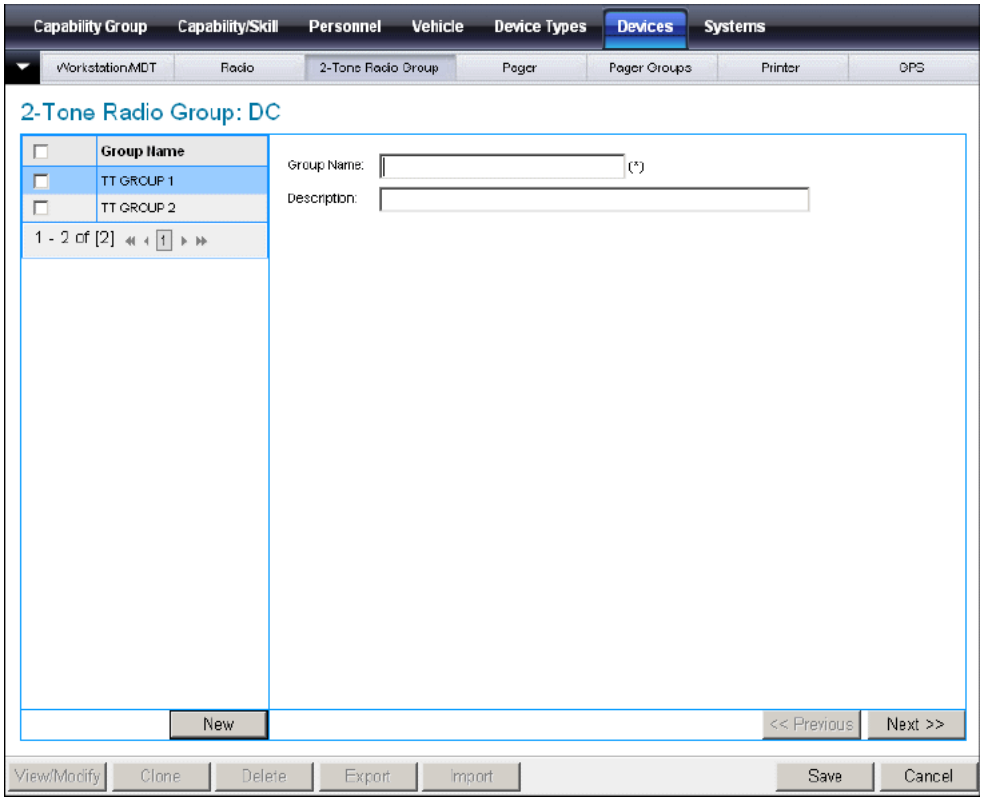


Figure 11-32 Two-Tone Radio Group Form

3. Click **New** at the bottom of the form.
4. In the Group Name field, type the name of the two-tone radio group.
5. In the Description field, type a description for this group.
6. Click **Save**.

Configuring Pagers

Use the Pager configuration item to manage your agency's pagers.

You can add, modify, export, import, clone, and delete pagers. For details on modifying, importing, exporting, deleting, and cloning pagers, see "Working With Configuration Items" on page 2-9.

Adding Pagers

Add a pager when your agency obtains a new pager. Modify a pager when you need to change anything other than the Pager Name or Serial # fields. You cannot change the Pager Name or Serial # values. You must delete the record if the Pager Name or Serial # values are no longer valid.

To add or modify a pager:

1. From the navigation panel, select **Resources**
2. Select **Devices**, and then select **Pager**.

   The Pager form appears with a list of existing pagers on the left side of the form.

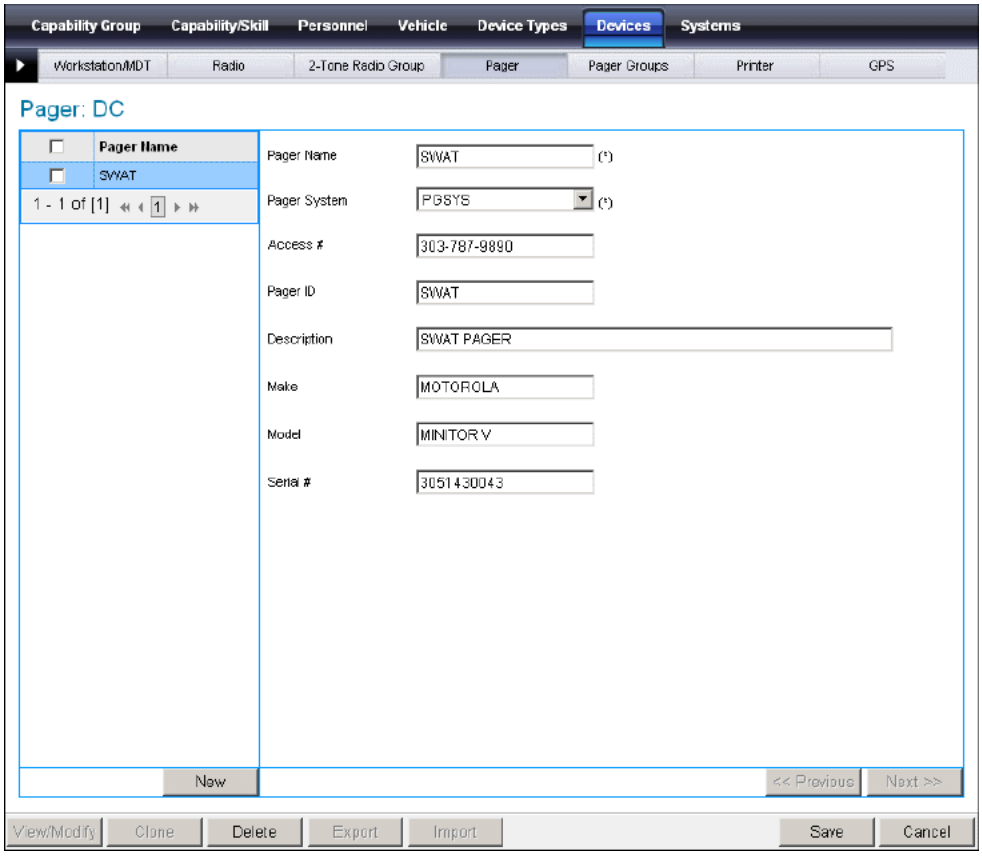


Figure 11-33 Pager Form

3. In the Pager Name field, type the name by which the pager is commonly called.
4. From the Pager System list, select the Pager System.
5. In the rest of the fields, type or change the information specific to the pager.
6. Click **Save**.

Configuring Pager Groups

Use the Pager configuration item to manage your agency's pager groups. Pager groups are used by the toning command (TN) to send the same information to a set of pagers using the pager group name.

You can add, modify, export, import, clone, and delete pager groups. For details on importing, exporting, deleting, and cloning pagers, see "Working With Configuration Items" on page 2-9.

Adding Pager Groups

Pager Group information is on one tab.

To add a pager group:

1. From the navigation panel, select **Resources.**
2. Select **Devices**, and then select **Pager Groups**.

   The Pager Groups form appears with a list of existing pager groups on the left side of the form.

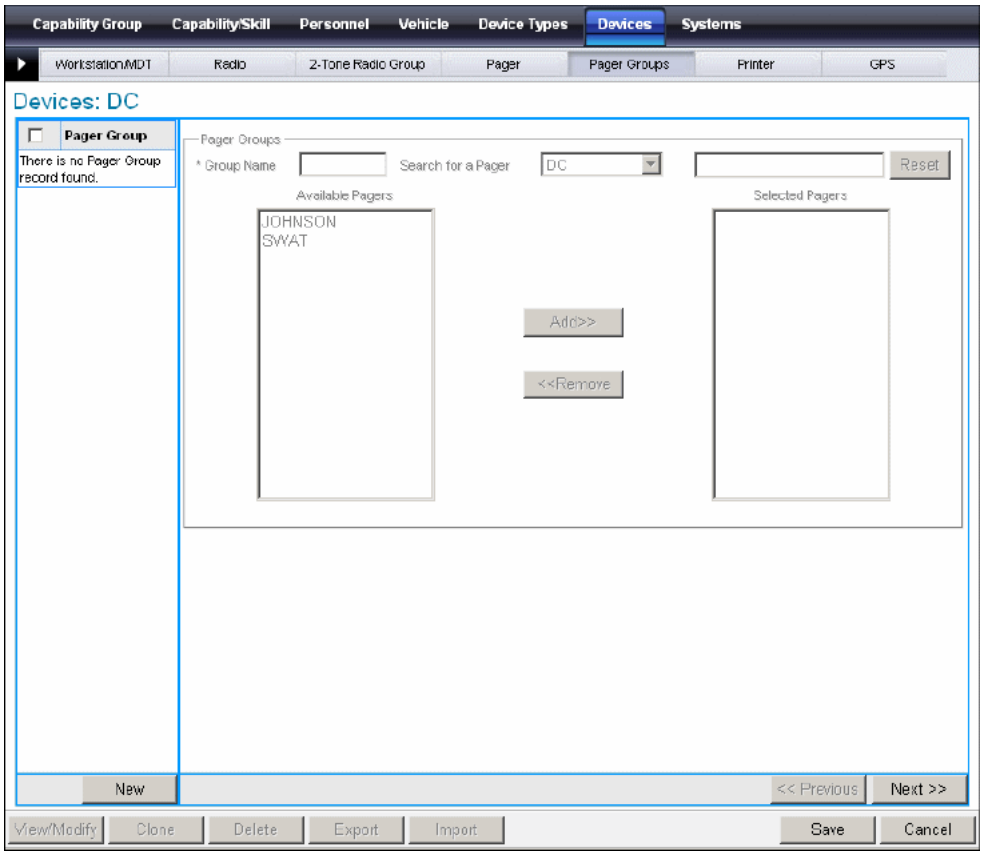


Figure 11-34 Pager Group Form

3. Click **New** at the bottom of the Pager Group list.

4. In the Group Name field, type a name for your new pager group.
5. To add a pager to a pager group by searching:
   a. From the first Search for a Pager field, select the agency that owns the pager.
   b. From the second Search for a Pager field, type at least the first part of the pager name; for example, SGT for pager SGT06, or PAGER for PAGER10.

      As you add search criteria to the second field, results display in the Available Pagers list.
   c. To clear the search criteria in the search fields, click **Reset**.

      The list of Available Pagers displays the default list of all available pagers.
6. Click **Save**.

Configuring Printer Devices

Use the Printer configuration item to manage your agency's printers.

You can add, and delete printers. For details on deleting printers, see "Working With Configuration Items" on page 2-9.

To configure printers for devices:

1. Access the form for printers.

   The Printer form appears. A list of existing printer names displays on the left side of the form.

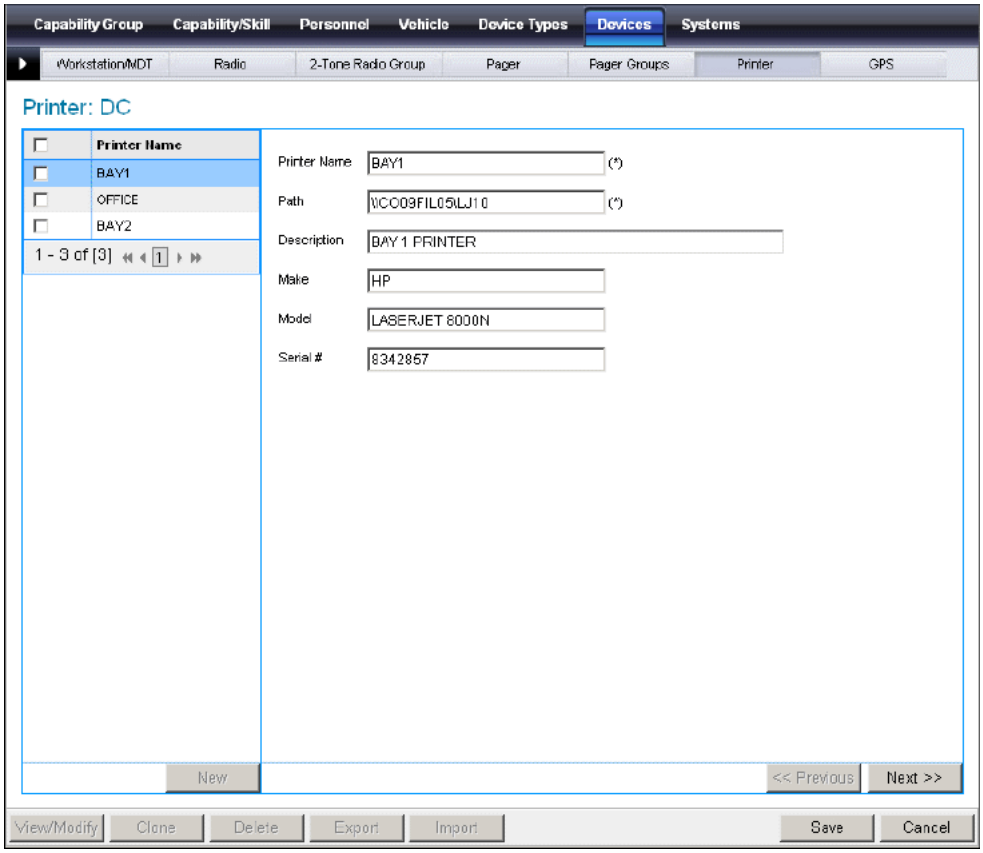


Figure 11-35 Printer Form

2. Click **New** at the bottom of the Printer Name list.
3. In the Printer Name field, type a name for your new printer.
4. In the Path field, type the path to the network printer.

   Example:

   \\server\printer

5. Fill in the rest of the fields as shown.
6. Click **Save**.

Configuring a Tear and Run Printer in a High Availability (HA) Environment

In addition to the standard configuration information given in “Configuring Printer Devices” on page 11-61, the following criteria must be met:

- All users who will be printing to the Tear and Run printer must have permission to use that printer. This is done from the Windows configuration settings.
- Each application server in an HA environment needs to have the same printer or printers defined, each with a different IP address. For example, if there are ten network printers, each application server must have all ten printers defined. Each application server acts as a print server for CAD clients that are connected to that application server when that CAD client requests a Tear and Run print. The request goes from the CAD client to the application server and then to the specific network printer.
- If there is a disaster recovery site, the servers at the disaster recovery site must be set up with the same printers.
- The application servers must have the ability to access the network printers.

The following script is a script for a single printer – an `HP LaserJet 1320 PCL 5E` printer with a **Device ID** of `STA01-TnR` and a **Location** of `Fire Station 1`. You run a script on each application server. The requirements to run a script are:

- IP Address of the network printer or printers (in this case, `170.190.175.155`)
- Name of the printer driver or drivers to be associated with the network printer(s) (in this case, `HP LaserJet 1320 PCL 5E`)
- Name to be assigned to the network printer(s) (in this case, `STA01-TnR`)
- Location of the network printer (in this case, `Fire Station 1`)

In addition, at least one network printer using this print driver must already have been installed.

```
'On Error Resume Next

'SETS 'LOAD DRIVER' PRIVILEGE.

Set objWMIService = GetObject("Winmgmts:")

objWMIService.Security_.Privileges.AddAsString
"SeLoadDriverPrivilege", True


'-------------------------------------------------------------
----------------------------------------

'STA01

'SETS PRINTER PORT.

Set objNewPort = objWMIService.Get _
```

```
                    ("Win32_TCPIPPrinterPort").SpawnInstance_
objNewPort.Name = "STA01_170.190.175.155"
objNewPort.Protocol = 1
objNewPort.HostAddress = "170.190.175.155"
objNewPort.PortNumber = "9100"
objNewPort.SNMPEnabled = False
objNewPort.Put_
'SETS PRINTER TO PORT.
Set objPrinter = objWMIService.Get _
                    ("Win32_Printer").SpawnInstance_
objPrinter.DriverName = "hp LaserJet 1320 PCL 5e"
objPrinter.PortName = "STA01_170.190.175.155"
objPrinter.DeviceID = "STA01-TnR"
objPrinter.Location = "Fire Station 1"
objPrinter.Network = True
objPrinter.Shared = False
'objPrinter.ShareName =
objPrinter.Put_
'------------------------------------------------------------
----------------------------------------
```

Configuring GPS Devices

GPS devices must be created and their IDs mapped to an appropriate unit ID for the vehicle in which the device is assigned. You can provision GPS devices to work through PremierOne Mobile to the vehicle modem, or directly to the vehicle modem.

In deployments where tracing off-duty units is desired and the PremierOne Mobile Client is present, Motorola Solutions strongly recommends separate GPS devices be used for each purpose. Even if a single GPS device has the ability to direct its output to both PremierOne Mobile and directly to PremierOne Server, it may not have the ability to support discrete reporting rates for each channel, which could have negative impact on bandwidth or PremierOne Mobile Client response.

Use the GPS configuration item to manage your agency's GPS devices.

You can add, modify, import, export, clone, and delete GPS device IDs. For details on importing, exporting, cloning, and deleting GPS device IDs, see "Working With Configuration Items" on page 2-9.

GPS Through PremierOne Mobile

PremierOne receives information from a vehicle-mounted GPS device using a logged-in PremierOne Mobile or Premier MDC client session. Because the processing of GPS information is dependent on the Mobile client, there is no way to track the vehicle after an officer signs off of the Mobile client session, closes the Mobile client application, powers down or removes the MDT, or if the vehicle is not regularly equipped with a Premier MDC or PremierOne Mobile client.

Direct GPS

Direct GPS communication can be used without PremierOne Mobile, or with PremierOne Mobile. By adding a suitable in-vehicle GPS device to communicate directly with the PremierOne Server (through a Trimble Direct adapter), position information can be recorded within a historical database. This information displays on the CAD mapping client when the vehicle is associated with an on-duty unit, and allows historical data recorded for the device to be searched.

NOTE

In deployments where tracking off-duty units is desired and the PremierOne Mobile Client is present, Motorola Solutions recommends using separate GPS devices for each purpose. Even if an individual GPS device has the ability to direct its output to both the PremierOne Mobile Client and directly to the PremierOne Server, it may not have the ability to support discrete reporting rates for each channel. The result is a negative impact on either bandwidth utilization or the Mobile Map user experience.

Adding GPS Devices

Normally the GPS device is configured before configuring PremierOne. This is typically done using a GPS configuration utility provided by the vendor. The following must be configured on the GPS device:

- Identification number – A user-assigned identification number that contains a unique combination of four alphanumeric characters. This value is used as the device ID for the Trimble Direct GPS device. (Refer to the TAIP “ID” command).
- Reporting Mode – A flag to indicate the report mode (ID-Flag). An Identification number is not included in location reports by default. Modify the reporting mode to enable the “ID_FLAG”. (Refer to the TAIP “RM” command).
- Default Reporting Rate – The default reporting rate for the Position/Velocity report (Refer to the TAIP “PV” command).
- IP Address and Port of Trimble Direct adapter – The IP Address and Port of the Trimble Direct adapter to which the GPS device send its location reports. This is provided by Motorola Solutions.

To add a GPS device:

1. From the navigation panel, select **Resources**.
2. Select **Devices**, and then select **GPS**.

The GPS form appears with a list of existing GPS devices on the left side of the form.

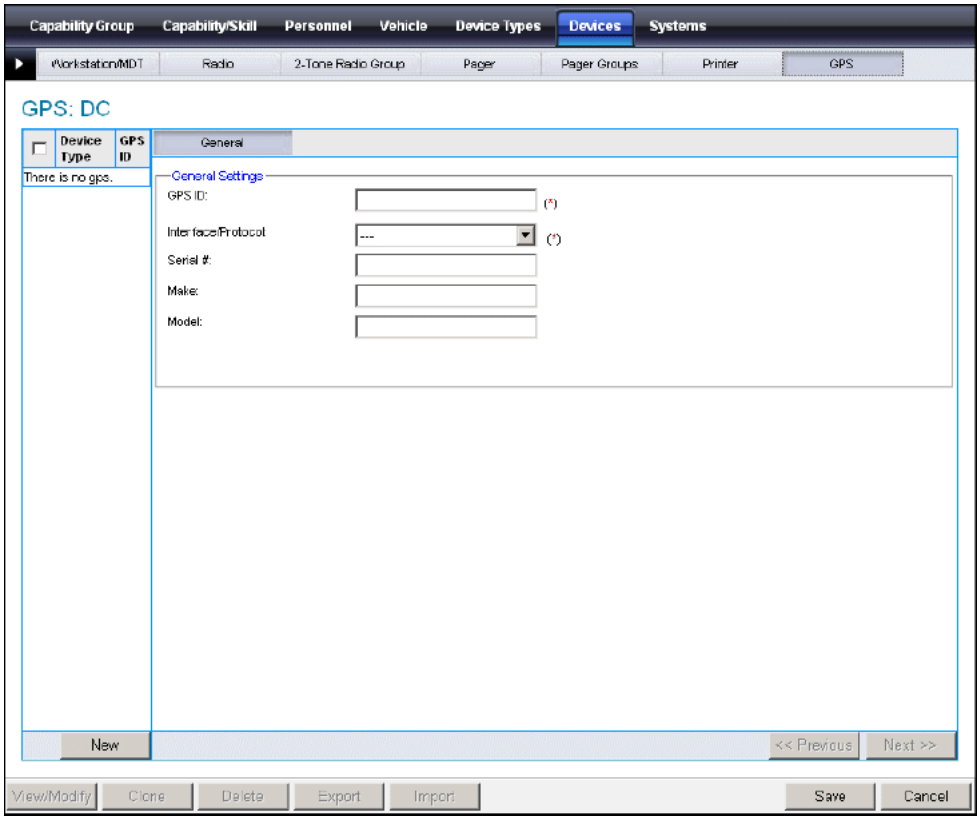


Figure 11-36 GPS Form

3. At the bottom of the GPS device list, click **New**.
4. In the Device ID field, type a numeric ID for the GPS device. This is the four-alphanumeric characters configured for the GPS device by the vendor utility.
5. From the Interface/Protocol field, select the interface or protocol used for this device.

   The Trimble Direct selections is used for GPS devices that send location report data directly to the PremierOne ARL service. For details on configuring the cadence for trimble-equipped units, see “Configuring GPS Cadence” on page 25-22.
6. In the Serial # field, type the serial number of the GPS device.
7. In the Make field, type the make of the GPS device.
8. In the Model field, type the model of the GPS device.
9. Click **Save**.
10. If you want to assign the GPS unit to a vehicle, do the following:

    a. In Resources, select **Vehicle**.

The Vehicle form appears.

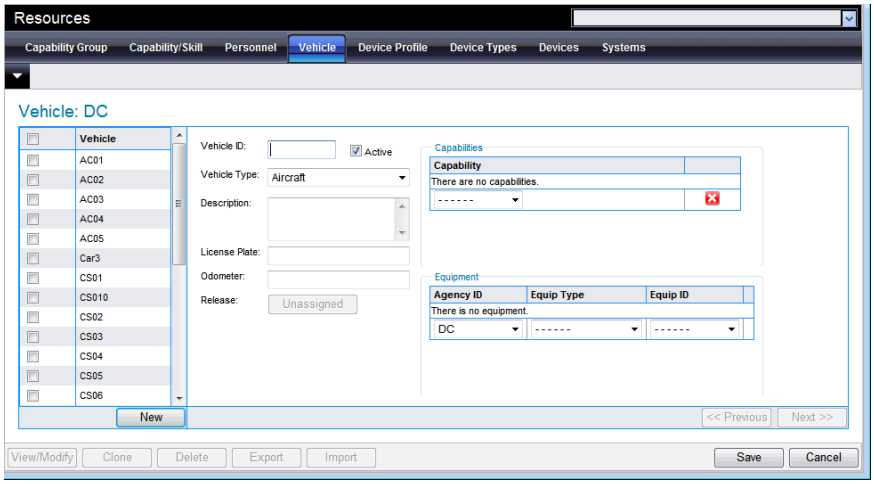


Figure 11-37 Vehicle Form

b. In the Equipment area, click **Equip Type**, and select the GPS type.

c. In the Equipment area, click **Equip ID**, and select the GPS ID.

11. Click **Save**.

Configuring Systems

Use the Systems configuration item to add new 9-1-1, TDD, or other systems.

You can add, modify, delete, and clone systems. For details on deleting and cloning systems, see “Working With Configuration Items” on page 2-9.

Adding Systems

Add a system when you get a new 9-1-1, Paging, TDD, or Toning system that needs to be configured globally so that multiple agencies can use the system.

To add a system:

1. From the navigation panel, select **Resources**, and then select **Systems**.

The Systems form appears with the 911 tab in focus. A list of existing 911 servers displays on the left side of the form.

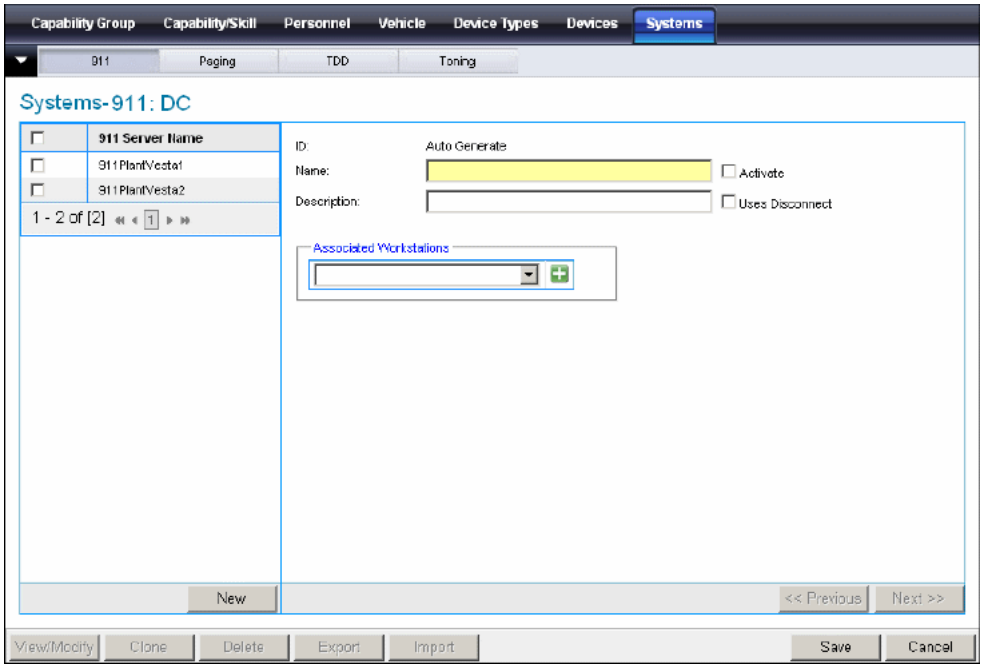


Figure 11-38 Systems Form – 911 Tab

2. To add a 9-1-1 server, do the following:

   a. At the bottom of the 911 Server list, click the **New** button.

      The ID field is generated by PremierOne.

   b. In the Name field, type the name of the new 9-1-1 system.

   c. In the Description field, type a description of the new system.

   d. Select whether to activate the system.

   e. Select whether the system uses disconnect (this does not apply to NG 9-1-1 systems).

   f. In the Associated Workstations box, select a workstation to associate with the 9-1-1 system.

   g. Click the plus symbol to the right of the associated workstation to save the entry and add another row.

      CAUTION
      If you do not click the plus symbol, PremierOne does not save the associated workstation, even after you click Save.

   h. Repeat the procedure for any other systems.

Each unsaved system appears in the System list in blue text.

i. Click **Save**.

3. To add a Paging system, do the following:

   a. Click the Paging tab.

   b. Click **View/Modify.**

   c. In the Paging System Name field, type the name of your paging system.

      The System ID is automatically generated when a new form is displayed. It is a read-only field.

   d. In the Paging Interface field, select the type of interface.

   e. In the Description field, type a description for this paging system.

4. To add a TDD system, do the following:

   a. Click the TDD tab.

   b. In the Name field, type the name of the TDD system.

   c. In the Description field, type a description for the TDD system.

   d. Click **Save**.

5. To add a toning system, do the following:

   a. Click the Toning tab.

   b. Click **View/Modify.**

   c. In the Toning System Name field, type the name of your toning system.

   d. In the Toning System Code field, select the code for this system.

      Each system much have a unique code.

      The System ID is automatically generated when a new form is displayed. It is a read-only field.

   e. In the Toning Interface field, select the type of interface for this toning system.

   f. In the Description field, type a description for this toning system.

6. For Tear and Run only, ensure that all users who will be printing to the Tear and Run printer have permission to use that printer. This is done from the Windows configuration settings.

7. To configure the 911, Paging, or Toning system, do the following:

   a. Click **View/Modify**.

   b. From the list on the left, select the system you need to configure.

   c. In the main window, copy the ID or System ID.

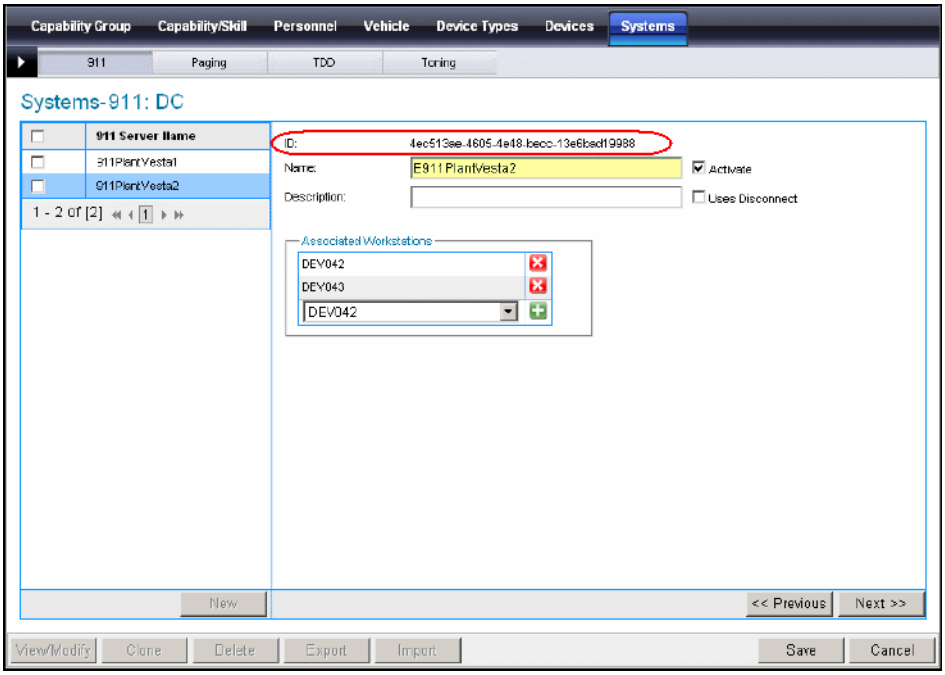


Figure 11-39 E911 ID Field

   d. From the **View** menu, select **Web Portal**.

e. Select the **Configuration** module.

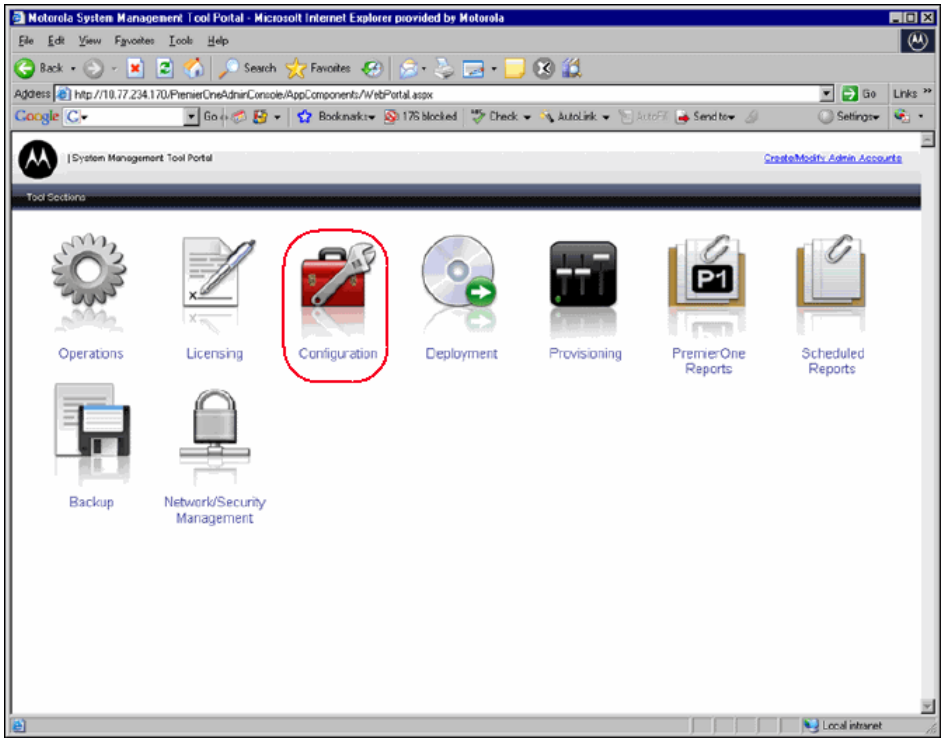


Figure 11-40 System Management Tool Portal – Configuration Module

f. Click the Edit tab.

g. Do one of the following:

1) For E9-1-1, select `E911\E911_config.xml`.

2) For Paging, select `Pager_Pager_config.xml`.

3) For Toning, select `Toning\Toning_config.xml`.

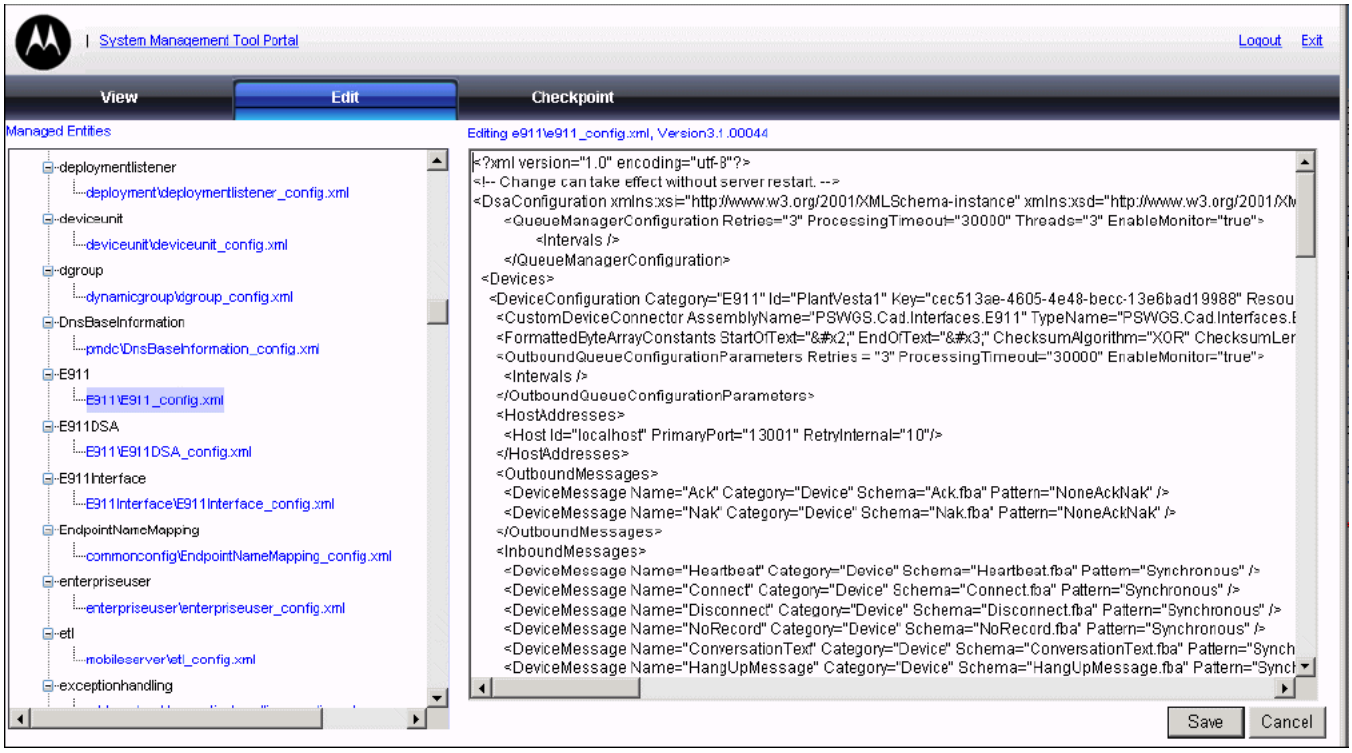


Figure 11-41 E911_config.xml File

h. Paste the ID or System ID that you copied into the Key attribute value.

i. Change the Host ID and PrimaryPort attribute values.

For most installations, the values will be your Lantronix ID and the Lantronix port number. If you are not using Lantronix, the values will be your external IP address and port number.

j. Save the file.

k. For Toning only, do the following:

1) Access `Toning\Toningdsa_config.xml`.

2) Locate the toning system used by your agency.

3) Set the add key values, such as PAOnTimer, and so on. The time is in milliseconds; therefore 60000 milliseconds = 60 seconds and 20000 milliseconds = 20 seconds.

4) Save the file.

5) Access `Toning\Toning_config.xml`.

6) Locate the following element:
```
<DeviceConfiguration Category “Toning”
id=“Zetron26”...
```

7) Under the <InboundMessages> element, locate the following element:
```
<Device Message Name=“NULLPacket” Category=“Device”
Schema=“NULLPacketfba” Pattern=“Synchronous” />
```

8) Replace the <Device Message Name=“NULLPacket”... element with the following:

```
<Device Message Name=“ALARM1” Category=“Device”
Schema=“Alarm1fba” Pattern=“NoneAckNak” />
```

9) Add the following element immediately after the element in step 8:

```
<Device Message Name=“ALARM2” Category=“Device”
Schema=“Alarm2fba” Pattern=“NoneAckNak” />
```

CHAPTER 12

Call Control

PremierOne integrates with the existing vendor's NG9-1-1 customer premise equipment to provide an interface for setting up NG9-1-1. PremierOne does not directly communicate with the phone company equipment to enable NG9-1-1 functionality.

The Call Control configuration item contains the following:

- General – Where you set the time before a call is considered to be on hold too long or the time in which a text message has not received an update.
- Debounce Factor – Where you set the amount of time used to prevent the user from performing the same or another phone function before the back-room telephony system is able to accept the command. Depending on the age of your telephony system, this is usually less than a second (older systems need longer to respond).
- Incoming Line – Where you configure the incoming lines; the lines must match the lines configured in the CPE (customer present equipment).
- Incorrect ALI – Where you can view and print reports for incorrect ALI numbers received by the CAD client.
- Intelligent Transfer – Where you provision service providers for transferring voice calls.
- Preprogrammed Messages – Where you can create preprogrammed messages for text messages and TDD (Telecommunication for the Deaf).
- Window – Where you configure the Call Control window and the associated Queue buttons, and set the roles and workstations that have permissions to access the window.

Configuring General Call Control Settings

General Call Control settings include the time before a call is considered to be held too long and the time in which a text message has not received an update before a notification is issued. Notifications are configurable. For details, see “Adding Windows Alerts Information” on page 32-44.

To configure General Call Control settings:

1. From the navigation panel, select **Call Control**, and then select **General**.

   The General tab appears. Sections are available for Voice Calls and for SMS conversations.

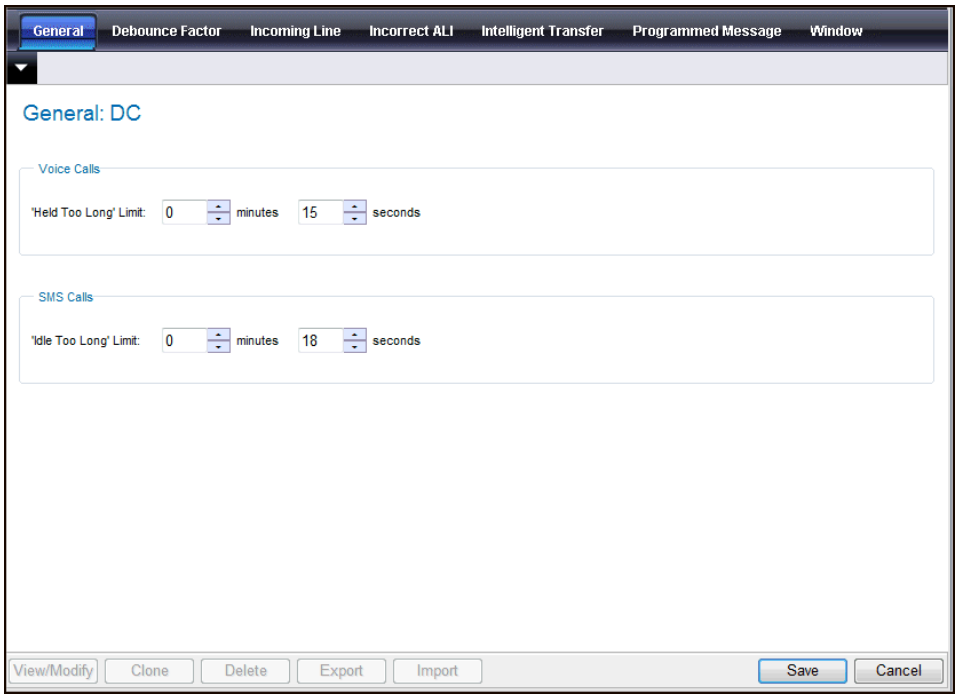


Figure 12-1 Call Control Form – General Tab

2. In the Voice Calls section, set the time before a call is considered to be held too long.

   The user receives a notification when the call exceeds the specified time. To disable this timer, set the timer to 60 minutes.

3. In the SMS Calls section, set the time before a text message is considered to be idle for too long.

The user receives a notification when a text message has been idle for the specified time. The notification does not terminate a text conversation, but only indicates to the user that the conversation has been idle longer than the set time and further action may be needed. To disable this timer, set the timer to 60 minutes.

4. Click **Save**.

Configuring the Debounce Factor

Certain functions that manipulate the phone system require a noticeable amount of time to complete. The phone system requires this lag time to process requests. During this time, users may attempt to repeat the same or a different function. Repeating a request or performing another request before obtaining the results of the last or initial request can cause further delay in processing.

To prevent this issue, you can set a time interval called the Debounce Factor. This interval is used to prevent the user from performing the same or another phone function while the previous action completes. The provisioning of this factor is made at a system-wide level.

The Debounce Factor also applies to CAD commands that interact with the telephony system (the factor is never applied to any function that does not rely upon response from the telephony system).

To configure the Debounce Factor:

1. From the navigation panel, select **Call Control**, and then select **Debounce Factor**.

The Debounce Factor tab appears. A field displays for the debounce factor.

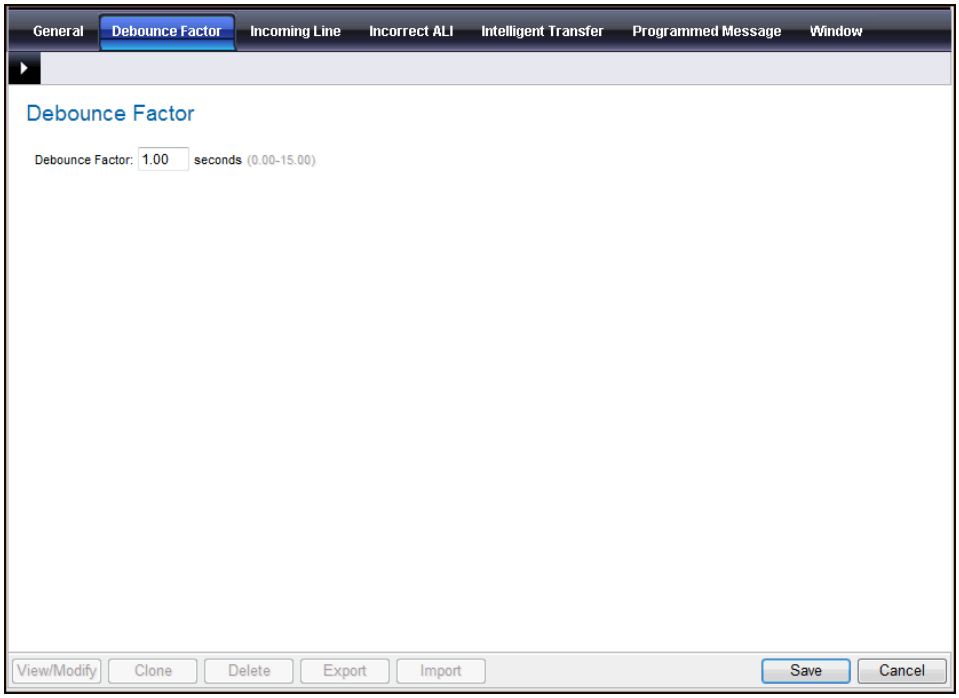


Figure 12-2 Call Control Form – Debounce Factor Tab

2. In the Debounce Factor field, enter the amount of time used to prevent the user from performing the same or another phone function that requires a noticeable amount of time to process.

3. Click **Save**.

Configuring Incoming Line Types and Lines

As a part of Call Control configuration, you must configure the Line types and Lines. Line types are defined at the system level and lines are defined at the agency level.

Provisioning settings for Line Types and Lines are on two tabs:

- Line Type – Where you configure the type of lines, defined by a name and description.
- Line – Where you configure the actual lines for the agency, assigning a display name, description, and type of line.

Configuring Incoming Line Types

Line Types are provisioned at the system level. Intercom and Ringdown are required line types and cannot be deleted. You can add additional line types to describe ACD queues and types of lines managed by your PSAP's phone systems. Any lines that will be managed by the Call Control module within PremierOne need to have a line type associated.

Line types that you add are available for selection when provisioning different lines on the Line tab and the Intelligent Transfer – Service Provider tabs.

To configure incoming line types:

From the navigation panel, select **Call Control**, and then select **Incoming Lines**.

The Line Type tab appears. Fields display for incoming line information.

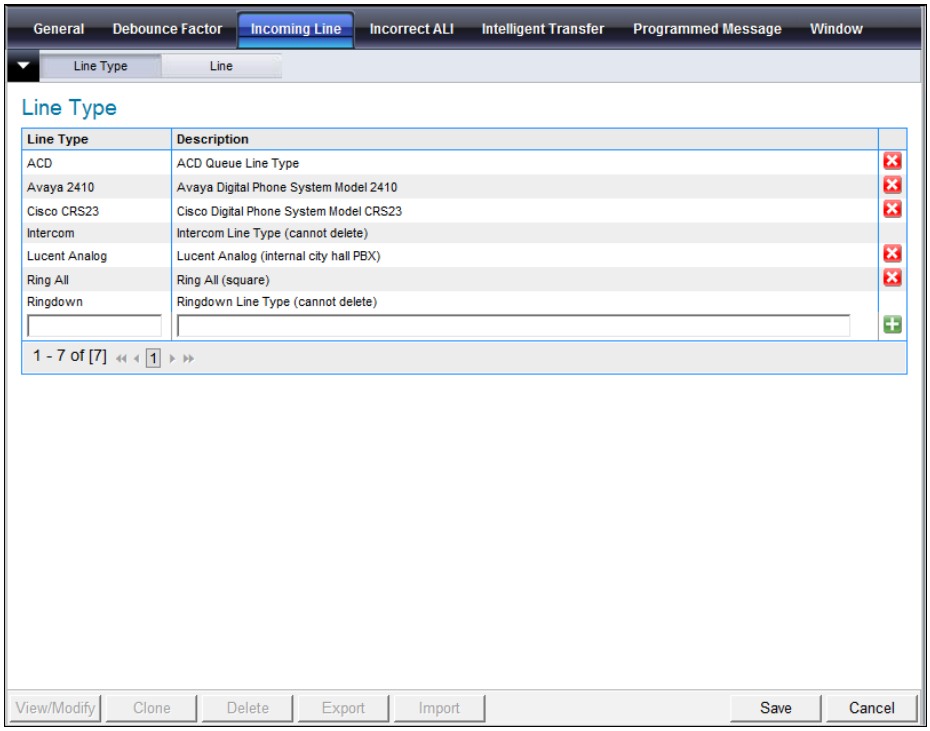


Figure 12-3 Call Control Form – Incoming Line Tab

Configuring Incoming Lines

Lines are provisioned by each agency and must be unique within an agency; they are not required to be unique across agencies. Lines in PremierOne must match the lines that are configured in the telephony system. There is no check ensure that line IDs match between the two systems.

NOTE
You can import lines from the telephony system.

To configure incoming lines:

1. Access the Incoming Line form.
2. For details, see "Configuring Incoming Line Types" on page 12-5.

   The Incoming Line Type tab appears.
3. Click the Line tab.

   Line fields display.

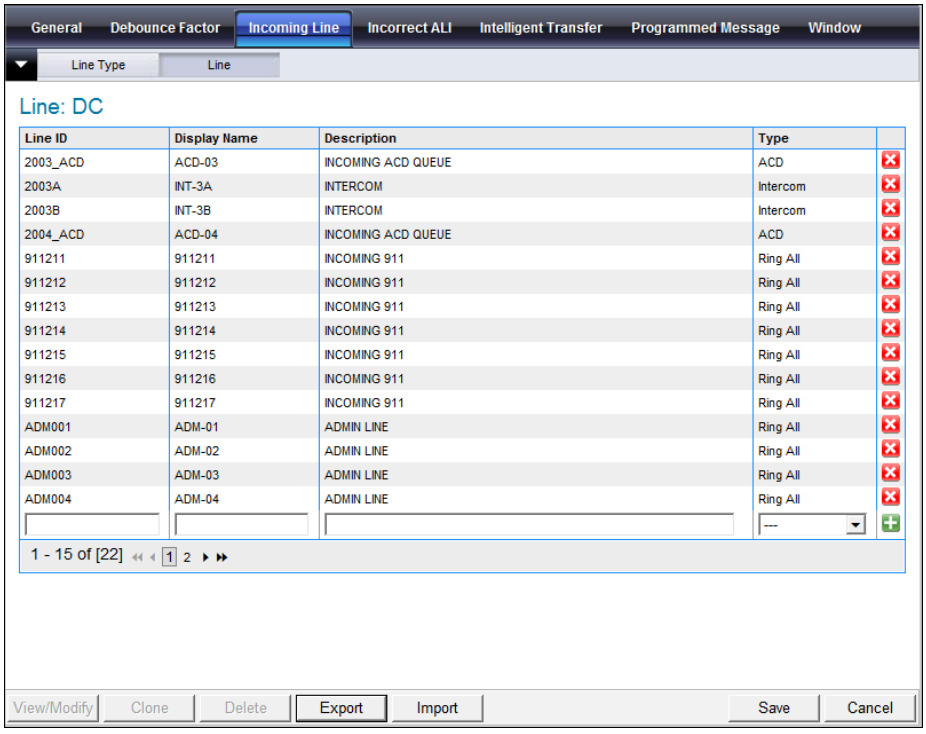


Figure 12-4 Call Control Form – Line Type Tab

4. In the Line ID field, type the line ID.

   The line ID is configured in the telephony system.

5. In the Display Name field, type the name to display in the Call Control window on the Queue buttons.

6. In the Description field, type a description to identify the line.

7. From the Type field, select the line type elect the appropriate line type that describes the line types being managed by your PSAP's phone system.

   The type is not a required field, but the line will not function without a line type. This allows you to import lines from the telephony system and then assign the line type after the import.

8. Click **Save**.

Managing Incorrect ALI Records

The Incorrect ALI tab contains all the ALI records that have been flagged as incorrect on the CAD client for the specified agency. Incorrect ALI records are intended to be printed in a report that can be given to your ALI provider(s) for correction. When corrected by your ALI provider, incorrect ALI records are deleted so they no longer show as incorrect ALI records in the Call Control module.

You can view records, delete records, and run and print a report of the incorrect records.

To manage incorrect ALI records:

1. From the navigation panel, select **Call Control**, and then select **Incorrect ALI**.

The Incorrect ALI tab appears. A list of incorrect ALI entries display with the address, city, phone number, and customer name for each record. If the incorrect ALI record was included in a previously printed report, the date and time that report was printed also displays.

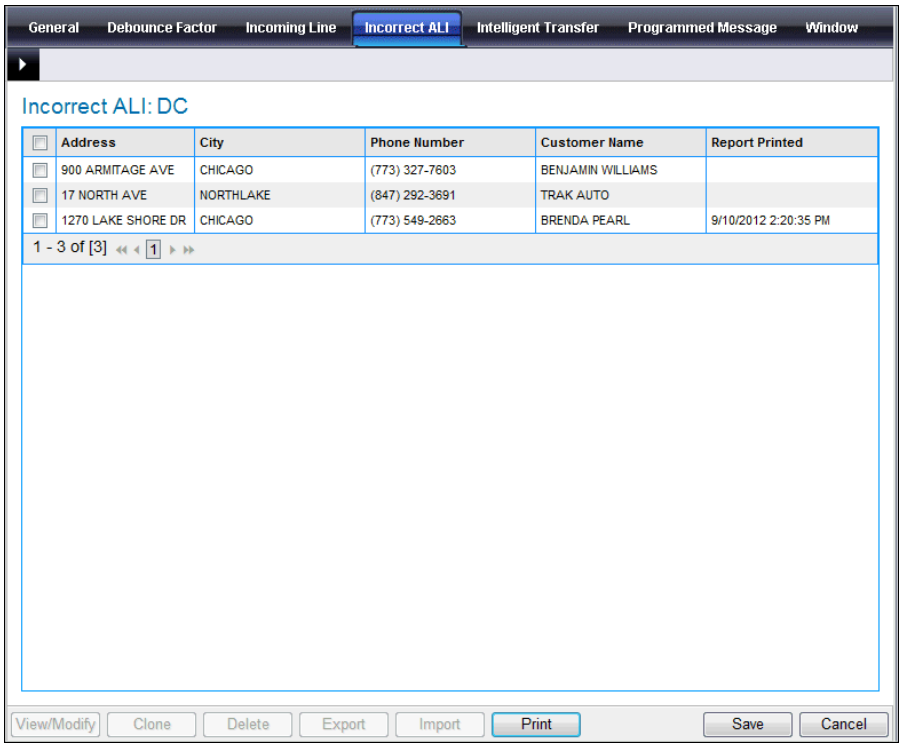


Figure 12-5 Call Control Form – Incorrect ALI Tab

2. Do any of the following:

   - To delete a record, select the record and click **Delete**. You can delete multiple records at a time.

     The delete action also removes the incorrect ALI flag for the record in the CAD client.

   - To print a list of records, select the records you want to print and click **Print**.

     The Print Incorrect ALI Report appears.

?

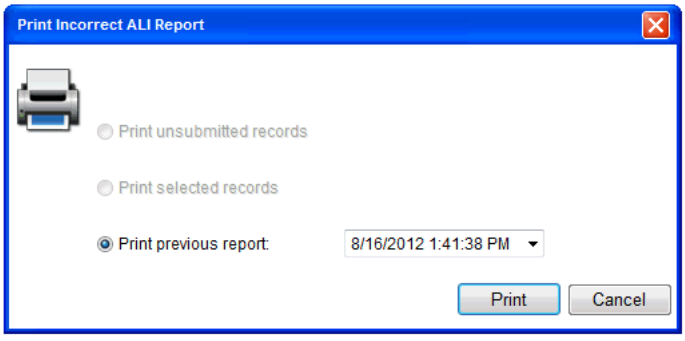


Figure 12-6 Print Incorrect ALI Report Dialog Box

3. Select one of the following:

   - To print records that have not been previously printed, select **Print unsubmitted records**.
   - To print selected records, select the records you want to print and click **Print**.
   - To print a previous report, select **Print previous report** and then select the report you want to print from the adjacent list.

4. Click **Print**.

Configuring Intelligent Transfer Settings

You can provision service providers for transferring voice calls to. Typical service provider types might be police, fire, medical, FAA, HazMat, or foreign languages. You can provision multiple providers for a provider type, and you can also provision the service providers that are recommended for different schedules.

Service providers Queue buttons display in the Transfer area of the Call Control window. The order you provision the service providers controls the order in which the transfer buttons display in the Transfer area, but these can be changed. There is a one-to-one correspondence between service provider types and service provider transfer buttons.

Provisioning settings for intelligent transfer are on four tabs:

- Provider Types – Where you enter the name, description, display name, and default service provider for the provider type.
- Service Providers – Where you provision what service providers will exist within each service provider type.
- ESN Recommendation – Where you provision the service provider and schedules for ESN recommendations.
- Line Recommendation – Where you provision the service provider and schedules for recommendations by specific incoming lines.

Configuring Intelligent Transfer Service Provider Types

Properties for service provider types include name, description, display name, and the default Response Service Provider.

To configure Service Provider types:

1. From the navigation panel, select **Call Control**, and then select **Intelligent Transfer**.

   The Service Provider tab appears. A list of existing service providers displays on the left side of the window.

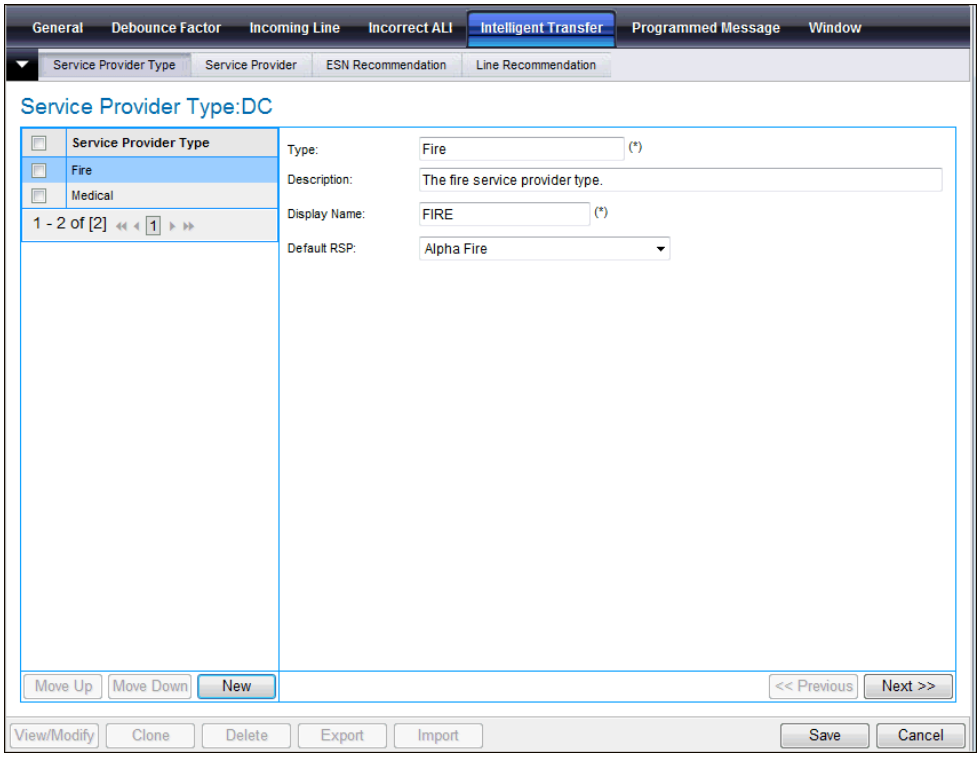


Figure 12-7 Call Control Form – Intelligence Tab, Service Provider Subtab

2. At the bottom of the Window list, click the **New** button.
3. In the Type field, enter the type of service provider.
4. In the Description field, type a description for the service provider.
5. In the Display Name field, type the name to use to display on the Service button.
6. From the Default RSP list, select the default response service provider.

   The default response service provider is the provider used if the system cannot determine the provider to use based on the ESN or line number. The service providers that display in the list are derived from the service providers you configure on the Service Provider tab.

7. Click **Save**.

Configuring Intelligent Transfer Service Providers

Any Ready Reference record can be provisioned as a service provider; for details on creating ready reference records, see “Adding Address Books” on page 18-2. You can add service providers for your agency using Ready Reference records from your own or other agencies. Properties for service providers include the description, service provider type, default phone, display name, and schedules.

Each service provider must have a default phone number. Phone numbers can be scheduled per recommendation type (either ESN or Line) and the line type to use when the service provider is recommended.

You use the default phone number to make an outgoing call when clicking the single-click transfer button when the calltaker is not on a call.The default phone is used when there is no scheduled phone number for a particular time and day. You can schedule multiple default phone numbers per recommendation type (ESN or line) as long as their schedules do not overlap. Similarly, multiple phone numbers can be provisioned per schedule block as long as each phone number has a unique line type.

To configure an intelligent transfer Service Provider:

1. Access the Call Control form.

   For instructions, see “Configuring Intelligent Transfer Service Provider Types” on page 12-9.

   The Intelligent Design form appears with the Service Provider Types tab in focus.

2. Select the Service Provider tab.

The General tab appears.

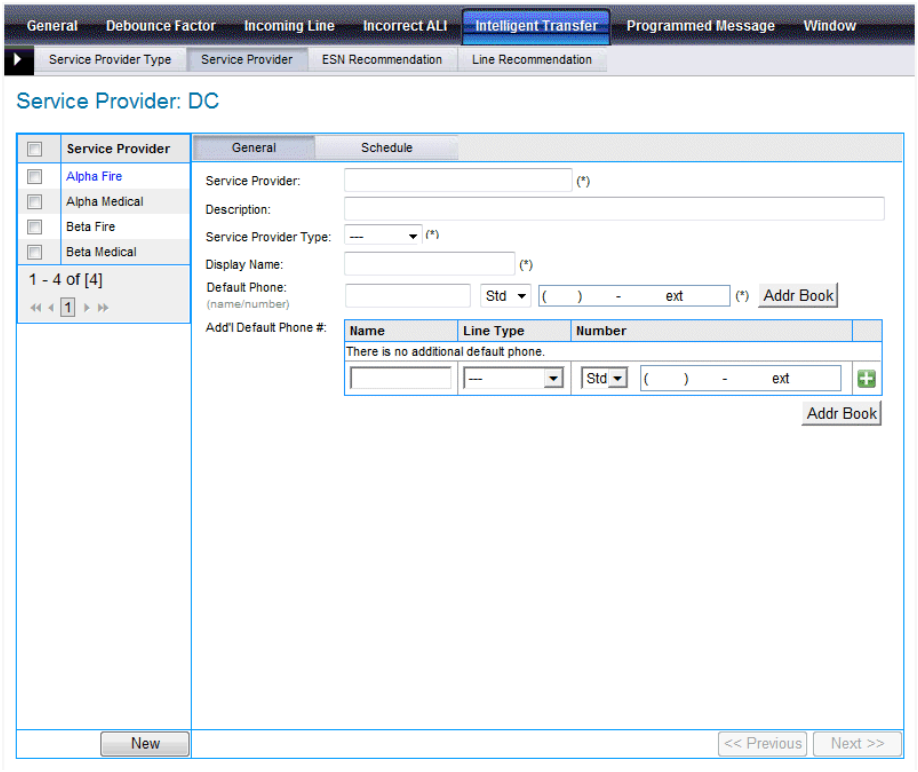


Figure 12-8 Call Control Form – Intelligence Tab, Service Provider – General Subtab

3. In the Service Provider field, enter the name of the service provider.
4. In the Description field, enter a description of the service provider.
5. From the Service Provider Type list, select the type of service provider.

   Service provider types are defined on the Service Provider Type tab.
6. In the Display Name field, select the name to display for the service provider.

   This name is displays when the call taker right-clicks the service provider transfer button.
7. To search for default phone number to use, continue with the following substeps. To enter the default phone number manually, skip to the next step.

   If no other number is provisioned for the circumstance of a recommendation, then the default phone number is the one to be used. The default phone number does not have a line type for this reason.

   a. Click the **Addr Book** button.

The Find Service Provider dialog box appears.

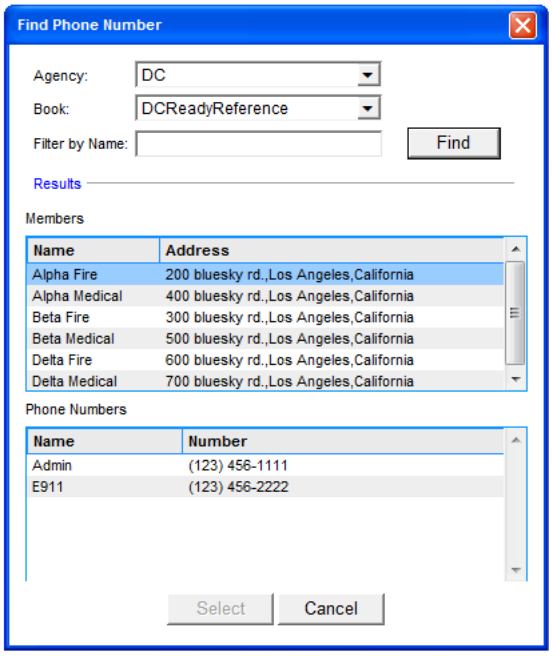


Figure 12-9 Find Service Provider Dialog Box

b. Select the Agency and Ready Reference address book containing the service provider.

Providers that display are configured in Ready Reference books. For details on ready reference books, see “Adding Address Books” on page 18-2.

c. Select the phone number and click **Select**.

8. To manually enter the phone information do the following

a. In the first Default Phone # field, enter the name to use for the phone number, such as front desk.

The default phone number is used when a phone number is not scheduled for a particular time and day.

b. In the second Default Phone # field, select the type of phone number. These include the following:

- STD – Standard 7-, 10- or 11-digit numbers.

  By leading the entry with a + symbol, you can type any characters/phone number length regardless of the phone number template used by your system.

- SC – Star Code number. Star codes are pre-programmed in the selective router to allow PSAPs to transfer E9-1-1 calls to predetermined PSAPs while keeping the complete original ANI/ALI data retrieved with the original 9-1-1 call.

- HF – Hook flash number. Hook flash simulates quickly hanging up and then picking up again. How this works depends on the agency configuration.
- RD – Ringdown line.

c. In the third Default Phone # field, enter the phone number.

d. Click the plus symbol at the end of the row to save the information.

CAUTION
If you do not click the plus symbol, PremierOne does not save the entry, even after you click Save.

9. Repeat for any other line types that you are using.

NOTE
You cannot add multiple phone numbers with the same line type.

10. To set up a schedule for the phone numbers, click the Schedule tab.

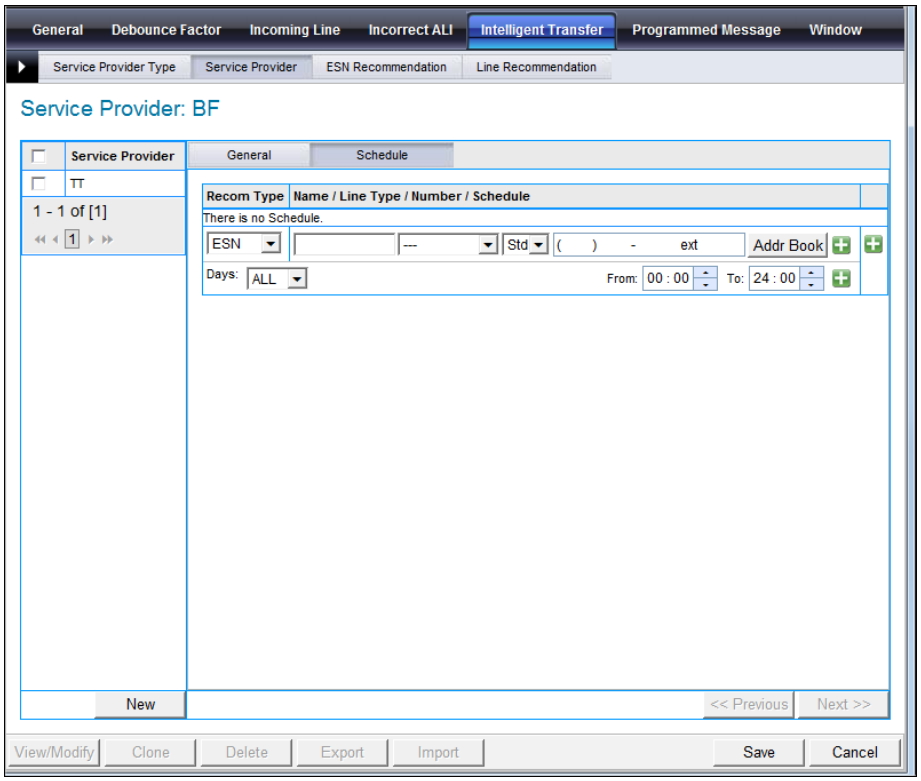


Figure 12-10 Call Control Form – Intelligence Tab, Service Provider – Schedule Subtab

11. Do the following:

a. From the Recomm Type field, select the recommendation type: ESN or line.

b. In the second field, enter a name for the line, such as Admin, Default ACD, or Default Ring Group.

c. In the third field, select the type of line: Intercom, Ringdown, ACD, Ringroup, and other agency-defined line types.

d. In the fourth field, select the type of phone number:

- STD – Standard 7-, 10- or 11-digit numbers.

  By leading the entry with a + symbol, you can type any characters/phone number length regardless of the phone number template used by your system.

- SC – Star Code number. Star codes are pre-programmed in the selective router to allow PSAPs to transfer E9-1-1 calls to predetermined PSAPs while keeping the complete original ANI/ALI data retrieved with the original 9-1-1 call.

- HF – Hook flash number. Hook flash simulates quickly hanging up and then picking up again. How this works depends on the agency configuration.

- RD – Ringdown line.

e. In the fifth field, either manually enter the phone number or click the **Addr Book** button to search for and select the phone number.

f. Click the plus symbol at the end of the row to save the information.

CAUTION
If you do not click the plus symbol, PremierOne does not save the entry, even after you click Save.

g. Select the days and times for the schedule.

h. Click the plus symbol at the end of the row to save the information.

CAUTION
If you do not click the plus symbol, PremierOne does not save the entry, even after you click Save.

i. Repeat for any other lines.

NOTE
You cannot add multiple phone numbers with the same line type.

12. Click **Save**.

Configuring Intelligent Transfer ESN Recommendations

As part of service provider provisioning, phone numbers can be scheduled per type of recommendation type (either ESN or Line ID). Multiple phone numbers can be provisioned, per recommendation type, as long as their schedules do not overlap.

To configure an intelligent transfer ESN recommendation:

1. Access the Call Control form.

   For instructions, see "Configuring Intelligent Transfer Service Provider Types" on page 12-9.

   The Intelligent Design form appears with the Service Provider Types tab in focus.

2. Click the ESN Recommendation tab.

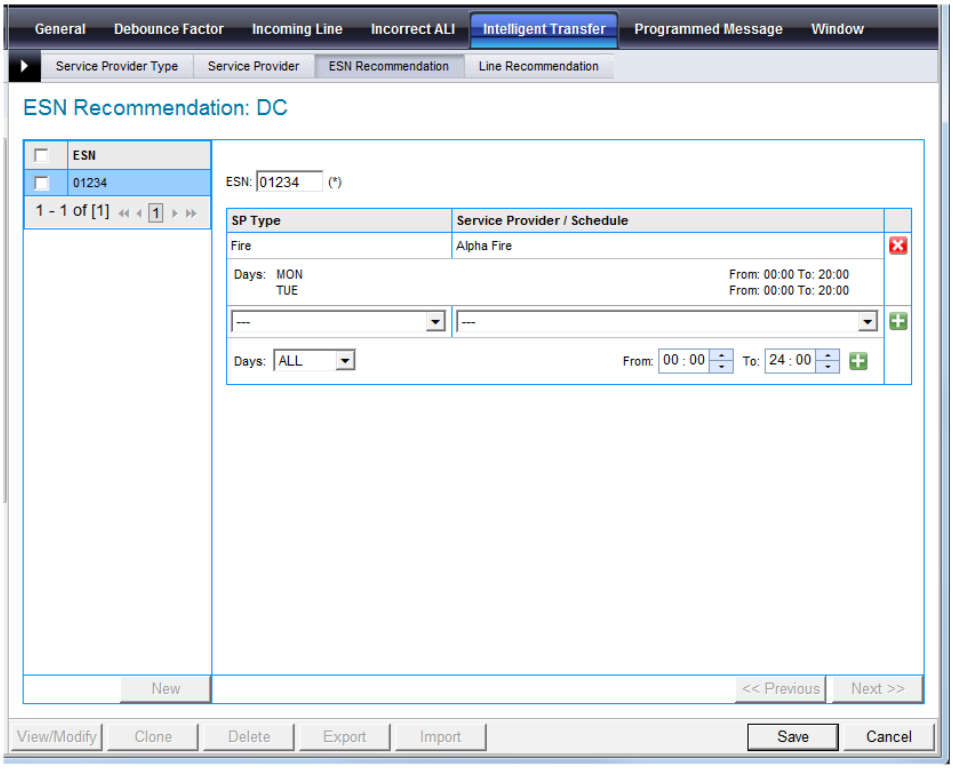


Figure 12-11 Call Control Form – Intelligence Tab, ESN Recommendation Subtab

3. Click **New**.

4. In the ESN field, enter the ESN number.

5. In the Schedule section, enter the Service Provider type and schedule.

   For instructions on configuring schedules, see "Configuring Intelligent Transfer Service Providers" on page 12-11.

6. Click **Save**.

Configuring Intelligent Transfer Line Recommendations

As part of service provider provisioning, phone numbers can be scheduled per type of recommendation type (either ESN or Line ID). Multiple lines can be provisioned per recommendation type, as long as their schedules does not overlap.

To configure an intelligent transfer Line recommendation:

1. Access the Call Control form.

   For instructions, see "Configuring Intelligent Transfer Service Provider Types" on page 12-9.

   The Intelligent Design form appears with the Service Provider Types tab in focus.

2. Click the Line Recommendation tab.

   A list of provisioned lines displays on the left side of the window.

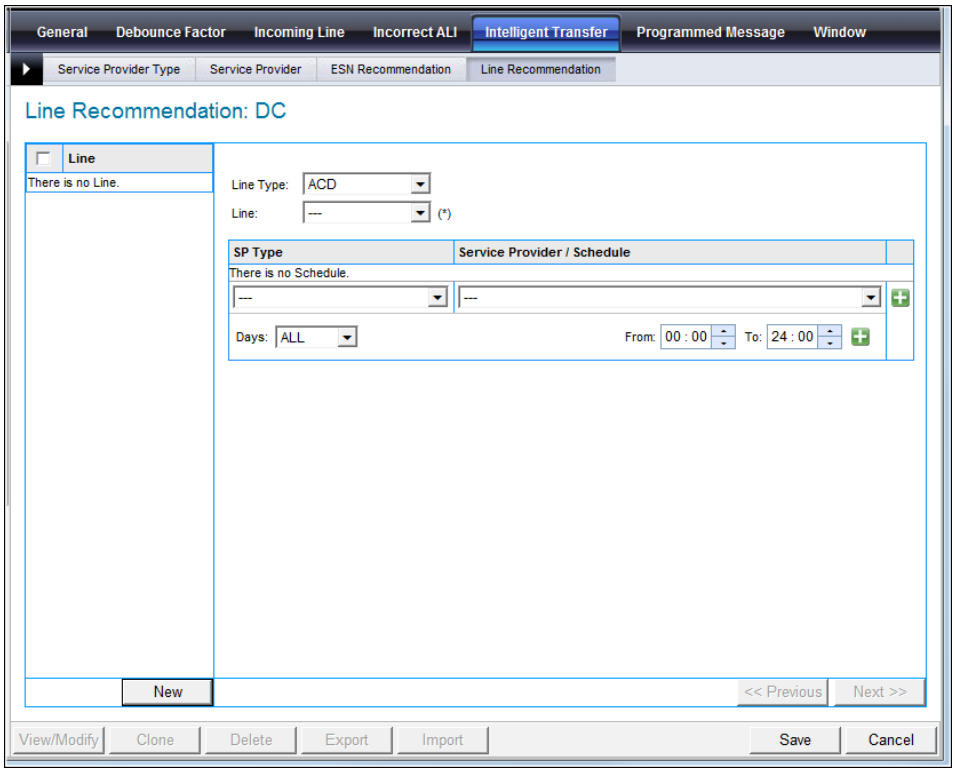


Figure 12-12 Call Control Form – Intelligence Tab, Line Recommendation Subtab

3. Click **New**.

4. From the Line Type field, select the line type.

   Line types are provisioned on the Incoming Line – Line type tab. For details, see "Configuring Incoming Line Types" on page 12-5.

5. From the Line field, select the line.

Lines are provisioned on the Incoming Line – Line tab. For details, see “Configuring Incoming Lines” on page 12-6.

6. In the Schedule section, select the Service Provider type and Service Provider.
7. Enter the schedule.

   For instructions on configuring schedules, see “Configuring Intelligent Transfer Service Providers” on page 12-11.

8. Click **Save**.

Understanding the Recommended Service Provider Display

The response service providers that display on the transfer buttons correspond to the call currently displaying on the Status bar in the Telephony area, regardless of the status of the call. The combination of call characteristics (ESN value and line ID) and the provisioning of Intelligent Transfer determine what is displayed on the service provider transfer button for each service provider type.

The following two scenarios define the behavior of an individual service provider transfer buttons for all possible provisioning conditions:

Call contains an ESN:

- ESN is provisioned *and* an service provider is scheduled for the ESN with a scheduled ESN phone number: Display the service provider’s scheduled ESN phone number
- ESN is provisioned *and* an service provider is scheduled for the ESN but no ESN phone number is scheduled: Display the service provider’s default phone number
- ESN is provisioned *but* no service provider is scheduled for the ESN: Use the default response service provider for the service provider type (if provisioned) and do one of the following
  - Display the service provider’s scheduled ESN phone number (if provisioned)
  - Display the service provider’s default phone number
  - Disable transfer button on client
- ESN is not provisioned: Use the default response service provider for the service provider type (if provisioned) and do one of the following:
  - Display the service provider’s scheduled ESN phone number (if provisioned)
  - Display the service provider’s default phone number
  - Disable transfer button on client

Call does not contain an ESN:

- Line ID is provisioned *and* an service provider is scheduled for the Line ID with a scheduled Line ID phone number: Display the service provider's scheduled Line ID phone number
- Line ID is provisioned *and* an service provider is scheduled for the Line ID but no Line ID phone number is scheduled: Display the service provider's default phone number
- Line ID is provisioned *but* no service provider is scheduled for that Line ID: Use the default response service provider for that service provider type (if provisioned), and do one of the following:
  - Display the service provider's scheduled Line ID phone number (if provisioned)
  - Display the service provider's default phone number
  - Disable transfer button on client
- Line ID is not provisioned: Use the response service provider for the service provider type (if provisioned), and do one of the following:
  - Display the service provider's scheduled Line ID phone number (if provisioned)
  - Display the service provider's default phone number
  - Disable transfer button on client

Configuring Preprogrammed Messages

You can configure preprogrammed SMS and TDD messages. This is useful for messages that are most commonly used. The call taker types the first few words of the sentence and the preprogrammed message autopopulates the field. You associate a tag with each message so the call taker can just type the tag and the entire message displays.

NOTE
Preprogrammed messages can be configured at the agency type or the agency level.

To configure preprogrammed messages:

1. From the navigation panel, select **Call Control**, and then select **Programmed Message**.

   The Preprogrammed Message tab appears. A list of existing messages and tags display.

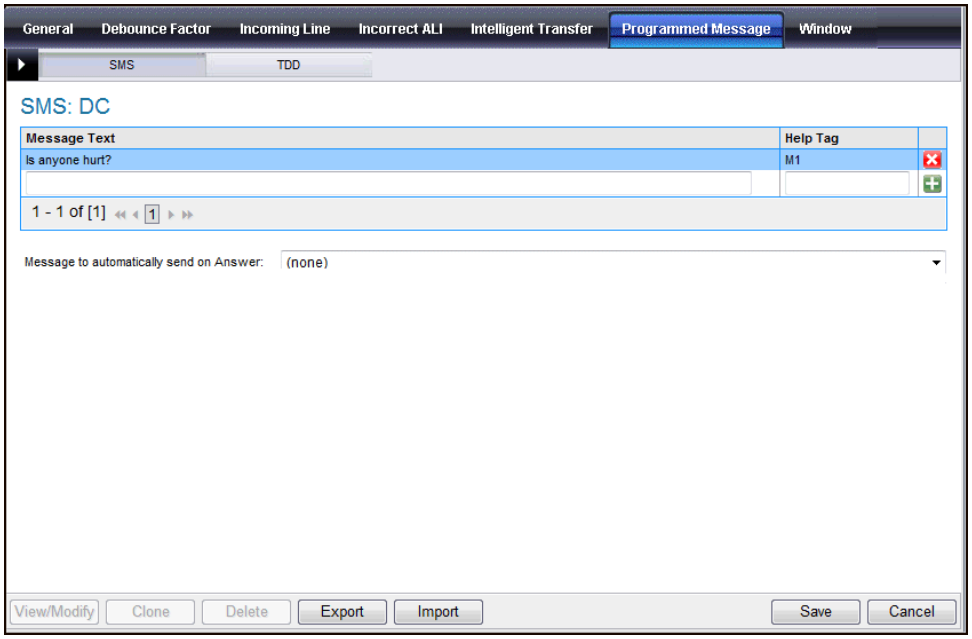


Figure 12-13 Call Control Form – Preprogrammed Messages Tab, SMS Subtab

2. In the Message Text field, type the SMS message, such as `Is Anyone hurt?`

3. In the Help tag field, type the tag to use for the message (optional).

   When the call taker enters the tag, the entire message displays.

4. Click the plus symbol at the end of the row to save the information and add another message row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the message, even after you click Save.

5. Below the list of help tags, select the messages you want to automatically send on Answer or on Release.

   These lists are populated with the Message text that you enter at the top of the form.

6. Click the TDD tab.

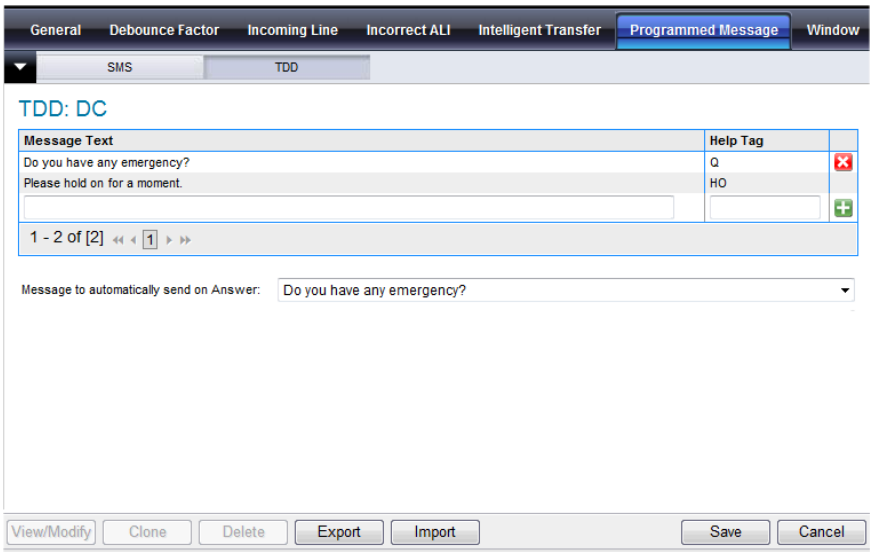


Figure 12-14 Call Control Form – Preprogrammed Messages Tab, TDD Subtab

7. In the Message Text field, type the TDD message such as `Are you hurt? GA`
8. In the Help tag field, type the tag to use.

   When the call taker enters the tag, the entire message displays.
9. Click the plus symbol at the end of the row to save the information and add another row.
10. Below the list of help tags, select the messages you want to automatically send on Answer.

    This list is populated with the Message text that you enter at the top of the form.

CAUTION
If you do not click the plus symbol, PremierOne does not save the alternative routing information, even after you click Save.

Configuring the Call Control Window

You can configure several settings for the Call Control window:

- General – Where you enter a name, select how phones are rung, select whether SMS conversations and abandoned calls are presented to the workstation, set whether the window can be moved, resized, or minimized, and set whether panels can be orphaned.
- Queue Button – Where you set the label, line type, and selected lines for the respective Queue buttons.
- Permissions – Where you set the roles and workstations that have permissions to access the window.

NOTE
Call Control Window settings can be exported and imported.

Configuring General Settings for the Call Control Center Window

General settings for Call Control windows include a name, how phones are rung, whether SMS is used, whether Abandoned Call Notifications are presented to the workstation, whether the window can be moved, resized, or minimized, and whether panels can be orphaned.

To configure General settings for the Call Control Center window:

1. From the navigation panel, select **Call Control**, and then select **Window**.

The Window tab appears. A list of existing windows displays on the left side of the window.

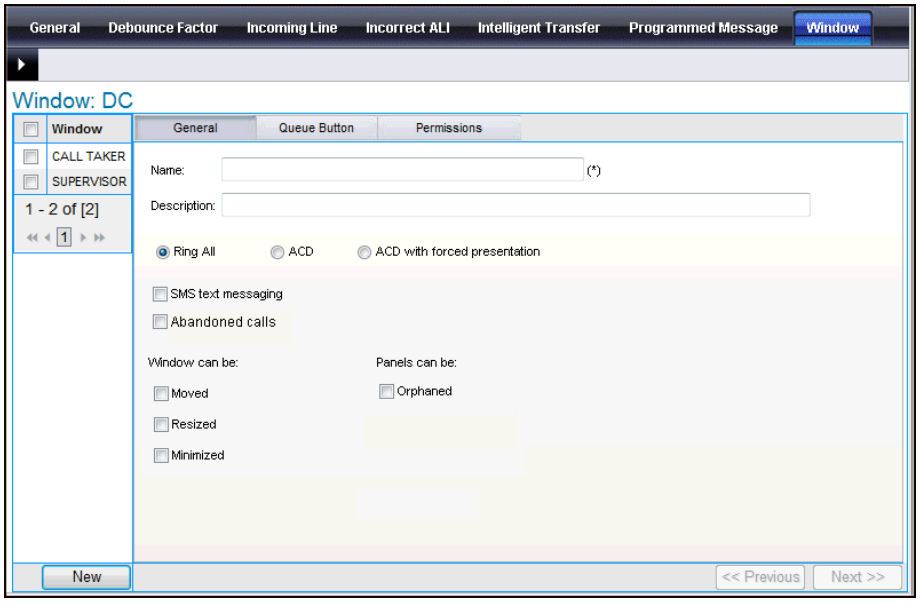


Figure 12-15 Call Control Form – Window Tab, General Subtab

2. At the bottom of the Window list, click the **New** button.
3. In the Name field, type a name for the new window.
4. In the Description field, type a description for the new window.
5. Select one of the following:
   - If your PSAP uses a Ring All, Square, or UCD, select **Ring All.**
   - If your PSAP uses ACD (Automatic Call Distribution) to present calls, select ACD.

     For this option, only the calls that are directed to the workstation display.
   - If your PSAP uses ACD (Automatic Call Distribution) with forced presentation where your call takers are presented calls without the need to manually answer the call, select **ACD with forced presentation**.
6. To display SMS conversations, select **SMS**.
7. To display abandoned calls, select **Abandoned calls**.
8. In the Window can be section, select any of the following (applies to Call Telephony and ALI panels):
   - To allow the window to be moved, select **Moved**.
   - To allow the window to be resized, select **Resized**.

- To allow the window to be minimized, select **Minimized**.

9. In the Panels can be section, select **Orphaned** to allow panels to be orphaned (applies to Call Telephony and ALI panels).

10. Click **Save**.

Configuring Queue Buttons for the Call Control Center Window

The Queue buttons display in the lower-left corner of the Call Control Center window and are used to access incoming calls. You can set the button label, line type, and selected lines for the Queue buttons.

To configure queue buttons for the Call Control Center window:

1. Access the **Call Control**, and then select **Window**.

   The Window tab appears. A list of existing window types displays on the left side of the window.

2. On the left side of the window, select the window you want to configure.

3. Click the Queue Buttons tab.

   The Queue Button tab appears. Fields for defining Queue buttons display.

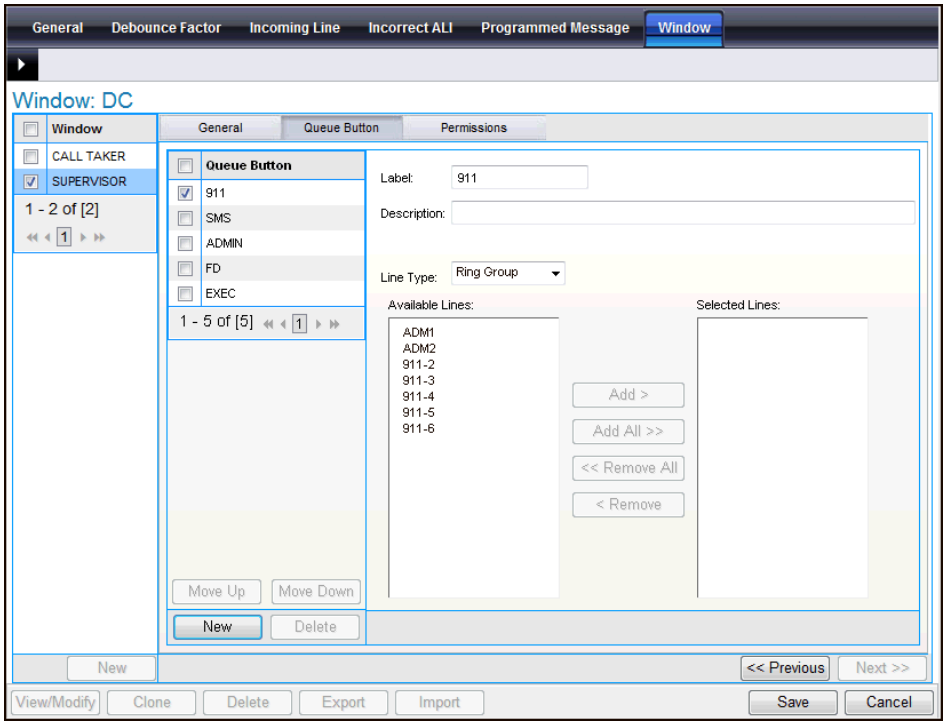


Figure 12-16 Call Control Form – Window Tab, Queue Button Subtab

4. At the bottom of the Queue Button list, select **New**.
5. In the Description field, type a description for the queue button.
6. From the Line Type list, select the type of line you want to configure.
7. From the Available Lines box, select the lines you want to add and click the **Add** button to add them to the Select Lines box.

   After a line is added to a queue button, the line is not be available to any other queue buttons.
8. Click **Save**.

Configuring Permissions for the Call Control Window

You can set permissions to access the Call Control window by role and by workstation. If there is a conflict between the permissions a role has and a workstation has, the role permission takes precedence.

To configure permissions for the Call Control window:

1. From the navigation panel, select **Call Control**, and then select **Window**.

   The Window tab appears. A list of existing window types displays on the left side of the window.
2. Click the Permissions tab.

Two sections appear for setting permissions.

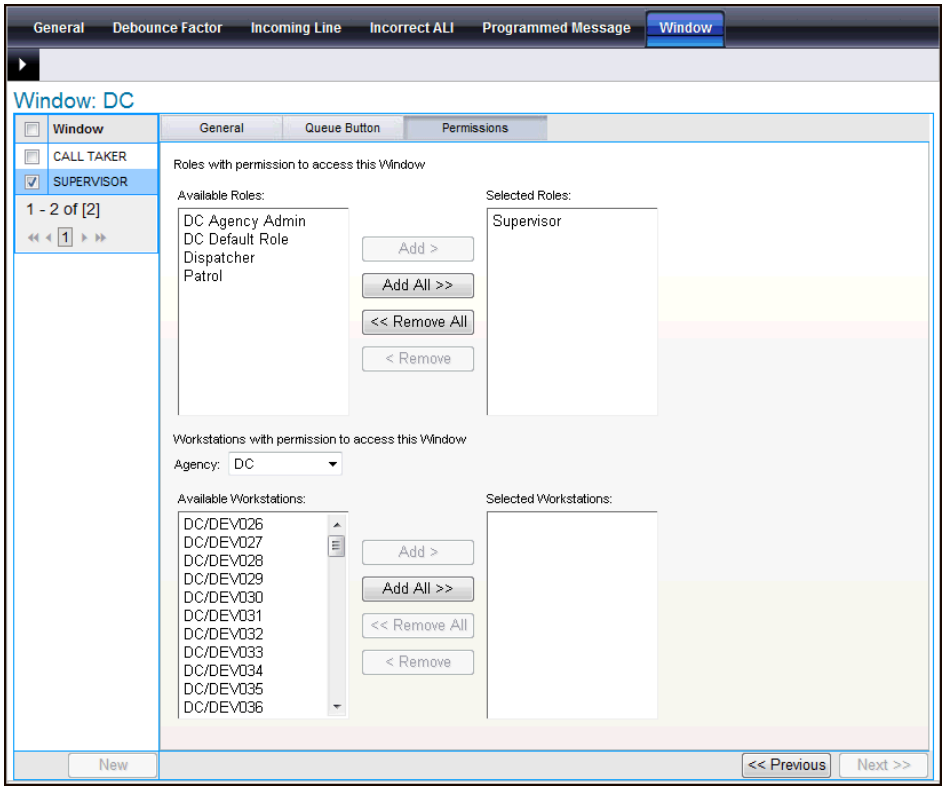


Figure 12-17 Call Control Form – Window Tab, Permission Subtab

3. From the Available Roles list, select the roles that you want to have access to the window and click **Add**.

4. In the Workstations section, select the agency for which you want to set workstation access.

5. From the Available Workstations list, select the workstations that you want to have access to view the window and click **Add**.

   A role or workstation can only be assigned to a single Call Control window configuration within each agency. Once used, it is removed from the list of Available items in future Call Control Window provisioning.

6. Click **Save**.

CHAPTER 13

Configuring Incident Management

The Incident Management configuration item contains the following items. Most incident items are set at the agency level. Incident type, modifying circumstances, and source codes are set at the agency-type level (such as fire, medical, and law). Incident response factors are also set at the agency-type level but can be modified at the agency level.

- Coverage Groups – Where you configure groups of areas in one or more agencies used for login purposes. For details, see “Configuring Coverage Groups” on page 13-2.
- Incident Type – Where you configure codes and aliases used to identify the type of incident. For details, see “Configuring Incident Type Codes” on page 13-4.
- Modifying Circumstance – Where you configure codes used under certain conditions to override the priority, subpriority, and response settings of an existing incident type. For details, see “Configuring Modifying Circumstance Codes” on page 13-8.
- Service Settings – Where you configure general incident initiation settings, such as initiation defaults, duplicate incident checks, dispositions, search defaults, incident priority definitions, and incident and report number formats, incident timeouts, and priority update notifications. For details, see “Configuring Service Settings” on page 13-10.
- Mobile/Handheld Settings – Where you set audio alerts and visual alerts notifying mobile users when new incidents are sent to the mobile or handheld units. For details, see “Configuring Mobile/Handheld Incident Settings” on page 13-32.
- Incident Response Factors – Where you configure factors that control the response to an incident, including the incident type, modifying circumstance, alarm levels, incident priority, response ID, associated incidents, and notification messages. For details, see “Configuring Incident Response Factors” on page 13-37.
- Dispositions – Where you configure the codes used to close incidents and clear the primary unit from the call. For details, see “Configuring Dispositions” on page 13-43.
- Response Message – Where you configure messages used to indicate circumstances regarding a specific geographic location. For details, see “Configuring Response Messages” on page 13-45.

- Incident Source Code – Where you configure the codes that identify the sources of emergency calls, such as 9-1-1 or an alarm interface. For details, see “Configuring Incident Source Codes” on page 13-50.
- Premise Hazard – Codes that define the premise hazard types and details for known individual premise and hazard records. For details, see “Configuring Premise/ Hazard Types and Records” on page 13-53 and “Configuring Premise Hazard Records” on page 13-58.

Configuring Coverage Groups

Use the Incident Management Coverage Groups item to manage groups of areas in one or more agencies for login purposes. A user can sign on to a coverage group as a quick way to sign on to all of the areas and agencies included in the group.

You can add, modify, clone, and delete coverage groups. For details on modifying, cloning, and deleting groups, see “Working With Configuration Items” on page 2-9. You cannot change the Coverage Group Name. If you want to change the name, you must delete and re-add the record.

Adding Coverage Groups

General information for a coverage group includes the coverage group name, description, and agency.

To add a coverage group:

1. From the navigation panel, select **Incident Management**, and then select **Coverage Groups**.

The Coverage Groups form appears with a list of existing Coverage Groups on left side of the form.

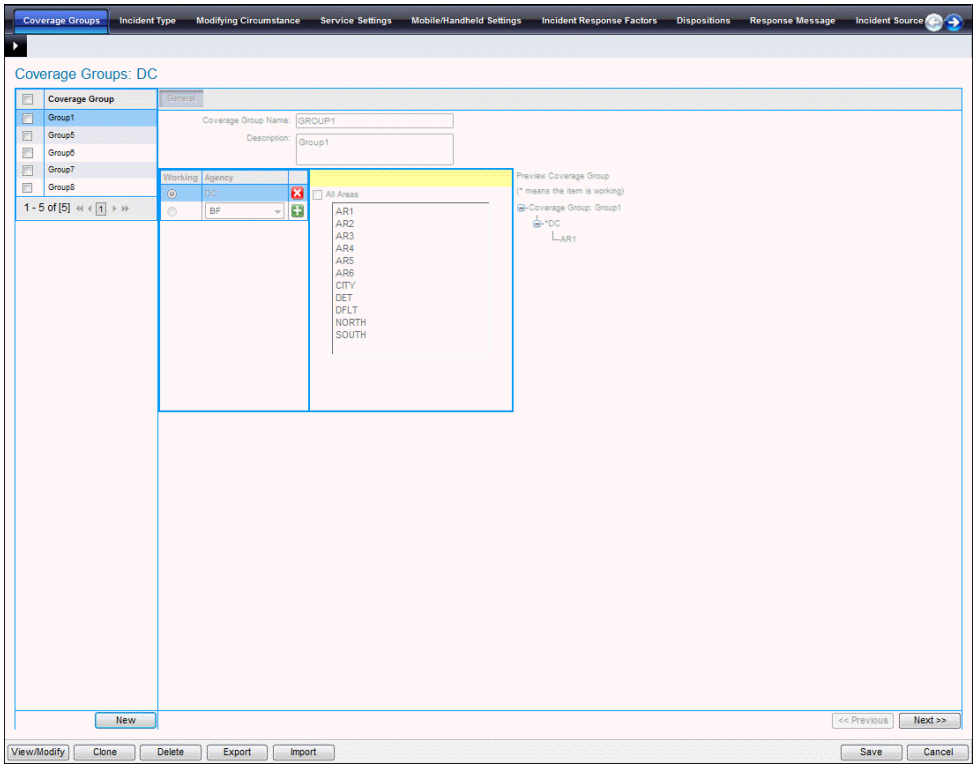


Figure 13-1 Coverage Groups Form

2. At the bottom of the Coverage Group list, click the **New** button.
3. In the Coverage Group Name field, type a name for the new coverage group.
4. In the Description field, type a description for the new coverage group.
5. From the Agency list, select an agency.

   Click the plus symbol to the right of the agency to save the agency and add another row.

CAUTION

If you do not click the plus symbol, PremierOne does not save the agency information, even after you click Save.

---

6. From the Working list, select the agency that will be the working agency for the coverage group.

   The working agency is the agency used for the commands issued by the user. The agency only needs to be included with commands if it is different than the working agency.

7. In the Areas section, select the areas to be covered by this coverage group.

To select more than one area, click your selections with the mouse.

The area to the right of the Areas section shows a preview of your coverage group as you build it.

8. Repeat the procedure to add any additional coverage groups.

   Each unsaved coverage group appears in the Coverage Group list on the left in blue text.

9. Click **Save**.

   The coverage groups you added appear in the Coverage Group list on the left in black text.

Configuring Incident Type Codes

Use the Incident Management Incident Type configuration item to set up the codes and aliases defining different incident types. Incident types are specific to each agency type, such as law, fire, or medical.

NOTE
You must associate an incident type with an IRF or the incident type will not be available in incident drop-down lists in CAD.

You can add, clone, modify, delete, and import and export incident type codes. For details on cloning, modifying, deleting, importing, and exporting codes, see "Working With Configuration Items" on page 2-9. You cannot change the incident type code name. If you want to change the code name, you must delete and re-add the record.

Adding Incident Type Codes

Incident type code details include the code ID, the name of the incident type, the description, and whether the incident type should be available to Mobile.

To add an incident type:

1. From the navigation panel, select **Incident Management**, and then select **Incident Type**.

The Incident Type Codes form for the agency type you selected appears. A list of existing incident type codes displays on the left side of the form.

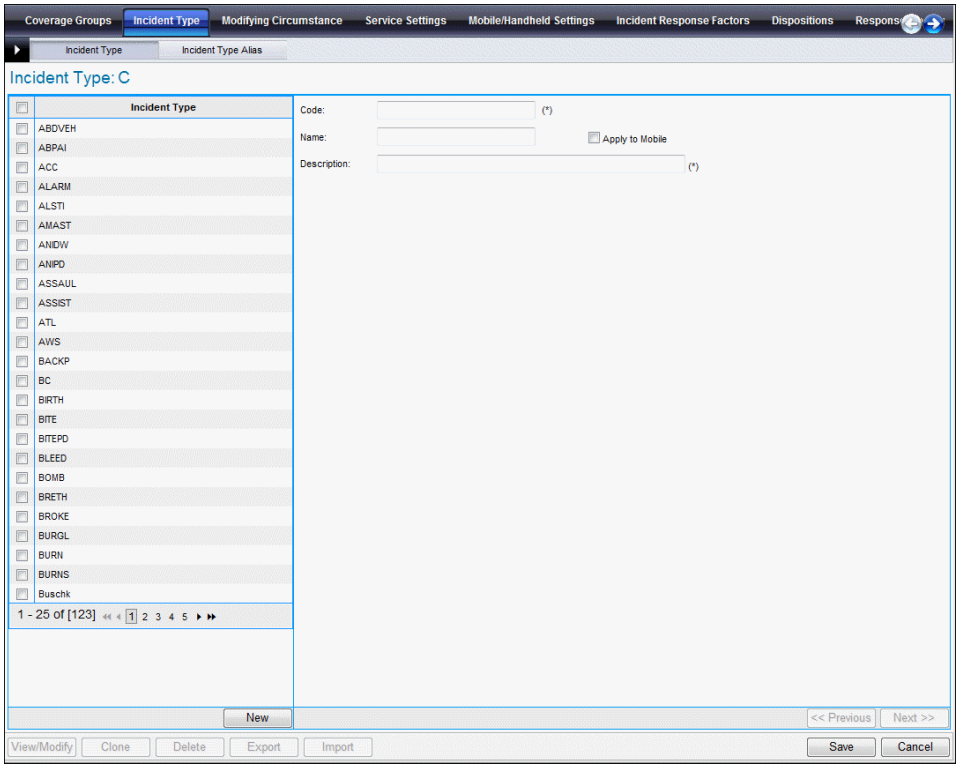


Figure 13-2 Incident Type Form

2. At the bottom of the Incident Type list, click the **New** button.
3. In the Code field, type a short code for your new incident type code.

   The asterisk (*) indicates this is a required field.
4. In the Name field, type the name of the incident type code.

   The name does not display to the user.
5. In the Description field, type a description for your new incident type code.

   The description displays to the user.
6. If you want this incident type code to apply to PremierOne Mobile, select the Apply to Mobile check box.
7. Repeat the procedure for any other incident types.

Each unsaved incident type code appears in the Incident Type list on the left in blue text.

8. Click **Save**.

   The incident type codes you added appear in the Incident Type list on the left in black text.

Adding Incident Type Aliases

You can add an alias for any incident type. An alias can help the CAD user identify the incident type. CAD users can enter the alias in place of the incident type code anywhere an incident type is used, including on the command line.

You can add, clone, modify, delete, import, and export incident type aliases. For details on cloning, modifying, deleting, importing, and exporting codes, see “Working With Configuration Items” on page 2-9.

A Provisioning setting controls whether the alias or real incident type displays in CAD forms. For details, see “Adding Agencies” on page 4-4.

To add an incident type alias:

1. Access the form for incident types. For instructions, see “Adding Incident Type Codes” on page 13-4.

   The Incident Type form for the agency type you selected appears. A list of existing incident type codes displays on the left side of the form.

2. Click the Incident Type Alias tab.

Fields for alias information display.

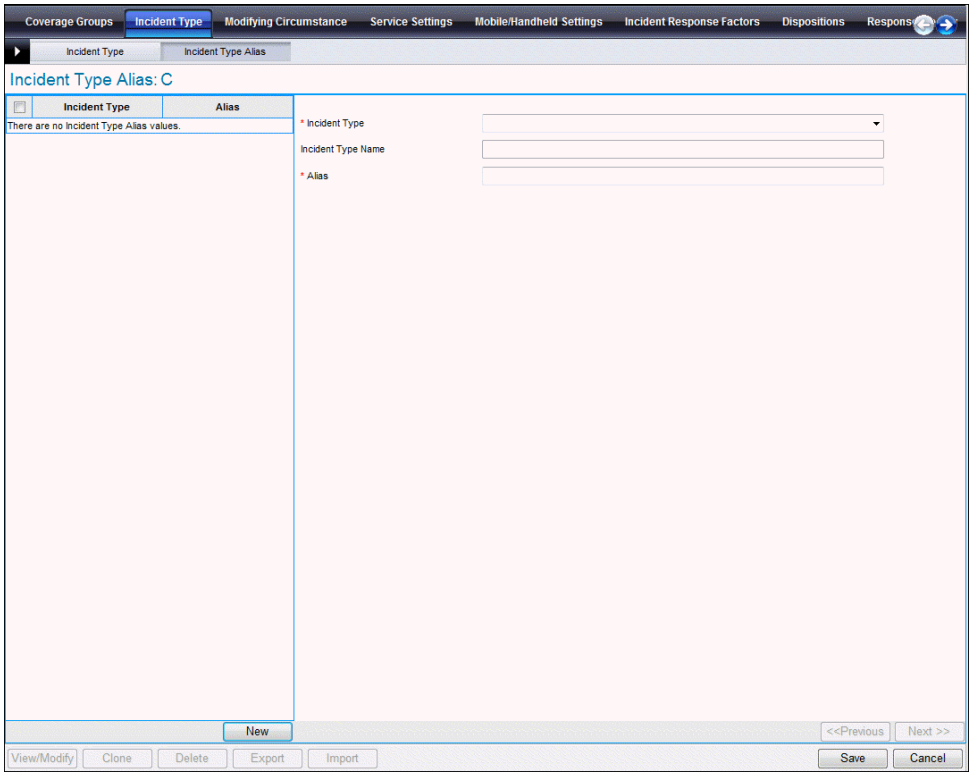


Figure 13-3 Incident Type Form – Alias Tab

3. From the Incident Type list, select the incident type for which you want to create an alias.

   The incident type name populates the Incident Type Name field.

4. In the Alias field, enter the alias for the incident type.

   NOTE
   The alias cannot be the same as the Incident Type.

   Each unsaved incident type alias appears in the Incident Type Alias list on the left in blue text.

5. Repeat the procedure for any other incident types.

   You can have multiple aliases for an incident type.

6. Click **Save**.

Configuring Modifying Circumstance Codes

Use the Incident Management Modifying Circumstance configuration item to create and manage codes that are used under certain conditions to override the priority, subpriority, and response settings of an existing incident type with the settings defined for the particular modifying circumstance.

NOTE
Modifying circumstances are defined at the agency-type level (such fire, law, EMS).

Modifying circumstances can also be viewed as subincidents. They can be used to help limit the number of incident types used by your agency. For example, you could have an incident type of fire (without injury), and then have modifying circumstances for a structure fire, trash fire, or automobile fire. When you run reports, you would then have far fewer numbers of incident types.

You can add, clone, modify, delete, import, and export modifying circumstance codes. For details on cloning, modifying, deleting, importing, and exporting codes, see "Working With Configuration Items" on page 2-9. You cannot change the modifying circumstance code name. If you want to change the code name, you must delete and re-add the record.

Adding Modifying Circumstances Codes

Modifying circumstance code details include the code ID and the description.

To add modifying circumstance codes:

1. From the navigation panel, select **Incident Management**, and then select **Modifying Circumstance**.

The Modifying Circumstance form appears.

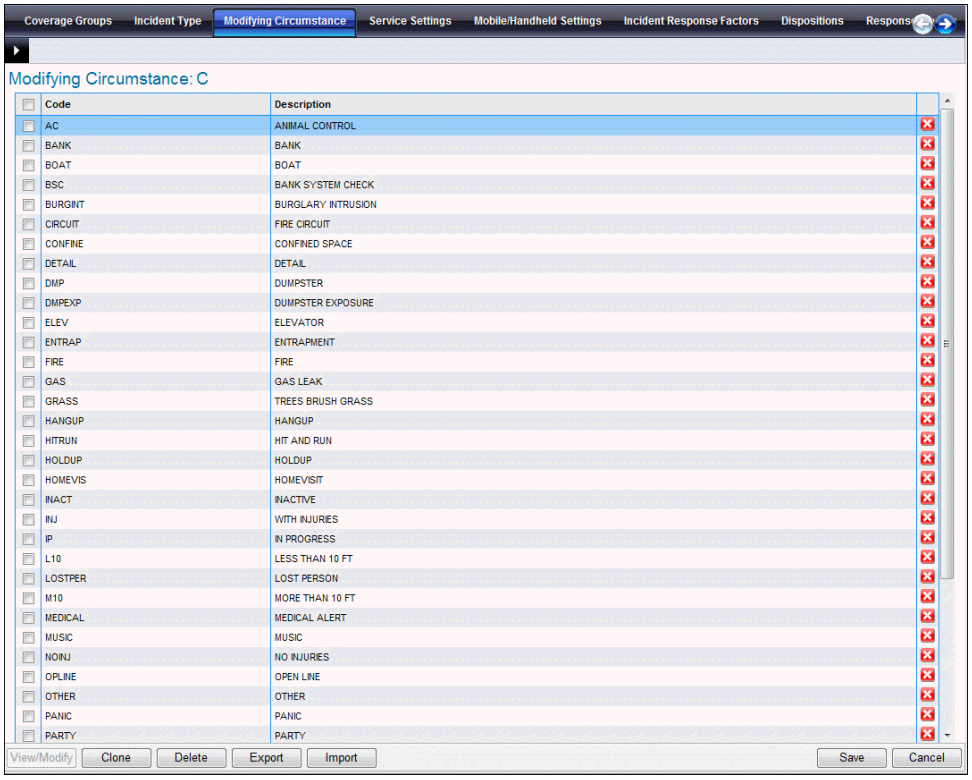


Figure 13-4 Modifying Circumstance Form

2. In the first blank field, type the code for your new modifying circumstance.
3. In the second blank field, type a description for your new modifying circumstance.
4. Click the plus symbol at the end of the row.

   PremierOne adds your new modifying circumstance code and description in blue text and another set of blank fields appears at the bottom of the list.
5. Repeat the procedure for any other modifying circumstances codes that you want to add.

   PremierOne adds your new modifying circumstance code and description in blue text and another set of blank fields appears at the bottom of the list.
6. Click **Save**.

   The modifying circumstance codes you added appear in the list in black text.

Configuring Service Settings

Use the Incident Management Service Settings configuration item to manage incident initiation defaults, search defaults, incident priority definitions, general service information such as distance and weight units, incident and report number formats, and priority update notifications.

Service Settings

When you configure service settings, you can enter information on any of the six tabs of the Incident Management – Service Settings form:

- Configuring Service Defaults– Where you modify general information, such as the initial status for incidents, whether a disposition is required to close an incident, whether open incidents are allowed, distance and weight units, incident number formats, reset interval for incident numbers, report number formats, and reset interval for report numbers.
- Configuring Initiation Defaults – Where you modify general information, such as whether to contact the complainant and what form to display after incident initiation, enable duplicate incident checks, configure traffic stops and field-initiated incidents, enable call stacking, and set the default city and state.
- Configuring Search Defaults– Where you set the search distance and default sort for incident searches, and set the parameters for previous subject/vehicle searches including subject, vehicle, and additional caller roles.
- Configuring Priorities – Where you set incident priorities, determine whether to sort incident priorities in ascending or descending order, and set sub-priorities.
- Configuring Incident Timeouts – Where you set durations that incidents can remain in a specific status before a timeout operation occurs.
- Configuring Priority Updates – Where you enable priority updates and select the fields to be monitored for updates.

Configuring Service Defaults

Configure service defaults when you need to change general information, incident number formats, reset incident numbers, reset report number formats, reset report numbers, and assign report numbers.

To configure service defaults:

1. From the navigation panel, select **Incident Management**, and then select **Service Settings**.

The Service Settings form appears with the Service Defaults tab in focus.

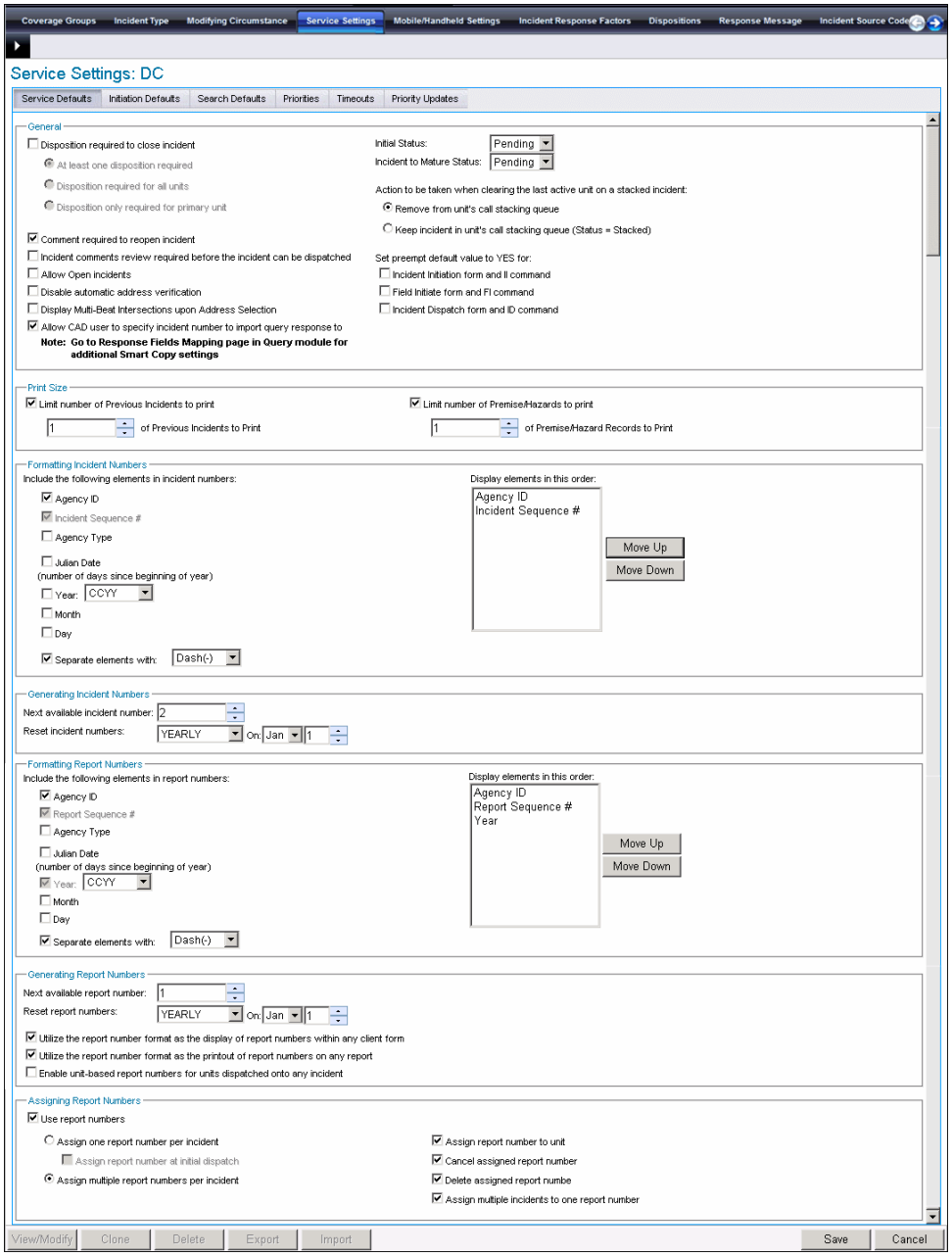


Figure 13-5 Service Settings Form – Service Defaults Tab

2. Click **View/Modify**.

3. To require a disposition to close incidents, select the **Disposition required to close incident** check box. Then select one of the following:

   - To require at least one disposition for any unit on the incident, select the **At least one disposition is required** check box. In this case, all but one of the units can be cleared without a disposition.
   - To require a disposition for all units, select the **Disposition required for all units** check box. In this case, a unit cannot be cleared without a disposition.
   - To require a disposition only for the primary unit, select the **Disposition only required for primary unit** check box. In this case, the primary unit cannot be cleared without a disposition. Other units can clear without a disposition.

4. From the Initial Status list, select the status to be used for all incidents created on the Local CAD system for the Foreign CAD agency

   The choices are Open or Closed. Pending is not an option because the local agency will not be managing the incident.

5. From the Dispo list, select the disposition code to be used when creating closed incidents for this Foreign CAD agency.

   This field displays only if the agency is a foreign agency.

   This field is required if the Initial Status field is set to **Closed** and/or the Incident to Mature Status field is set to **Closed**.

6. From the Incident to Mature Status list, select the status to be used for all scheduled incidents that mature on the Local CAD system for the Foreign CAD agency.

   A scheduled incident matures when it reaches its scheduled date and time.

7. If you require the dispatcher to review incident comments before dispatching incidents, select the **Incident comments review required before the incident can be dispatched** check box.

   Selecting this check box disables command-line dispatching, requiring the dispatcher to open the Incident Management form and review the incident information.

8. To allow open incidents, select the **Allow Open incidents** check box.

   An open incident is an incident that was active, but the unit assigned to it was cleared (generally occurs with fire agencies).

9. To disable automatic address verification, select the **Disable Automatic Address Verification** check box. Automatic address verification occurs when the user tabs out of the City field.

   This may be necessary for other countries besides the U.S.

10. To immediately display the Multi-Beat Selection form for the user's working agency in the Work Assist Area if the intersection contains multiple beats for the agency (and Global Offset = 0), select the **Display Multi-Beat Intersections upon Address Selection** check box.

    For details on the Global Offset feature, see "Configuring Location Verifications" on page 25-6.

11. To allow a CAD user to specify an incident to import a query response to, other than the incident currently opened in one of the work areas, select the **Allow CAD user to specify incident number to import query response to** check box.

    When this check box is selected, the Incident # field appears in the Import to Incident dialog box when importing query responses to an incident. For details on other query response import settings, see "Configuring Response Fields Mapping" on page 31-52.

12. Select one of the following actions to take when the last active unit is cleared from an incident that has units stacked against it:

    - To close the incident whenever the last active unit is cleared from a stacked incident, select the **Close the incident** button.

      This removes the incident from the call stacking queue of all the units.

    - To keep the incident in the call stacking queue of units stacked against the incident when the last active unit on the incident is cleared, select the **Keep incidents in unit's call stacking queue** button.

    - In the Set preempt default value to Yes section, select the check boxes for the commands/forms for which you want the default preempt value unit for the unit set to Yes. When the preempt value is Yes, the unit the incident is active on is returned to the unit's call stack queue or the pending queue depending on system settings, and the unit is dispatched to the new incident. The dispatcher can change the preempt value.

      Following is a list of forms and commands that contain the preempt value:

      Incident Initiation form and II command (follows working agency's setting)

      Field Initiate form and FI command (follows working agency's setting)

      Incident Dispatch form and ID command (follows incident's agency)

13. In the Print Size section, make any necessary changes.

14. In the Formatting Incident Numbers section, make any necessary changes.

    The Incident Sequence Number is a number that increments each time a new incident is created.

    CCYY is a two-digit century followed by a two digit year, such as 2008.

15. In the Generating Incident Numbers section, make any necessary changes.

16. In the Formatting Report Numbers section, make any necessary changes.

    The Reporting Sequence Number is a number that increments each time a new report number is created.

17. In the Generating Report Numbers section, set the next available report number, when to reset report numbers, and whether the report number format displays in client forms and on reports.

    To assign report numbers to units so that the report number comes from the agency owning the unit and *not* the agency owning the incident the unit is assigned to, select the **Enable unit-based report numbers for units dispatched onto any incident** check box. The two options below are enabled.

    - Select **Assign report number at initial dispatch** (default) to have a report number automatically assigned when the first unit for a given agency is assigned to the incident.
    - Select **Assign report number upon first unit being placed in Status Category**, and then select a status from the drop-down list to have a report number automatically assigned to the first unit assigned to the incident for a given agency that is placed in or *past* the provisioned status category.

    NOTE
    The Administrative and Clear statuses are not available because they are not associated with incidents. If your agency wants to generate a unit-based report number when the first unit clears from an incident, you can accomplish this by selecting the Assign Report Number At Initial Dispatch option.

18. In the Assigning Report Numbers section, make any necessary changes.

    - To only be able to assign one report number to an incident, select the **Assign one report number per incident** button.

      To assign report numbers automatically at dispatch, select the **Assign report number at initial dispatch** check box.
    - To be able to assign more than one report number to an incident, select the **Assign multiple report number per incident** button.
    - To be able to assign a report number using the unit ID, select the **Assign report number to unit** check box.
    - To be able to cancel a report number, select the **Cancel assigned report** check box.
    - To be able to delete a report number, select the **Delete assigned report** check box.
    - To only be able to assign one report number to multiple incident, select the **Assign multiple incidents to one report number** check box.

19. Click **Save**.

Configuring Initiation Defaults

Configure initiation defaults when you need to change any of the following information:

- General information, including whether to contact the complainant, the form to use after initiation, whether to automatically display ANI/ALI information, whether to automatically create associated incidents, and the role default for the initial caller.
- Duplicate incident check information, including whether to enable duplicate incident check, the duplicate check distance, and whether to include closed incidents and the time period for which to search for closed incidents.
- Traffic stop configuration information, including whether to use one pass or two pass traffic stops, whether to allow single-key traffic stop incident initiation, whether to require address verification, the unit's status, the incident type, the modifying circumstance, the alarm level, the default plate type, the home state, and how to create traffic stops for foreign units.
- Field-initiated incident information, including how to create field-initiated incidents for foreign units, the unit status, and whether to require address verification.
- Move up incident information, including whether to create incidents for move ups, and the default incident type, modifying circumstance, and disposition to associate with such incidents.
- Call stacking information, including whether to enable call stacking, the maximum call stack size, whether to automatically dispatch the next incident by incident priority or by first in first out, whether to allow the unit to dispatch the next incident, and to dispatch the first incident or any incident.
- Incident place of occurrence information, including the default city, default state, the latitude/longitude match distance parameters, and the location type search order.

To configure initiation defaults:

1. Access the form for existing service settings. For instructions, see "Configuring Service Defaults" on page 13-10.

   The Service Settings form appears with the Service Defaults tab in focus.

2. In the Service Settings form, select the Initiation Defaults tab.

The Initiation Defaults screen appears.

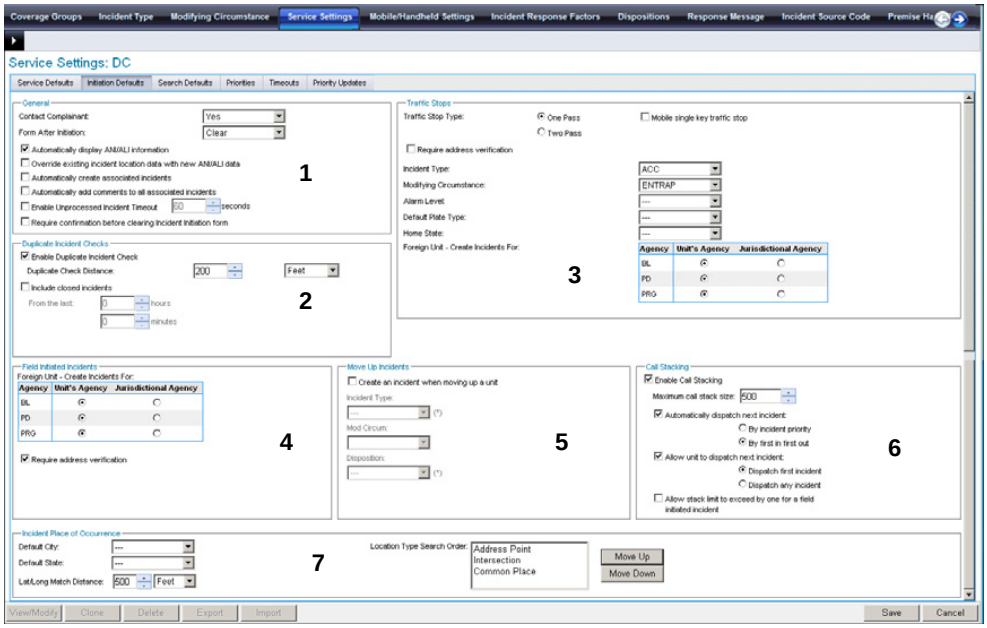


Figure 13-6 Service Settings Form – Initiation Defaults Tab

3. Click **View/Modify**.

4. In the General section (1 in the Figure 13-6), do any of the following:

   - From the Contact Complainant list, select the default Contact Complainant setting. The call taker can change this value.

     This is the setting that will automatically display in the II form; the call taker can change the value.

   - From the Form After Initiation list, select the form to display after an incident has been initiated: Update Incident, Dispatch Incident, or clear form.

   - To automatically populate the Incident Initiate form with 9-1-1 (ALI/ANI) information, select the **Automatically Display ALI/ANI** check box.

   - To override the existing incident location/address information with the new ANI/ALI information. select the **Override existing incident location data with new ANI/ALI data** check box.

   The following table describes the behavior of ANI/ALI data received from a voice call with respect to the two ANI/ALI settings. Each cell defines the behavior of either the Location or Caller fields when the position is in one of the three call modes. Because wireless phase 1 (WPH1) ANI/ALI typically contains cell tower location information, populating the Location fields in the Incident Initiation form with this information is not useful. Auto-populating the location would require the user to delete it from the Incident Initiation form each time.

Table 13-1 VOICE CALL: ANI/ALI & Incident Initiation Form

VOICE CALL: ANI/ALI & Incident Initiation Form						
Call Control Mode	**ACD**		**ACD w/ forced presentation**		**UCD**	
Provisioning Setting	**Incident Location**	**Caller Info**	**Incident Location**	**Caller Info**	**Incident Location**	**Caller Info**
Automatically display ANI/ ALI information = Yes (Non-WPH1 Call)	Auto-populates incident Location fields on RING when II form is displayed and blank	Auto-populates Caller fields on RING when II form is displayed and blank	Auto-populates incident Location fields on TALK when II form is displayed and blank	Auto-populates Caller fields on TALK when II form is displayed and blank	Auto-populates incident Location fields on TALK when II form is displayed and blank	Auto-populates Caller fields on TALK when II form is displayed and blank
Automatically display ANI/ ALI information = Yes (WPH1 Call)	Does not auto-populate Location location fields	Only name and phone number auto-populate in the Caller fields on RING when II form is displayed and blank	Does not auto-populate incident Location fields	Only name and phone number auto-populate the Caller fields on TALK when II form is displayed and blank	Does not auto-populate incident Location fields	Only name and phone number auto-populate Caller fields on TALK when II form is displayed and blank
Automatically display ANI/ ALI information = No	Does not auto-populate incident Location fields	Does not auto-populate Caller fields	Does not auto-populate Location location fields	Does not auto-populate Caller fields	Does not auto-populate incident Location fields	Does not auto-populate Caller fields
Override existing incident Location data with new ANI/ ALI data = Yes (via ANI/ALI button)	Will overwrite regardless of whether there are entries in the incident Location fields	Caller fields are always overwritten	Will overwrite regardless of whether there are entries in the incident Location fields	Caller fields are always overwritten	Will overwrite regardless of whether there are entries in the incident Location fields	Caller fields are always overwritten
Override existing incident location data with new ANI/ ALI data = No (via ANI/ALI button)	Will only update if incident Location fields are blank	Caller fields are always overwritten	Will only update if incident Location fields are blank	Caller fields are always overwritten	Will only update if incident Location fields are blank	Caller fields are always overwritten

- To create associated incidents without prompting the user for confirmation, select the **Automatically create associated incidents** check box.
- To automatically select the check box for adding comments to associated incidents, select the **Automatically add comments to all associated incidents** check box. The user can override this default.

- To display a warning icon in the Work Area tab when a user stops working on an incident (entering information or moving the cursor in the form), select the **Enable Unprocessed Incident timeout** check box. Then enter the time in seconds to use before displaying the icon in the adjacent field.

  This feature draws the user's attention to an unprocessed incident. When the user returns to the tab, the icon disappears.

- To display a confirmation dialog box before clearing the Incident Initiation form, select the **Require confirmation before clearing the Incident Initiation form** check box.

  The Conditional Clear feature prevents the CAD user from inadvertently losing data when performing an incident initiation.

  The following functions will display the conditional clear warning: Logoff, Exit/Close, Clear Form (F5, or CW command), and submission of any command line function that would normally clear the currently displayed form (for example, a request to display the Unit Status form).

  The user's cursor will return to the last field in which they were entering data when the action was taken.

5. In the Duplicate Incident Checks section (2 in the Figure 13-6), make any necessary changes.

   The duplicate incident check feature looks for incidents in the vicinity of the location.

   - To enable duplicate incident check, select the **Enable Duplicate Incident** check box. Then enter the duplicate check distance and select the units to use for the distance.

   - To include closed incidents in the search, select the **Include closed incidents** check box. Then enter the time period you want searched.

6. In the Traffic Stops section (3 in the Figure 13-6), do the following (see "Rules for Traffic Stop and Field-Initiated Incidents" on page 13-21 for more details on traffic settings):

   - From the Traffic Stop Type field, select whether traffic stops are one pass or two pass.

     For one-pass traffic stops, the incident is initiated immediately. For two-pass traffic stops, the unit is placed in a traffic stop status. A second action is required to initiate the incident.

   - To allow an officer to initiate a one pass traffic stop incident with a single key stroke, select the **Mobile single key traffic stop** check box.

The incident is created using the unit's GPS coordinates to derive both the incident location and the nearest crossroads. The officers status is automatically updated to the arrived state, as configured for the agency.

NOTE

Single key traffic stops can only be provisioned for one-pass traffic stops. If **Two-pass** is selected in the Traffic Stop Type field, then the Single key traffic stop field is disabled. Conversely, if One-pass and Single key traffic stop are selected, the unit cannot perform two-pass traffic stops.

- To require address verification, select the **Require address verification check** box.
- From the Incident Type list, select the incident type to use for the traffic stop. This incident type is always used unless the user enters or selects another value.
- From the Modifying Circumstance list, select the modifying circumstance for the incident type, if applicable.
- From the Alarm Level list, select the alarm level for the traffic stop, if applicable.
- From the Default Plate Type List, select the default plate type to use for the traffic stop, such as passenger vehicle or truck. This value is used when the unit does not specify a plate type.
- From the Home State list, select the state to use for the traffic stop. This value is used when the unit does not specify a state.
- In the Foreign Unit - Create Incidents For list, select the agency to use to create an incident when a unit from your agency enters the area of the agency responsible for the jurisdiction as defined by GIS.

  Unit's agency – Create an incident for the *unit's* agency whenever a unit from your agency creates a traffic stop incident within the jurisdiction of this incident's agency.

  Jurisdiction agency - Create an incident for the *jurisdictional* agency whenever a unit from your agency creates a traffic stop incident within the jurisdiction of this incident's agency.

For information on setting the unit status for traffic stops, see "Configuring Unit Status Transaction" on page 10-24.

7. In the Field Initiated Incidents section (4 in the Figure 13-6), do the following:.
   - In the Foreign Unit - Create Incidents From section, select the agency to use to create an incident when a unit from your agency enters the area of the agency responsible for the jurisdiction as defined by GIS.

     Unit's agency – Create an incident for the *unit's* agency whenever a unit from your agency creates a field initiated incident within the jurisdiction of the agency.

Jurisdiction agency - Create an incident for the *jurisdictional* agency whenever a unit from your agency creates a field initiated incident within the jurisdiction agency.

For information on setting the unit status for field initiated incidents, see "Configuring Unit Status Transaction" on page 10-24.

- To require address verification, select the **Require address verification check** box.

8. To configure move up settings, select the **Create an incident when moving up a unit** check box in the Move Up Incidents section (5 in the Figure 13-6). When you select this option, incidents are created each time a move up is performed. Therefore, select the incident type, modifying circumstance, and disposition for the incident.

   The moved units become the dispatched units on the incident.

   For information about move ups, see "Configuring Move Ups" on page 10-32.

9. In the Call Stacking section (6 in the Figure 13-6), make any necessary changes.

   - To enable call stacking, select the enable **Call Stacking** check box. Call stacking allows multiple calls to be assigned to an on-duty unit. Then enter the maximum call stack size (not greater than 999).

   - To automatically dispatch the next stacked incident to the unit when the unit completes a call, select the **Automatically dispatch next incident** check box. Then select whether the next incident should be selected by incident priority, or by first in first out (oldest incident dispatched next). This setting can be cleared by the dispatcher.

   NOTE
   When you enable this parameter, the unit automatically receives the next incident in the stack queue. When you disable this parameter, then the dispatcher can use the Dispatch action in the CS form or command to manually assign the next stacked incident to the unit.

   - To allow units to dispatch the next stacked incident to themselves, select the **Allow unit to dispatch next incident** check box. Then select whether the unit must dispatch the first incident or any incident.

   - To allow the call stack limit to be exceeded by one for a field-initiated incident, select the **Allow call stack limit to exceed by one for a field initiated incident** check box (this is for CAD use only). Mobile users are not limited by this setting. They will always be able to create field initiated incidents.

     This allows a dispatcher to create a field-initiated incident when the unit is already assigned another incident. If the unit's call stacking queue is equal to the maximum call stack size, what occurs depends on whether preempting is enabled for the incident.

The dispatcher controls whether a unit's currently assigned incident should be preempted, or placed on hold, for a new assignment. This setting is set by the dispatcher for each incident in the II, FI, and ID forms or commands, although you can provision a default value (see Set Preempt Default Value on page 13-13).

Allow call stack limit to exceed by one for a field initiated incident = Yes

For Preempt = Y, the unit is assigned to the new incident and the current incident is returned to the call stacking queue.

For Preempt = N, the unit remains assigned to the current incident and the new incident is placed in the unit's stack queue.

Allow call stack limit to exceed by one for a field initiated incident = No

For Preempt = Y, the unit is assigned to the new incident and incident the unit was active on is returned to the initial status configured for the agency (normally this would be the pending status).

For Preempt = N, the dispatcher cannot initiate the incident and will receive an error message to that effect.

NOTE

Mobile users can always create a field initiated incident or a traffic stop (the stack counter does not apply for mobile users). If an officer creates an incident while already active on another call, the first call is pre-empted.

10. In the Incident Place of Occurrence section (7 in the Figure 13-6), select the Default City, Default State, and Lat/Long Match Distance to be used during incident initiation.

    The Lat/Long Match Distance is how far you want to search from a Lat/Long coordinate that is entered during incident initiation for a matching address, intersection, or common place.

11. Click **Save**.

Rules for Traffic Stop and Field-Initiated Incidents

When a user performs a field-initiated or traffic stop transaction for a unit, PremierOne checks the corresponding parameters you provision for the unit's agency, regardless of which agency is responsible for the physical location of the incident. The following rules govern the creating of traffic stops and field-initiated incidents:

- Performing a field-initiated transaction without specifying an IRF creates a traffic stop
- Specifying multiple units for a field-initiated or traffic stop transaction

  The dispatcher is restricted to specifying multiple units from the same agency only.

- Determining the incident’s agency

  When a user creates a traffic stop incident, PremierOne checks the Traffic Stop Foreign Units - Create Incident For: parameters that you provision for the unit’s agency.

  When a user creates a field-initiated incident, PremierOne checks the Field Initiated Incident's Foreign Units - Create Incident For: parameters that you provision for the unit’s agency.

  When creating a field-initiated incident and an IRF is not specified, PremierOne uses the IRF provisioned for the *unit’s* agency to create the incident, regardless of the agency the incident is being created for.

- Field-initiated or traffic stop incident for the unit's agency’s

  A field-initiated or traffic stop incident is created for the unit's agency under the following conditions:

  - If the geo-validated or bypassed field-initiated location is within the jurisdiction of the unit’s agency.

    The incident will be assigned to the specified jurisdiction.

  - If Require Address Verification = No for the unit's agency and the user does not specify any jurisdictional information for the field-initiated incident.

    Because no jurisdiction is specified, the incident will be assigned to: Agency = Unit’s Agency and Area = Default Area for the unit's agency.

  - If the geo-validated or bypassed field-initiated location is within the jurisdiction of an agency other than the unit’s agency, and the unit’s agency has provisioned the {Foreign Unit} parameters for the jurisdictional agency to require an incident be created for the unit's agency.

    The incident will be assigned to the following jurisdiction: Agency = Unit's Agency and Area = Default Area for the Unit's Agency. This assignment occurs because PremierOne attempts to create an incident for the unit's agency based on the jurisdiction of the incident being in another agency's jurisdiction.

    If the incident is geo-validated, the incident will be given the Lat/Long coordinates for the location, even though the jurisdictional assignment does not correspond to these coordinates.

- Field-initiated incident for the jurisdictional agency

  A field-initiated incident is created for the jurisdictional agency responsible for the field-initiated location whenever the geo-validated or bypassed field-initiated location is within the jurisdiction of an agency other than the unit's agency, *and* the unit's agency has provisioned the {Foreign Unit} parameter for the jurisdictional agency to require an incident be created for that jurisdictional agency.

The incident is assigned to the specified jurisdiction. If the incident is geo-validated, the incident is given the Lat/Long coordinates for the location.

Configuring Search Defaults

Configure search defaults when you need to set the search distance for previous incidents, the default sort for returned incidents, and previous subject and vehicle search information.

To configure search defaults:

1. Access the form for existing service settings. For instructions, see "Configuring Service Defaults" on page 13-10.

   The Service Settings form appears with the Service Defaults tab in focus.

2. In the Service Settings form, select the Search Defaults tab.

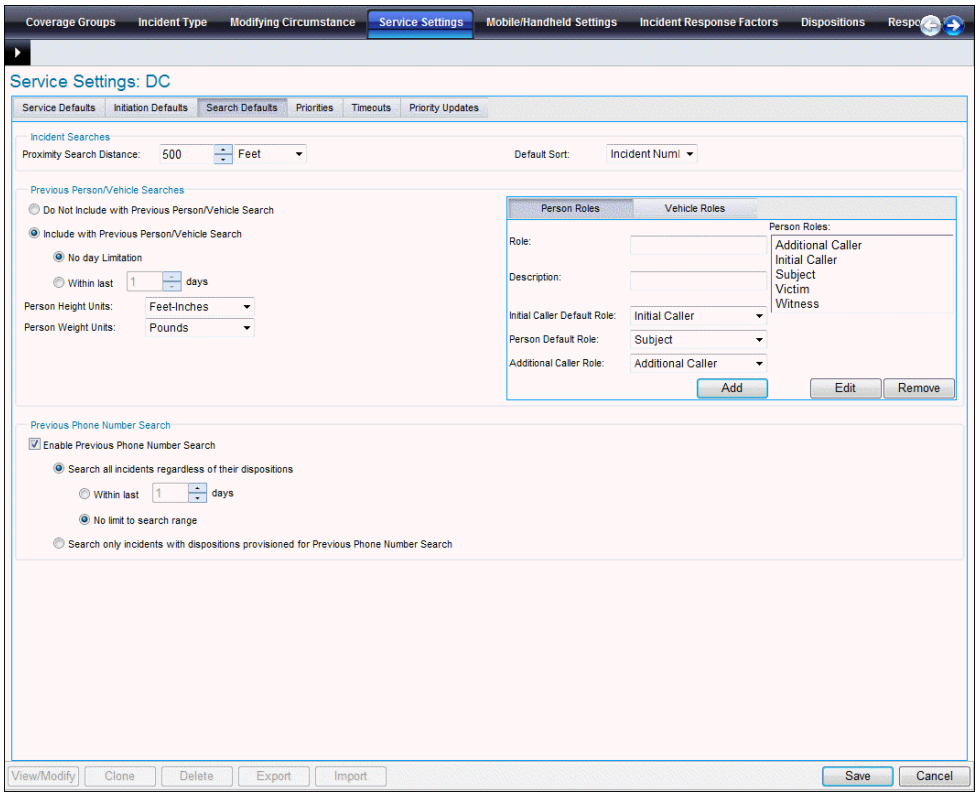


Figure 13-7 Service Settings Form – Search Defaults Tab

3. Click **View/Modify**.

4. In the Incident Searches section, do any of the following:

   - Using the Search Distance lists, enter the distance you want to search for previous incidents.
   - From the Default Sort list, select how you want the incidents sorted.

5. In the Previous Subject/Vehicle Searches section, do any of the following:

   - If you do not want persons or vehicles from previous searches in a search, select the **Do not include with previous Person/Vehicle Search** button.
   - If you want to include persons and vehicles from previous searches in a search, select the **Include with Previous Person/Vehicle Search** button. Then set the amount of time for the search to extend, either no day limitation or a specific limitation.
   - From the **Person Height Units** list, select the unit to use for the height of persons.
   - From the **Person Weight Limit**, select the unit to use for the weight of persons.

6. To search for incidents having the same phone number, select the **Enable Previous Phone Number Search** check box in the Previous Phone Number Search section.

   Then select one of the following:

   - To search for all incidents with a phone number regardless of their disposition, select the **Search all incidents regardless of their dispositions** check box. Then select the **Within last** button and enter the number to days to search, or select the **No limit to search range** button.
   - To search for all incidents with a phone number that only have dispositions provisioned for the Previous Phone Number Search, select the **Search only incidents with dispositions provisioned for Previous Phone Number Search** button.

     For details on configuring dispositions, see “Configuring Dispositions” on page 13-43.

7. In the Role section, do the following to add role types to the Persons and Vehicles forms in CAD.

   a. Select the subtab for the type of role you want to add: Subject role, Vehicle role, or Additional Caller role.

   b. In the Role field, type a name for the role.

   c. In the Description field, type a description for the role.

   d. Click **Add**.

      The role appears in the Subject, Vehicle, or Additional Caller Roles box.

      Edit or remove roles by selecting the role from the box and clicking **Edit** or **Remove**.

8. In the Role section, select the default roles for the Initial Caller, Person, and Additional Callers.

9. Click **Save**.

Configuring Priorities

Configure incident priorities to set which priorities are valid, whether to sort priorities by ascending or descending order, whether a sub-priority is required, which sub-priorities are valid, and whether to allow users to lower incident priority.

The priority determines where the call is positioned in the pending queue and potentially whether a priority message is sent to all consoles when an incident of the priority is initiated.

To configure priorities:

1. Access the form for existing service settings. For instructions, see "Configuring Service Defaults" on page 13-10.

   The Service Settings form appears with the Service Defaults tab in focus.

2. In the Service Settings form, select the Priorities tab.

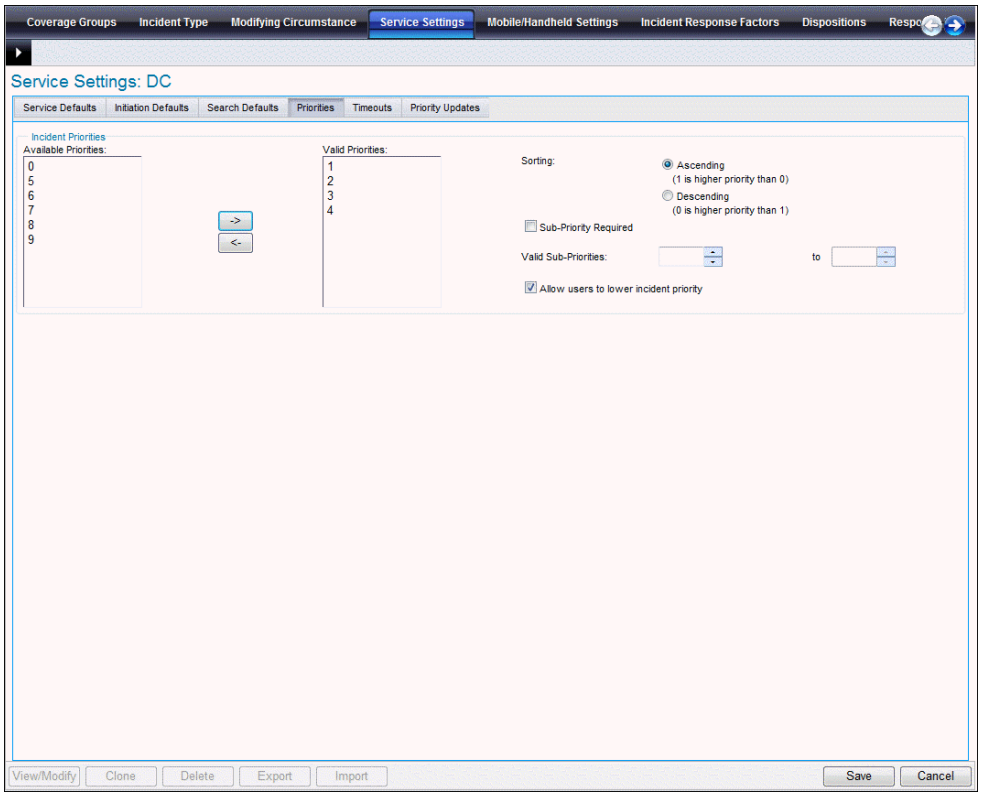


Figure 13-8 Service Settings Form – Priorities Tab

3. Click **View/Modify**.

4. From the Available Priorities list, select the priorities that will be available to your agency.

   Values must be in sequence, such as 0 through 4 or 4 through 8.

5. From the Sorting list, select whether your agency will use ascending or descending order for priorities.

   If you use ascending order, 1 is a higher priority than 0, 2 is a higher priority than 1, and so on.

   If you use descending order, 0 is a higher priority than 1, 1 is a higher priority than 2, and so on.

6. In the Sub-Priority Required field, select the check box if your agency will use sub-priorities.

   A priority without a sub-priority is higher than a priority/sub-priority combination. For example, 2 is higher than 2A.

   CAUTION
   If you want to use subpriorities, be sure to select this check box before configuring the IRFs; otherwise, an error message will display when you try to save this setting. If you have already configured IRFs and want to use subpriorities, you will need to delete the IRFs, select the Sub-Priority Required check box, and read the IRFs.

7. In the Valid Sub-Priorities field, select the range of letters to use for sub-priorities.

   Values must be in sequence, such as A through J or K through R.

8. In the Allow users to lower incident priority field, select whether the users in your agency can lower a priority.

9. Click **Save**.

Configuring Incident Timeouts

Incident timeouts control how long an incident of a specific priority and status can be in a status before a message is sent to specific recipients. Status monitors can also be provisioned to change colors when incidents timeout.

To configure incident timeouts:

1. Access the form for existing service settings. For instructions, see “Configuring Service Defaults” on page 13-10.

   The Service Settings form appears with the Service Defaults tab in focus.

2. In the Service Settings form, select the Timeouts tab.

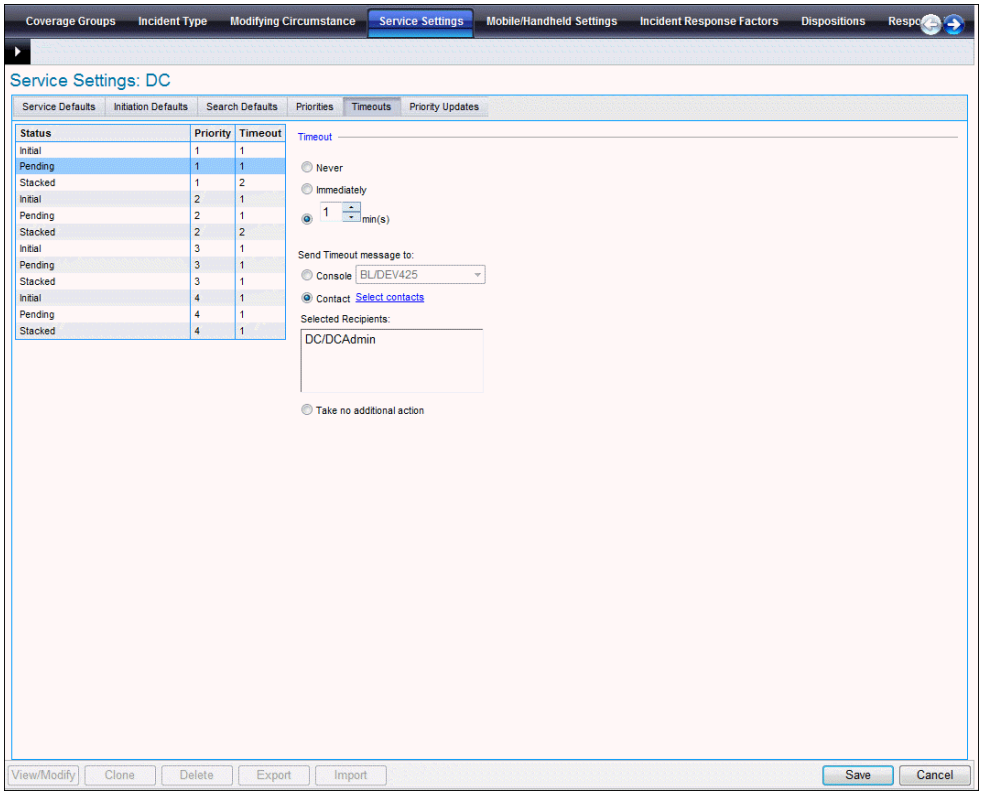


Figure 13-9 Service Settings Form – Timeouts Tab

3. From the Status list, select an incident status with the timeout you want to change.

   For example, instead of a priority 1 Pending status having a timeout value of 1 minute, you could change the timeout value to 2 minutes. Alternatively, you could change it to never timeout.

4. Set the timeout value to **Never**, **Immediately**, or a value in minutes.

5. Select whether you want to send a timeout message. You can send a message to a specified console, to a specified contact, or you can choose to take no action (send no message).

- If you select Console, select the specific console from the list.
- If you select Contact, click the **Select contacts** link to display the Select Contacts dialog box.

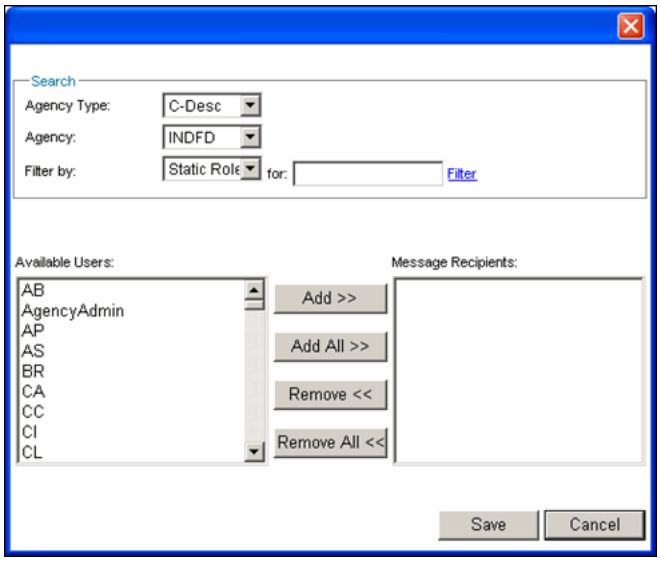


Figure 13-10 Select Contacts Dialog Box

a. If necessary, change the values in the Agency Type and Agency lists.

   You can also choose a value to filter by and enter a value to filter for.

b. From the Available Users box, select users and click **Add**.

c. Click **Save**.

6. Repeat the task to set up each status with the timeout as needed.
7. Click **Save**.

Configuring Priority Updates

You can configure fields to be monitored in the Incident Management form in CAD and mobile so that when a field is updated by a user (adding, modifying, or deleting a value), the field label and tab containing the field display in a different format to other users. When a user views and then closes the form, the special formatting is removed.

NOTE

The term *priority updates* does not refer to the Priority field itself. Although you can configure the Priority field to be monitored, it is not monitored by default.

- To set whether a Notification dialog box displays alerting users when priority updates occur, see “Adding Role General Information” on page 8-2.

- To configure status monitors so that an icon or text displays indicating priority updates exist that have not been viewed, see “Configuring CAD Status Monitor Icons” on page 32-3 (configure the Priority Notification icon).

To enable and configure priority updates:

1. Access the form for service settings. For instructions, see “Configuring Service Defaults” on page 13-10.

   The Service Settings form appears with the Service Defaults tab in focus.

2. In the Service Settings form, select the Priority Updates tab.

3. Select the CAD Settings tab.

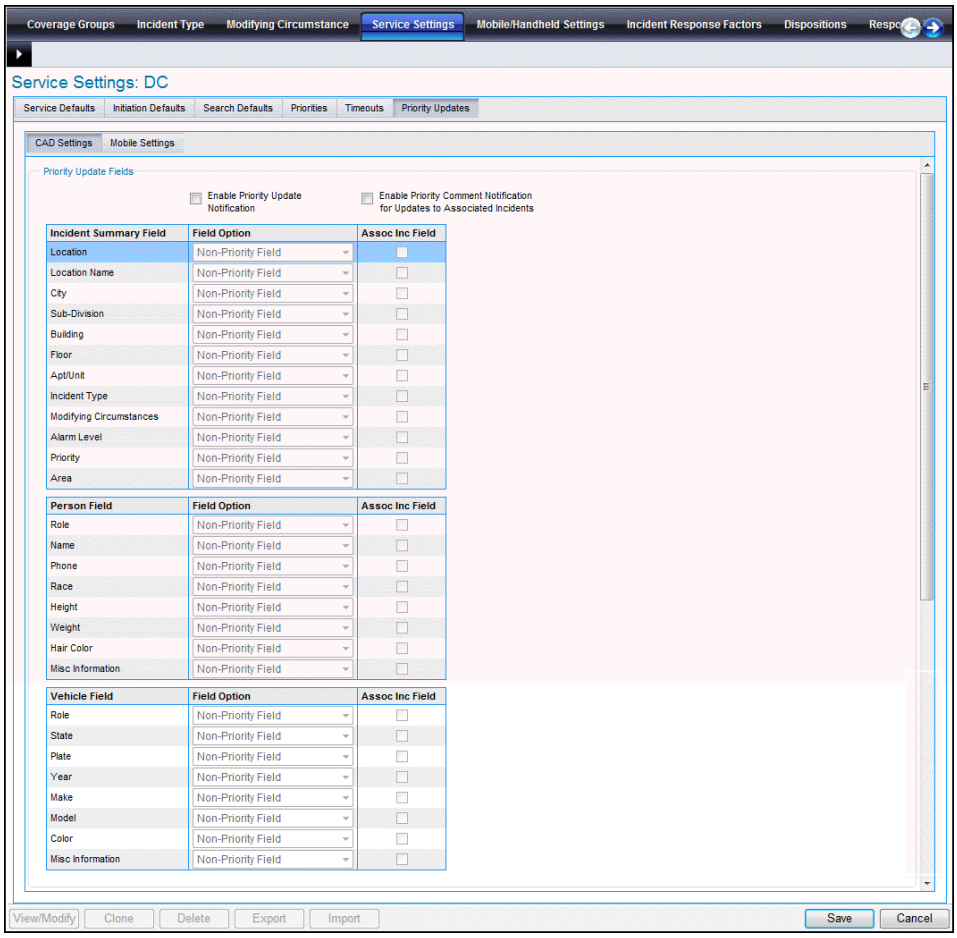


Figure 13-11 Service Settings Form – CAD Settings Tab For Priority Updates

4. To enable priority updates, select the **Enable Priority Update Fields** check box at the top of the form.

5. To enable priority updates for associated incidents, select the **Enable Priority Comment Notification for Updates to Associated Incidents** check box at the top of the form.

6. For each field you want monitored for updates, select one of the following:

   - Select **Non-Priority** field if you do not want to display the field label and tab in a different format and do not want to display a Priority Notification dialog box.

   - Select **Priority Field** to display the field label and tab containing the field in a different format.

     The label for the updated field displays in red and is followed by an asterisk (*).

     When a tab has an update to a priority field, the tab displays with a white label and an asterisk and red background when selected, and red label with an asterisk when unselected.

     When the Work Assist Area has an update to a priority field, the Person or Vehicle Summary record displays with white text and red background when selected and red text and white background when unselected.

     After a priority update is viewed and the form is closed, all special formatting is removed.

   - Select **Priority Field with Notification** to display the field label and tab containing the field in a different format *and* display the Priority Notification dialog box.

     The Priority Notification dialog box displays whenever another user enters priority comments or makes priority updates to an incident the dispatcher is monitoring. The title bar for the dialog box flashes to draw the user's attention to it.

   - Select the **Associate Inc field** check box to monitor the field for updates in any associated incidents. The same action will occur in the associated incident that you select: formatting of the priority field, or formatting of the priority field and display of the Priority Notification dialog box.

7. Click **Save**.

Configuring Priority Updates – Mobile

You can configure fields to be monitored in the Incident Management form in Mobile so that when a field is updated by a user (adding, modifying, or deleting a value), the field label and tab containing the field display in a different format to other users. When a user views and then closes the form, the special formatting is removed.

NOTE

The term *priority updates* does not refer to the Priority field itself. Although you can configure the Priority field to be monitored, it is not monitored by default.

To enable and configure priority updates for Mobile:

1. Access the form for service settings. For instructions, see "Configuring Service Defaults" on page 13-10.

   The Service Settings form appears with the Service Defaults tab in focus.

2. In the Service Settings form, select the Priority Updates tab.

3. Select the Mobile Settings tab.

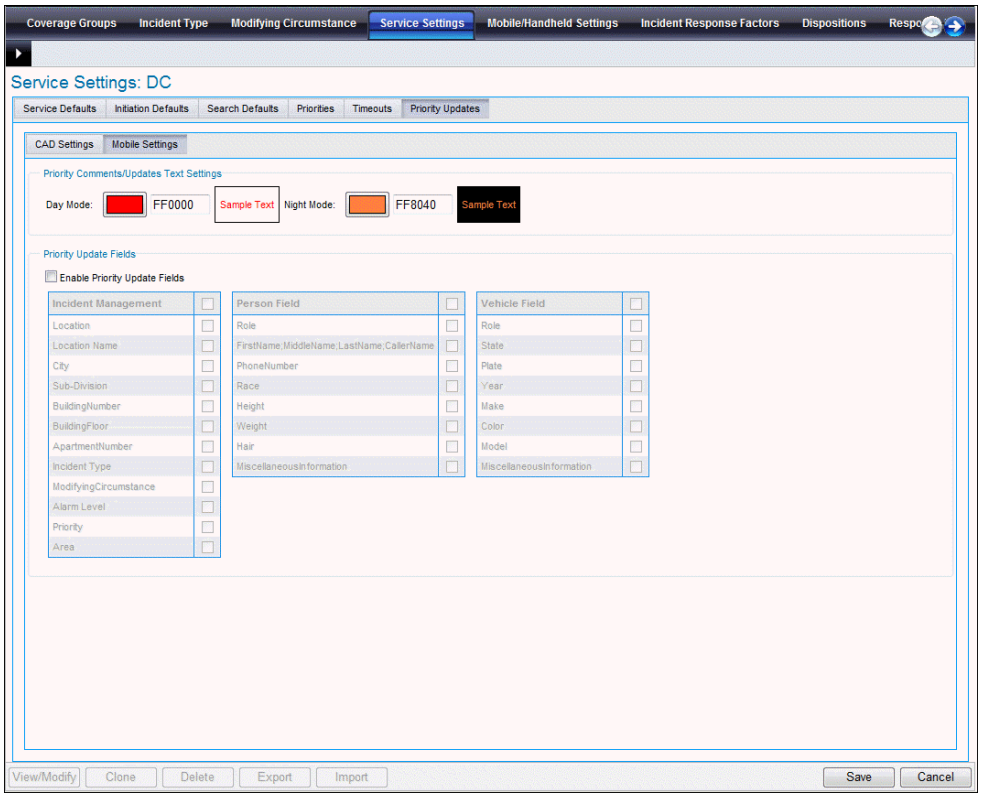


Figure 13-12 Service Settings Form – Mobile Settings Tab For Priority Updates Tab

4. In the Day Mode field, click the color field to select the color for the priority updates during the day. You can alternatively enter the Hexadecimal code in the adjacent box.

5. In the Night Mode field, click the color field to select the color for the priority updates at night. You can alternatively enter the Hexadecimal code in the adjacent box.

6. To enable priority update fields, select the **Enable Priority Update Fields** check box.

7. For each field you want monitored for updates, select the adjacent check box.

8. Click **Save**.

Configuring Mobile/Handheld Incident Settings

The Incident Management Mobile/Handheld Settings configuration contains the following configuration item:

Priority Settings – Audio and visual alerts that notify Mobile/Handheld users when new incidents are sent to their mobile unit.

Configuring Mobile/Handheld Priority Alert Settings

You can set audio or visual alert information to notify a mobile or handheld unit that an incident of a specific priority has been assigned to their unit, or that an active incident of a specific priority has been updated. You can also configure whether mobile/handheld units can change the settings for their own unit.

Configuring Mobile/Handheld Priority Alert Settings for Incident Dispatch

Use the Incident Dispatch tab to configure Mobile/Handheld priority alert settings for incident dispatch.

To configure Mobile/Handheld priority alert settings for incident dispatch:

1. Access the form for existing Mobile/Handheld settings. For instructions, see "Configuring Mobile/Handheld Incident Settings" on page 13-32.

   The Priority Settings screen appears, with the Incident Dispatch tab in focus and the Use default settings check box selected. The following figure shows the Use default settings field deselected so fields are easier to see.

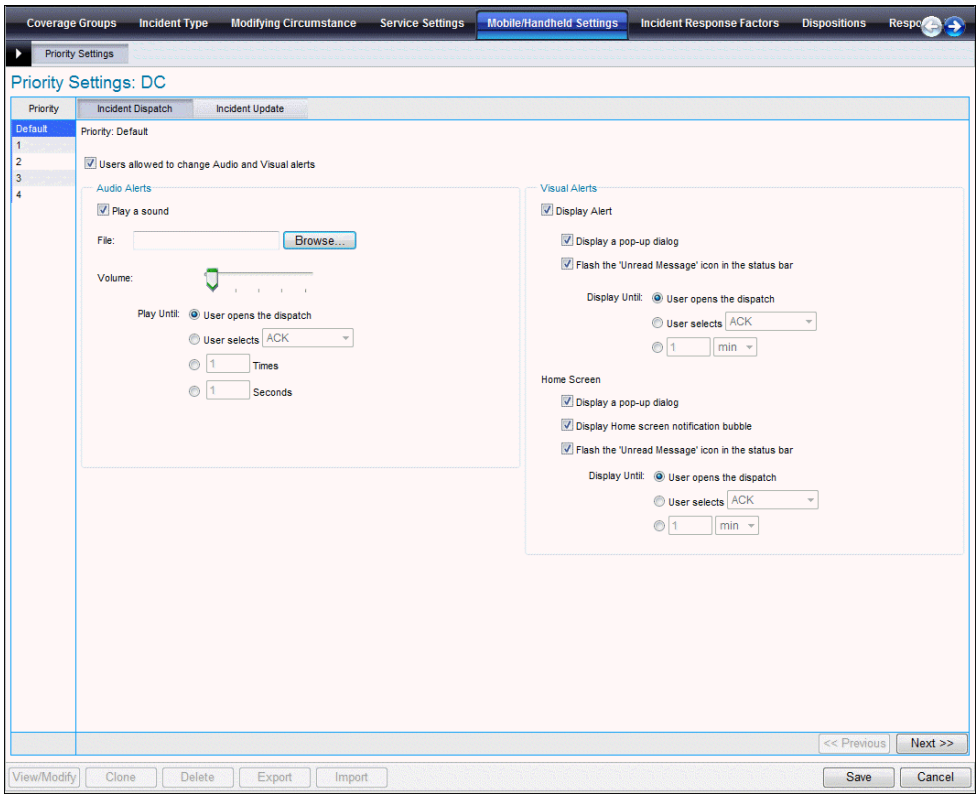


Figure 13-13 Priority Settings Form – Incident Dispatch Tab

2. Click **View/Modify**.

3. In the Priority column, select the incident priority for which you want to configure alerts.

4. Do one of the following:
   - To only use the Provisioning settings, select the **Use default settings** check box.
   - To allow Mobile/Handheld users to change the alert settings in their mobile unit, select the **Users allowed to change Audio and Visual alerts** check box.
5. To use Audio Alerts, select the **Play a sound** check box and then do the following:
   a. Browse to and select the audio file to play.
   b. Set the volume.
   c. In the Play Until field, select the action that will stop the alert:
      - the user opens the dispatch
      - the user selects the specified status
      - the audio file has played a specified number of times
      - the audio file has played for a specified number of seconds
6. To use Visual Alerts, select the **Display Alert** check box. Then do the following:
   a. To display a dialog box, select the **Display a popup dialog** check box.
   b. To flash an icon in the Mobile status bar, select the **Flash the "Unread Message" icon in the status bar** check box.
   c. In the Display Until field, select the action that will stop the alert:
      - the user opens the dispatch
      - the user selects the specified status
      - the icon has flashed for the specified amount of time
   d. To display a dialog box on the Home screen, select the **Display a pop-up dialog** check box.
   e. To display a notification bubble on the Home screen, select the **Display Home screen notification bubble** check box.
   f. To flash an icon in the status bar on the Home screen, select the **Flash the "Unread Message" icon in the status bar** check box.

      In the Display Until field, select the action that will stop the alert:

- the user opens the dispatch
- the user selects the specified status
- the alert has displayed for the specified amount of time.

7. Click **Save**.

Configuring Mobile Priority Alert Settings for Incident Updates

Use the Incident Updates tab to configure Mobile priority alert settings for incident updates.

To configure Mobile priority alert settings for incident updates:

1. Access the form for existing Mobile settings. For instructions, see "Configuring Mobile/Handheld Incident Settings" on page 13-32.

   The Priority Settings screen appears, with the Incident Dispatch tab in focus.

2. Select the Incident Update tab.

   The Incident Update Priority Settings screen appears, with the Use default settings check box selected. Figure 13-14 shows the Use default settings field deselected so fields are easier to see.

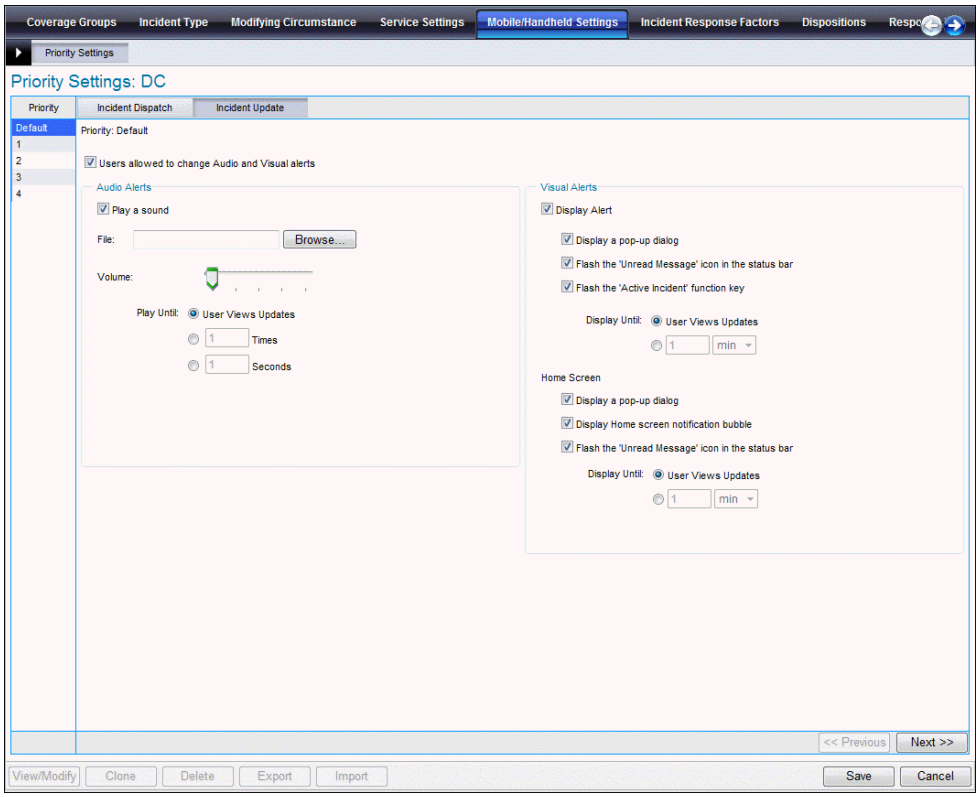


Figure 13-14 Priority Settings Form – Incident Update Tab

3. Click **View/Modify**.
4. In the Priority column, select the incident priority for which you want to configure alerts.
5. Do one of the following:
   - To only use the Provisioning settings, select the **Use default settings** check box.
   - To allow Mobile/Handheld users to change the alert settings in their mobile unit, select the **Users allowed to change Audio and Visual alerts** check box.
6. To use Audio Alerts, select the **Play a sound** check box and then do the following:
   a. Browse to and select the audio file to play.
   b. Set the volume.
   c. In the Play Until field, select the action that will stop the alert:
      - the user views the updates
      - the audio file has played the specified number of times
      - the audio file has played for the specified number of seconds
7. To use Visual Alerts, select the **Display Alert** check box. Then do the following:
   a. To display a dialog box, select the **Display a popup dialog** box check box
   b. To flash the unread message icon in the status bar, select the **Flash the "Unread Message" icon in the status bar** check box.
   c. To flash the Active Incident function key, select the **Flash the 'Active Incident' function key** check box.
   d. In the Display Until field, indicate whether to display the alert until the user views the updates or until the specified amount of time has expired.
   e. To display a dialog box on the Home screen, select the **Display a pop-up dialog** box.
   f. To display a notification bubble on the Home screen, select the **Display Home screen notification bubble** check box.
   g. To flash the unread message icon in the status bar, select **Flash the "Unread Message" icon in the status bar** check box.
   h. In the Display Until field, indicate whether to display the alert until the user views the updates or until the specified amount of time has expired.
8. Click **Save**.

Configuring Incident Response Factors

Incident Response Factor general information includes whether the dispatcher must review incident comments before dispatching the incident, previous incident search criteria, setting the override area, and available dispositions for the IRF.

You can add, clone, modify, delete, import, and export incident response factors. For details on cloning, modifying, deleting, importing, and exporting, see "Working With Configuration Items" on page 2-9.

Two tabs are available:

- Incident type – Where you set the incident type and modifying circumstance, and set General settings, which include whether command line dispatching is allowed, settings for previous searches for the incident type, incident priority, available dispositions, and dispositions used to create a closed incident.
- Attributes – Where you set alarm levels, incident priority, response ID, override area, associated incidents, and notification messages.

How each of these factors is used by agencies is highly variable.

NOTE

IRFs can be defined for agency types (such as fire, medical, and law) and then modified for an agency. If an IRF is defined for both an agency type and agency, the settings for the agency override those of the agency type.

Defining IRFs at the agency level helps limit the number of codes that exist for centers that have multiple agencies. Dispatchers can override any of the individual response factors, if needed.

You can add, modify, clone, delete, import, and export IRFs. For details on deleting and cloning IRFs, see "Working With Configuration Items" on page 2-9. You can only add IRFs for agency types, but you can modify existing IRFs for your individual agency.

Adding IRF General Information

Incident Response Factor general information includes whether the dispatcher must review incident comments before he or she dispatches the incident, previous incident search criteria, and available dispositions for IRF.

To add IRF general information:

1. From the navigation panel, select **Incident Management**, and then select **Incident Response Factors**.

The Incident Response Factors form appears with the General tab in focus. A list of incident types and their corresponding modifying circumstances displays on the left side of the form.

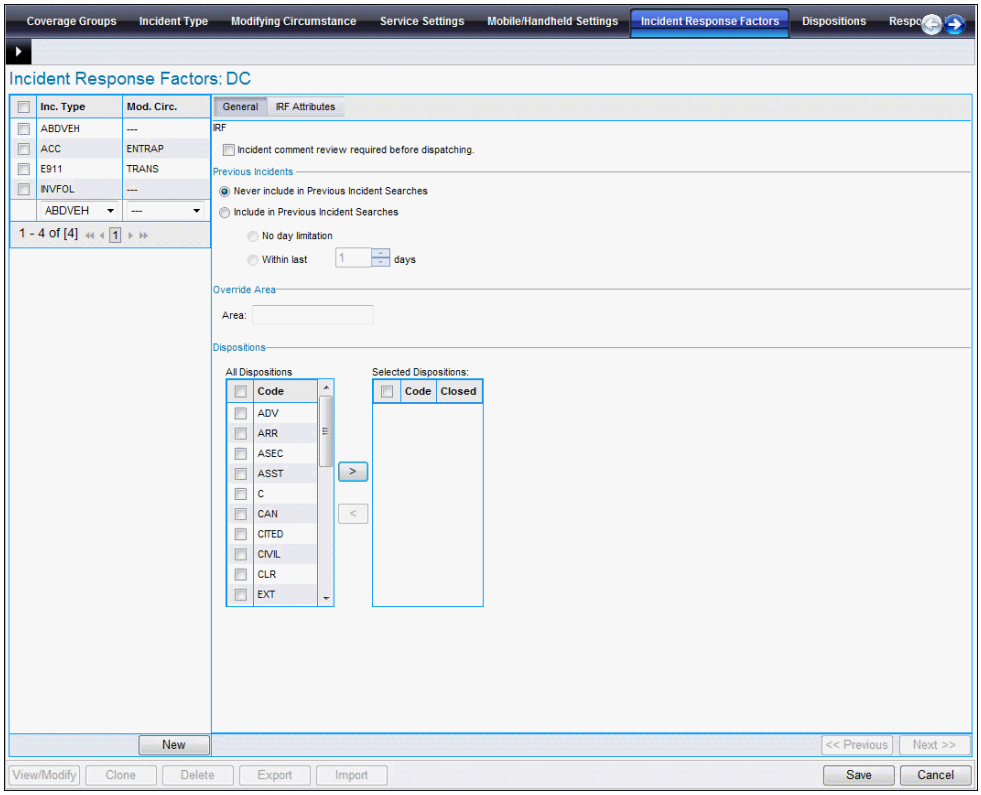


Figure 13-15 Incident Response Factors Form – General Tab

2. At the bottom of the Incident Type list, click the **New** button.

3. From the blank field at the bottom of the Incident Type list, select the incident type to which you want to associate the incident response factors.

4. In the blank field next to the incident type, select a modifying circumstance for the incident type.

   Modifying circumstances override the priority, subpriority, and response code settings of an existing IRF.

5. Select whether to require the dispatcher to review incident comments before dispatching an incident with the IRF.

   Selecting the check box disables command-line dispatching.

6. Select whether this IRF should be included in previous incident searches. If you include the IRF in previous incident searches, enter the limitation for the searches, no day limitation, or a set number of days.

7. In the Override Area field, enter an area to use whenever an incident is created using this IRF (optional). This value is provisioned against the incident type, modifying circumstance, and alarm level = Null only. The area that you enter is not validated in provisioning.

   When an incident of this IRF is created (with the exception of field-initiated incidents), the incident is created in the override area regardless of where it geographically. This is true for the II, CI, and LD commands and for creating associated incidents. If the incident is changed to a different IRF, address verification will reoccur.

   This allows the geographical area to be overridden and assignment of the incident to the override area. This can be useful, for example, when you want to assign non-emergency incidents to a fixed station such as a report desk.

8. From the All Dispositions list, select the check boxes for the dispositions you want made available for this IRF.

   These are the only dispositions that will be allowed for the IRF. If you do not select any dispositions for the IRF, then *all* dispositions are made available by default.

9. For a disposition to close an incident, select the **Closed** check box to the right of the disposition. Otherwise, the disposition will not close the incident.

   Agencies may want to create closed incidents for various reasons, such as accidental calls, prank calls, or nonemergency calls that come in as emergency calls.

   If an IRF is provisioned with a Close disposition, the incident will always be created as a closed incident. This includes the incident initiation process, the field initiation process, the clone incident process, and the creation of associated incidents. The call taker can always override the default.

   If an IRF is provisioned with a Close disposition, a dispatcher can also initiate the closed incident without entering a disposition.

10. Click **Save**.

Adding IRF Attributes

Incident Response Factors (IRF) attributes include alarm level, incident priority, response ID, associated incidents, and notification messages.

NOTE

When an incident is created using the Alarm #, the Alarm provisioning settings are followed and not the IRF provisioning settings.

To add IRF attribute information:

1. Access the form for new incident response factors. For instructions, see "Adding IRF General Information" on page 13-37.

   The Incident Response Factors form appears with the General tab in focus (see Figure 13-15). A list of incident types and their corresponding modifying circumstances displays on the left side of the form.

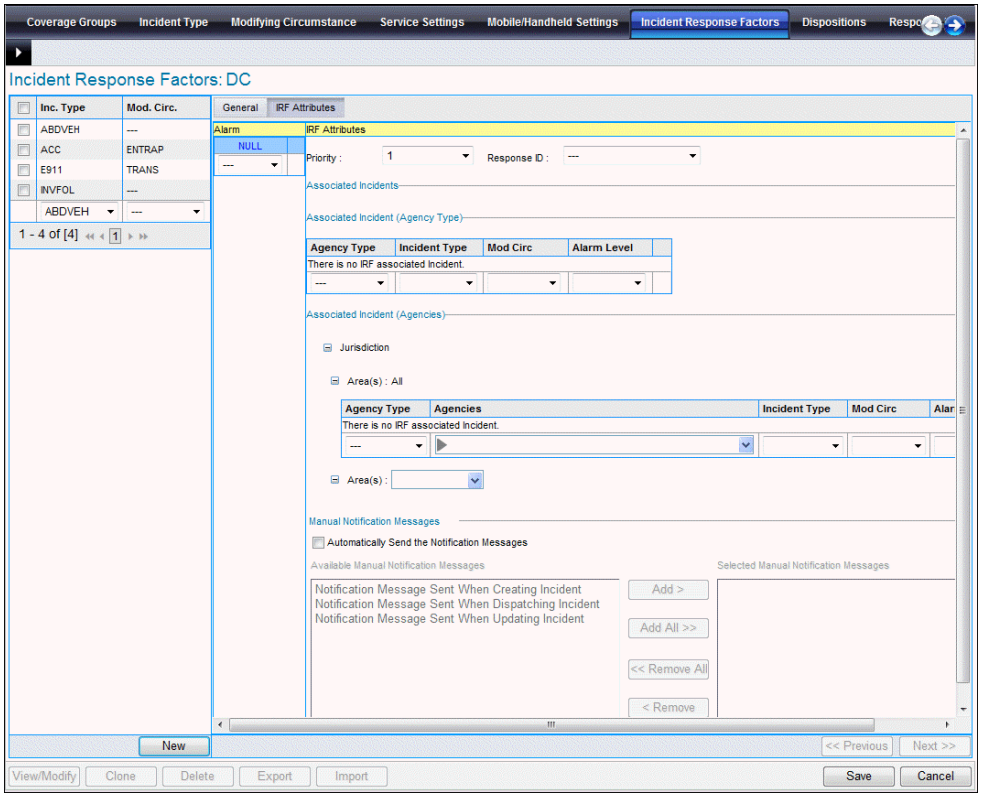


Figure 13-16 Incident Response Factors Form – IRF Attributes Tab

2. Select the incident type to which you want to associate the incident response factors.

3. If applicable, select the alarm level for the IRF in the alarm section. Alarms are used to escalate the response to an incident.

   The alarm level can be used in many different ways. The alarm level in an IRF only modifies the recommended response in the way that you define it to. Alarm levels are used to increase or decrease the manpower required on the scene. While alarm level usually applies to fire departments, they can be applied to any agency type.

4. From the Priority list, select the priority level for the IRF.

Incident priority determines where the call is positioned in the pending queue and controls whether a priority message is sent to all consoles.

CAUTION
If your agency is using subpriorities, be sure to configure those first or they will not be available for selection. For details, see "Configuring Priorities" on page 13-25.

5. From the Response ID list, select a response ID.

   Response IDs allow the IRFs to be grouped by common response requirements. For more information, see "Configuring Response IDs" on page 14-15.

6. To create associated incidents in other *agency types* for this IRF, select the agency type, incident type, modifying circumstance, and alarm level in the Associated Incidents (Agency Type) section. Click the plus symbol to the right of the row to save the entry to add a new line. These entries cannot be deleted.

CAUTION
If you do not click the plus symbol, PremierOne does not save the code information, even after you click Save.

These associated incidents are incidents you want created for other agency types, such as fire or EMS. These settings allow you to override the IRFs for the associated incidents.

NOTE
A Provisioning setting controls whether associated incidents are automatically created or whether the user is prompted for a confirmation before creating the incidents. For details, see "Configuring Initiation Defaults" on page 13-15.

7. If you are defining the IRF at the agency level and want to create associated incidents in other *agencies*, regardless of the agency type, do one of the following in the Associated Incidents (Agencies) section:

- To create associated incidents for all areas, click the plus sign (+) to the left of the Areas label to expand it. Fields for Agency Type, Incident Type, Modifying Circumstance, and Alarm will display.

Figure 13-17 Areas Label – All Areas

- To create incidents only in specific areas, click the green plus sign (+) to the right of the Areas label and select the areas. In addition to fields for Agency Type, Incident Type, Modifying Circumstance, and Alarm, a list of Areas will also display

Figure 13-18 Areas Label – All Areas

Selecting areas allows your agency to create associated incidents for neighboring agencies that are not primarily responsible for the incident's jurisdiction, but who have agreed to assist with incident response.

8. Select the agency type, agencies, incident type, modifying circumstance, and alarm level. You may need to scroll to the right to see all of these fields. You must first select the agency type before the agencies list is populated.

9. To automatically send notification messages when an incident of this IRF is initiated (alarm = blank) or updated to an alarm level greater than or equal to one, select the Automatically send Notification Message check box.

   Then select the messages to send from the Manual Notification Available list. For details on configuring the recipients and text of the message, see "Configuring Manual Notifications" on page 24-3.

10. Repeat the procedure beginning with selecting an alarm level for any other alarm levels you want to add to the IRF.

    The alarm level in an IRF only modifies the recommended response in the way that you define it to. Alarm levels are used to increase or decrease the manpower required on the scene.

11. Click **Save**.

    The IRFs you added appear the Incident Type list on the left in black text.

12. Repeat the procedure for any other IRFs you want to add.

Configuring Dispositions

Dispositions are usually required to close an incident and clear the primary unit from the call. Use the Incident Management Dispositions configuration item to configure and manage dispositions. Dispositions are defined at the agency level.

You can add, modify, clone, and delete disposition codes. For details on cloning and deleting disposition codes, see “Working With Configuration Items” on page 2-9.

Adding Disposition Codes

When you add a disposition code, you enter information on the Disposition Settings form.

Disposition code settings include the disposition code, code description, whether a comment is required, whether a report is required, and whether a false alarm is required.

You cannot change the disposition code itself. If you want to change the code, you must delete and re-add the record.

To add a disposition code:

1. From the navigation panel, select **Incident Management**, and then select **Dispositions**.

The Disposition Settings form appears. A list of existing disposition codes displays on the left side of the form.

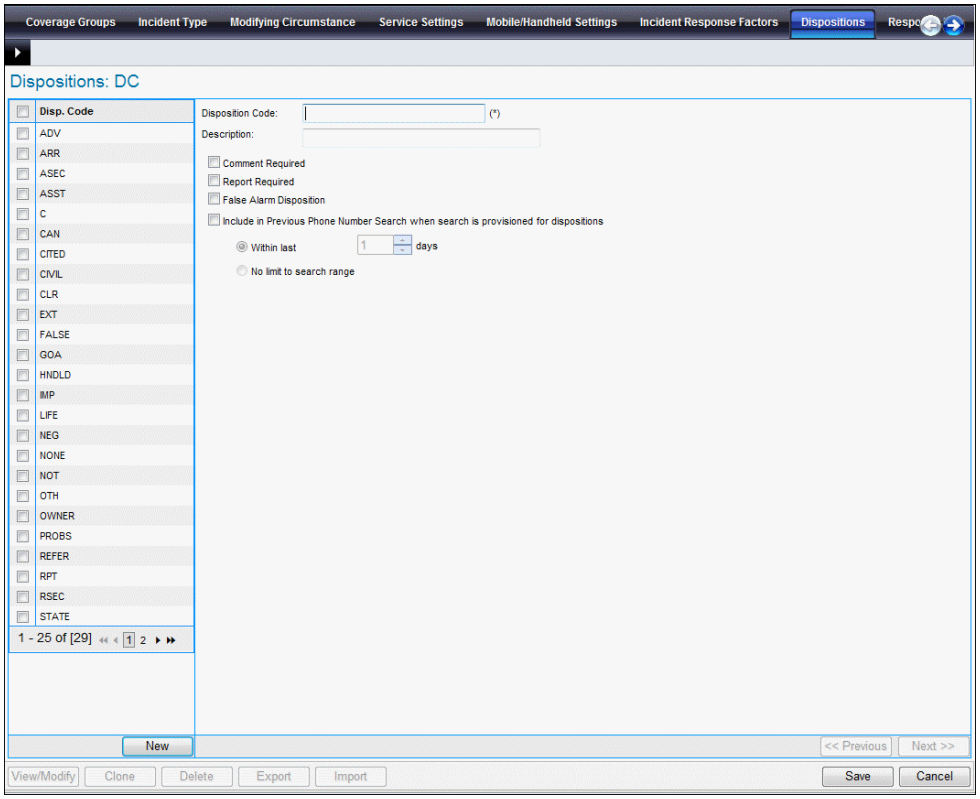


Figure 13-19 Disposition Settings Form

2. At the bottom of the Disposition Codes list, click the **New** button.
3. In the Disposition Code field, type your new code.
4. In the Description field, type a description for your new code.

   Do any of the following:

   - To require comments to be entered when the disposition is used, select the **Comment Required** check box.
   - To flag the incident with this disposition as needing the primary unit to fill out a report, select the **Report Required** check box. A report can then be run to retrieve a list of all incidents needing a report.
   - To create a false alarm incident, select the **False Alarm Disposition** check box. The incident will be counted as a false alarm at the location.
   - To include incidents with this disposition in Previous Phone Number searches, select the **Include in Previous Phone Number Search when search is provisioned for dispositions** check box. Then select the time period to use in the Search range.

For information on enabling Previous Phone Number searches, see "Configuring Search Defaults" on page 13-23.

5. Repeat the procedure for any other dispositions.

   Each unsaved disposition appears in the Disposition Code list in blue text.

6. Click **Save**.

Configuring Response Messages

Use the Incident Management Response Messages configuration item to define messages indicating a circumstances has occurred in a specific geographic location. Response messages can also be sent for specific incident types and alarms. Response messages are attached to incidents as comments when incidents are initiated.

Common examples of response messages include the following:

- Message identifying the beat as a gang prone area
- Message indicating an incident was not responded to due to Chronic Alarm Violator Status
- Message identifying an area as containing known drug labs
- Message indicating repairs are being done to a street
- Message indicating to always send back up for the incident type
- Message indicating an alarm was triggered

You can add, modify, clone, and delete response messages. For details on deleting and cloning response messages, see "Working With Configuration Items" on page 2-9.

NOTE
You can configure response messages to display with comments or separate from comments. For details, see "Configuring CAD WAA Settings" on page 17-1.

When you add response messages, you enter information on four tabs:

- Message – Where you enter the subject and text of the message.
- Areas/Sect/Beat – Where you select the areas, sectors, and beats to which the message will apply so that if an incident is initiated in that area, sector, or beat, the message is attached to the incident as a comment.

- Locations – Where you add locations to which the message will apply so that if an incident is initiated at that location, the message is attached to the incident as a comment.
- Incident Types – Where you select specific incident types to which the message will apply so that if an incident of that incident type is initiated, the message is attached to the incident as a comment.

If there are multiple criteria, a response message is sent when any of the criteria occur.

Adding Response Message Subject and Text Settings

The Message tab includes the response message subject and the text of the message.

To add response message subject and text settings:

1. From the navigation panel, select **Incident Management**, and then select **Response Message**.

   The Response Message Settings form appears with the Message tab in focus. A list of existing response messages displays on the left side of the form.

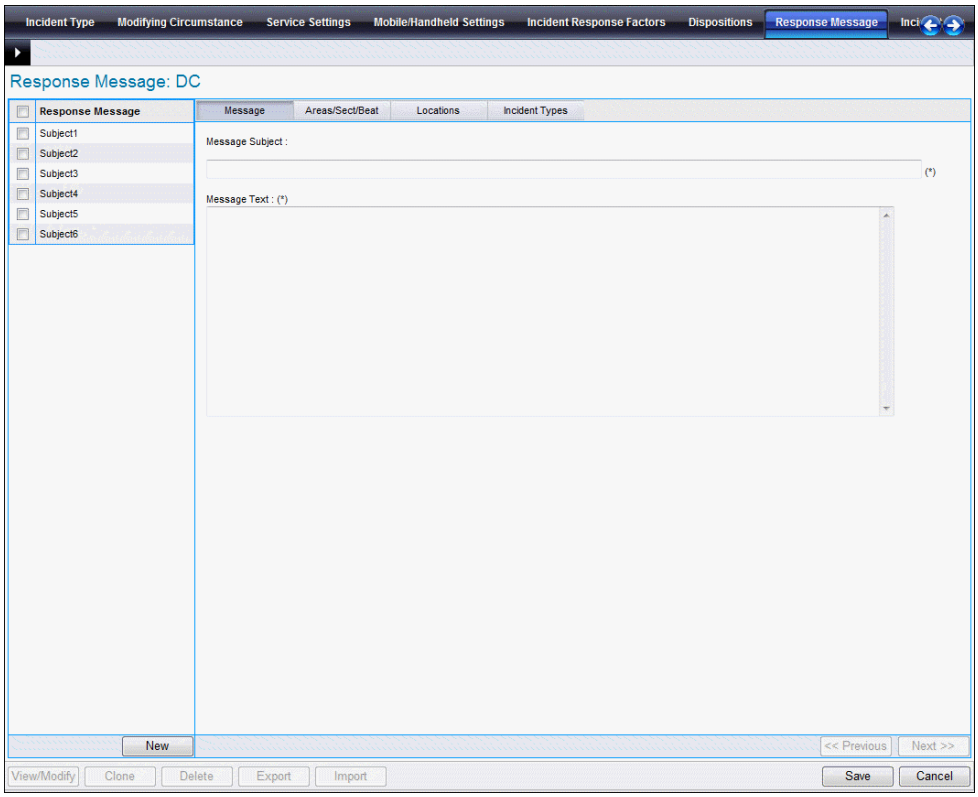


Figure 13-20 Response Message Settings Form – Message Tab

2. At the bottom of the Response Messages list, click the **New** button.

3. In the Message Subject field, type the subject of your message, similar to the subject of an email.

4. In the Message Text field, type the text of the message.

Adding Response Message Area, Sector, and Beat Settings

Add area, sector, or beat settings when you want a response message to be attached to an incident that occurs in that area, sector, or beat.

To add response message area, sector, and beat settings:

1. Access the form for new response messages. For instructions, see "Adding Response Message Subject and Text Settings" on page 13-46.

   The Response Message Settings form appears with the Message tab in focus (see Figure 13-20). A list of existing response messages displays on the left side of the form.

2. In the Response Message Settings form, select the Area/Sect/Beat tab.

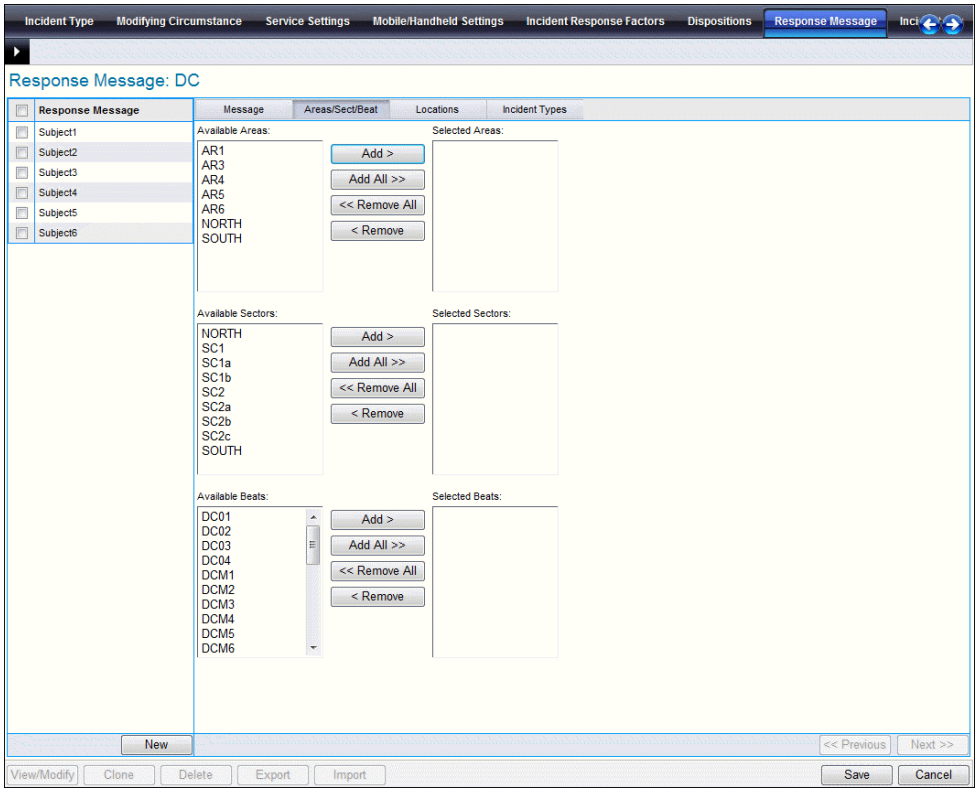


Figure 13-21 Response Message Settings Form – Areas/Sect/Beat Tab

3. In the Areas section, select the area(s) you want to associate with a message.

4. In the Sectors section, select the sector(s) you want to associate with a message.

5. In the Beats section, select the beat(s) you want to associate with a message.

6. Click **Save**.

Adding Response Message Locations Settings

Add location settings when you want a response message to be attached to an incident that occurs at that location.

To add location settings:

1. Access the form for new response messages. For instructions, see "Adding Response Message Subject and Text Settings" on page 13-46.

   The Response Message Settings form appears with the Message tab in focus (see Figure 13-20). A list of existing response messages displays on the left side of the form.

2. Select the Locations tab.

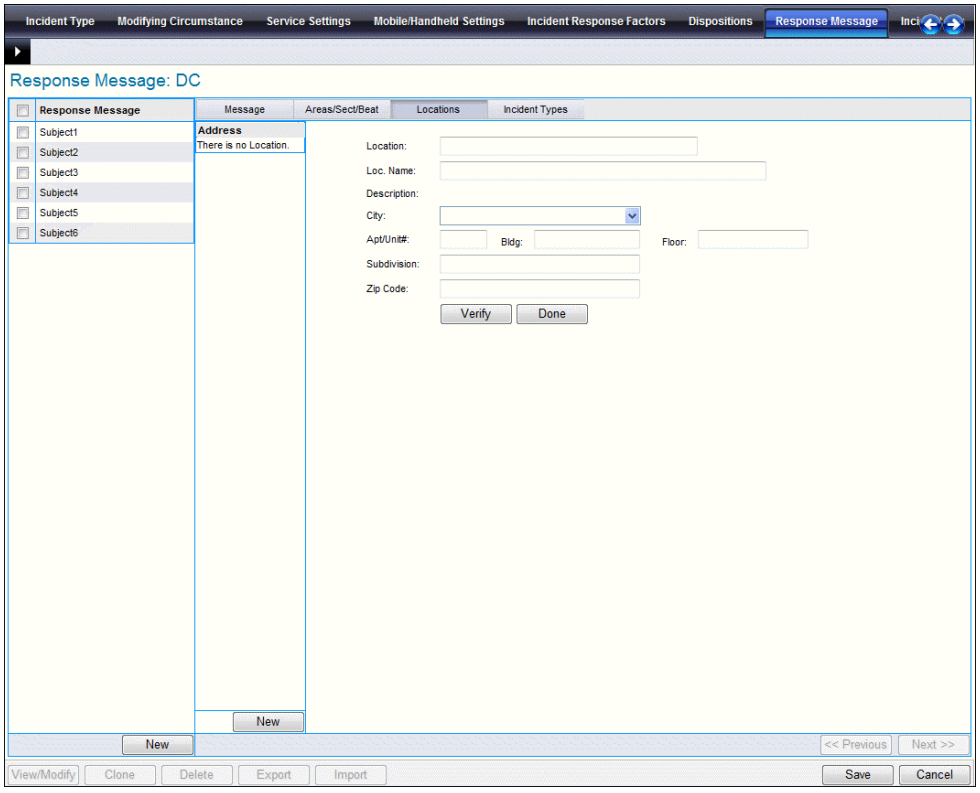


Figure 13-22 Response Message Settings Form – Locations Tab

3. Enter information in the Location fields.

4. Click **Verify** to use address verification.

5. Click **Done**.
6. Repeat the procedure to add any other locations.
7. Click **Save**.

Adding Response Message Incident Types Settings

Add incident type settings when you want a response message to be attached to an incident with that incident type.

To add response message incident types settings:

1. Access the form for new response messages. For instructions, see "Adding Response Message Subject and Text Settings" on page 13-46.

   The Response Message Settings form appears with the Message tab in focus (see Figure 13-20). A list of existing response messages displays on the left side of the form.

2. Select the Incident Types tab.

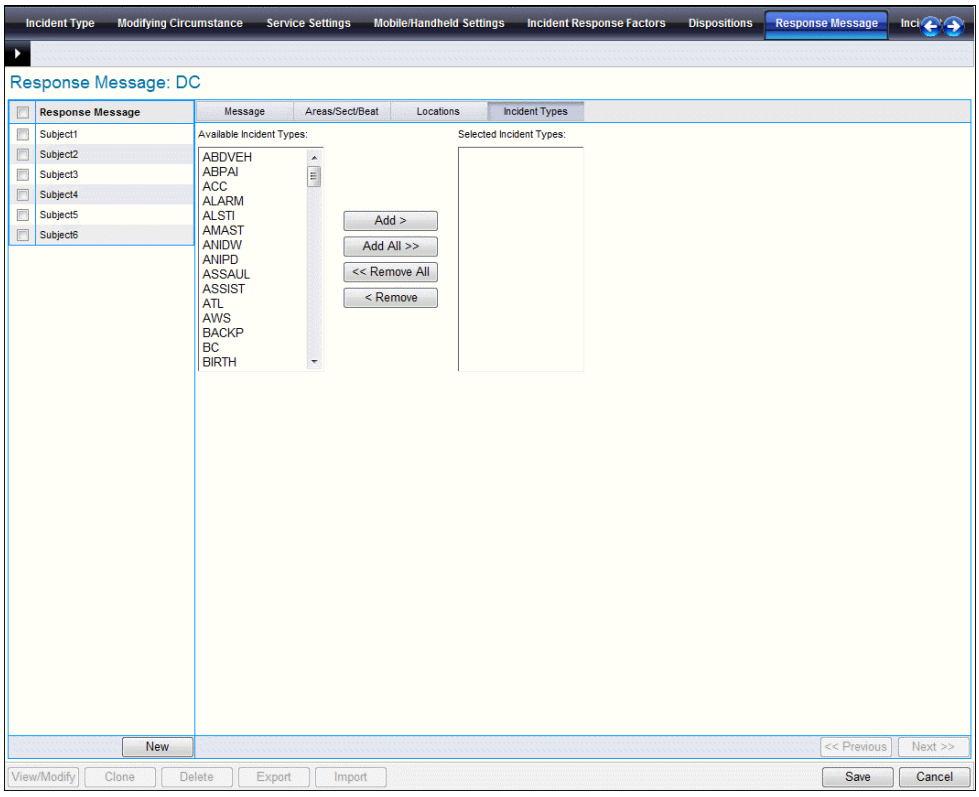


Figure 13-23 Response Message Settings Form – Incident Types Tab

3. From the Available Incident Types box, select the incident type or types that you want to associate with this response message. To select more than one incident type, select the first incident type, and then press the **Ctrl** key while selecting additional incident types.

4. Click **Add**.

   Alternatively, click **Add all** to associate all incident types with this response message.

5. Repeat the procedure for any other response messages.

   Each unsaved response message appears in the Response Message list in blue text.

6. Click **Save**.

Configuring Incident Source Codes

Use the Incident Management Source Code configuration item to manage the codes that identify the sources of emergency calls, such as 9-1-1 or an alarm interface.

NOTE
Incident source codes are specific to each agency type, such as law, fire, or medical.

You can add, modify, clone, and delete source codes. For details on cloning and deleting source codes, see "Working With Configuration Items" on page 2-9.

Adding Incident Source Codes

When you add new incident source codes, you enter the source code name and description on the Code List tab of the Incident Management – Incident Source Code form.

The Set Defaults tab is where you select code names for the six default incident source codes: 9-1-1 initiated, phone initiated, field initiated, mobile initiated, alarm initiated, and schedule initiated.

When you add a source code, you enter the new code and its description. You cannot change the Source Code name. If you want to change the name, you must delete and re-add the record.

To add a source code:

1. From the Navigation panel, select **Incident Management**, and then select **Incident Source Code**.

   The Incident Source Code form appears with the Code List tab in focus. A list of existing incident source codes displays on the left side of the form.

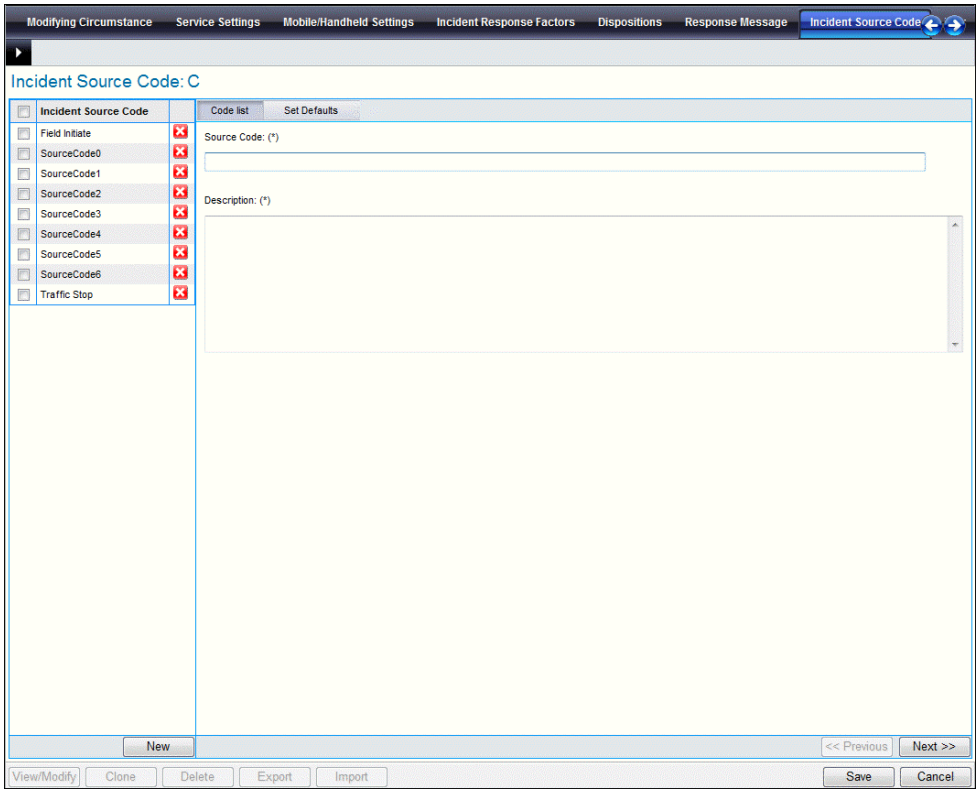


Figure 13-24 Incident Source Code Form – Code List Tab

2. At the bottom of the Incident Source Code list, click the **New** button.

3. In the Source Code field, type the new code.

4. In the Description field, type a description for the new code.

   Make sure you set up a code for each of the default sources listed on the Set Defaults tab. For more information, see “Setting the Default Source Codes” on page 13-52.

5. Repeat the procedure for any other incident source codes.

   Each unsaved incident source code appears in the Incident Source Code list in blue text.

6. Click **Save**.

   The new incident source codes appear in the list in black text.

Setting the Default Source Codes

There are six default sources for which you need to set codes: 9-1-1 initiated, phone initiated, field initiated, mobile initiated, alarm initiated, and schedule initiated.

You must always have a code for each of these default sources. They cannot be deleted.

To set the default source codes:

1. Access the form for new incident source codes. For instructions, see "Adding Incident Source Codes" on page 13-50.

   The Incident Source Code form appears with the Code List tab in focus (see Figure 13-24). A list of existing incident source codes displays on the left side of the form.

2. In the Incident Source Code form, select the Set Defaults tab.

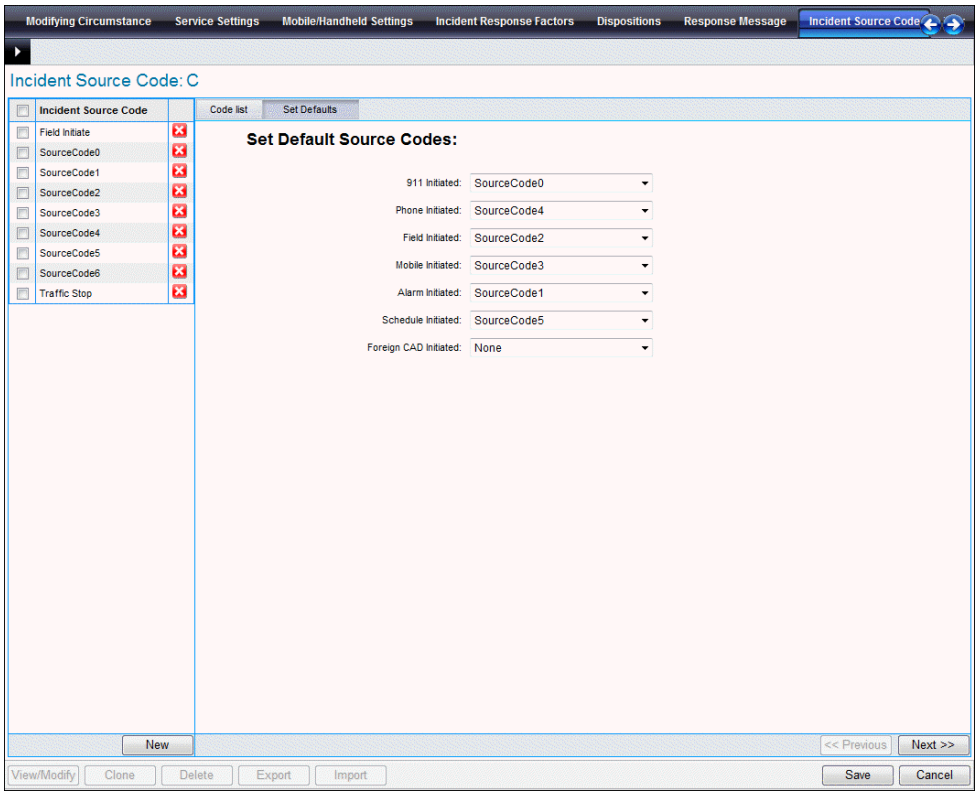


Figure 13-25 Incident Source Code Form – Set Defaults Tab

3. For each of the default sources, select a code that you have already created. For more information, see "Adding Incident Source Codes" on page 13-50.

4. Click **Save**.

Configuring Premise/Hazard Types and Records

Use the Incident Management Premise Hazard configuration item to manage hazard and premise types and records. Premise/Hazard type information consists of the agency type, agency combination, premise hazard code, proximities for searching, and incident address display order. Premise/Hazard record information consists of the information for a specific location.

NOTE

You can provision Premise/Hazard types and records at the agency or agency-type level.

You can configure, modify, clone, export, import, and delete premise/hazard types and records. For details on modifying, cloning, exporting, importing, and deleting, see "Working With Configuration Items" on page 2-9.

Configuring Premise/Hazard Types and Proximities

Premise/hazard codes and proximities information include the inner and outer default proximity for the agency and the individual premise/hazard code names, descriptions, and inner and outer proximities.

To configure premise/hazard codes and proximities:

1. From the navigation panel, select **Incident Management**, and then select **Premise/ Hazard**.

The Premise Hazard form appears with the Types & Proximities tab in focus.

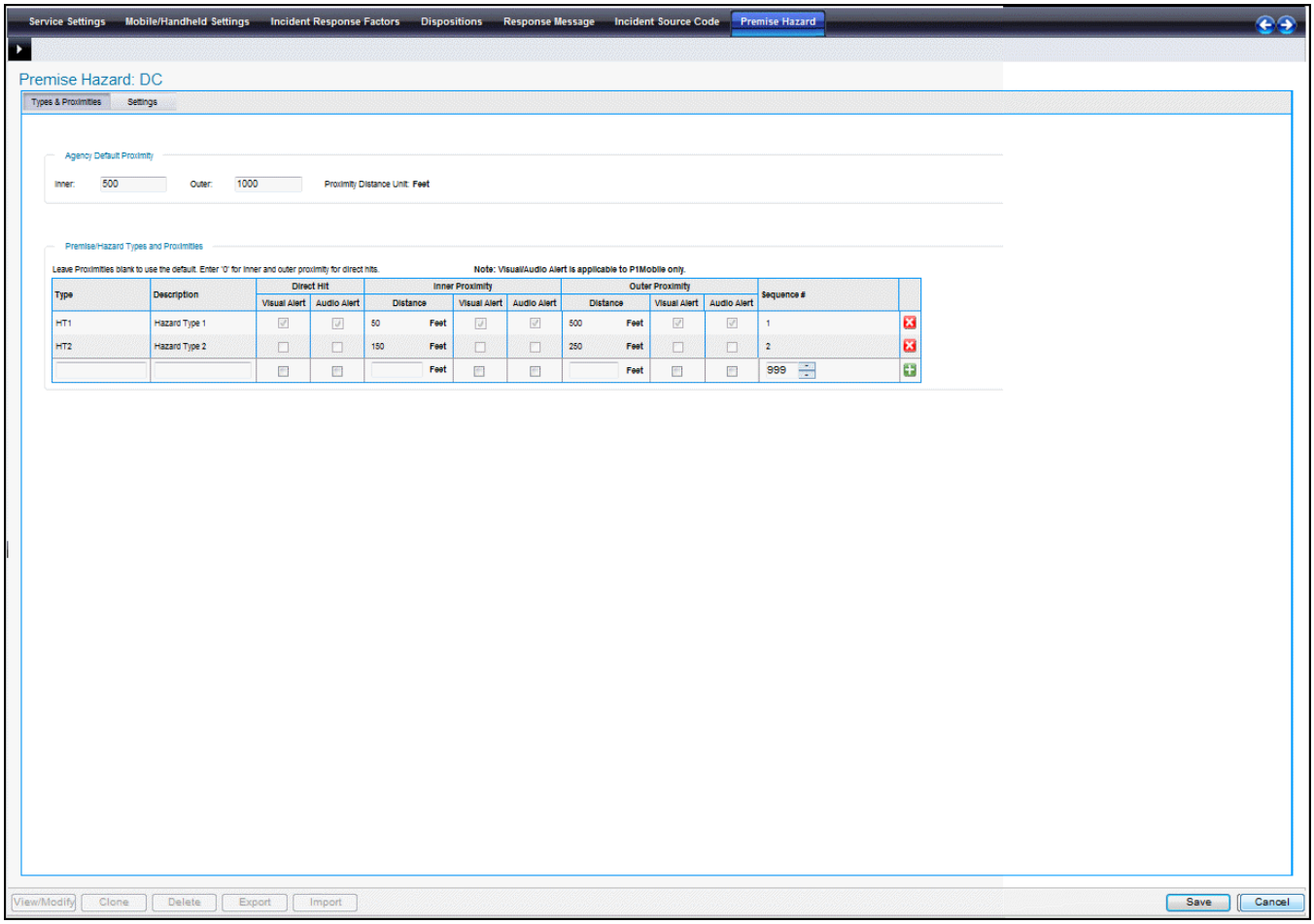


Figure 13-26 Premise Hazard Types Form – Types & Proximities Tab

2. Click **View/Modify**.

   You can now edit the fields in the form.

3. In the Agency Default Proximity section, type a value for the Inner and for the Outer fields.

   Inner proximity is an inner circle within which notification of the premise hazard information is made. For example, in a chemical explosion, all people within the inner proximity would be evacuated.

   Outer proximity is a circle of a larger dimension. The people living between the inner and outer proximity would have a different type of notification. For example, in a chemical explosion, only people with respiratory problems would be evacuated.

   For direct hits only, which are exact address matches, type a zero (0) in each proximity field.

4. In the Premise/Hazard Types and Proximities section, enter your new Type, Description, Direct Hit, Inner and Outer Proximity, and Sequence number information in the table columns.

   a. In the Type column, enter the code for the Premise Hazard type.

   b. In the Description column, enter a description for the code.

   c. Alerts

   NOTE
   Alerts apply only to PremierOne Mobile.

   In the Direct Hits, Inner Proximity, or Outer Proximity column, indicate whether you want a Visual Alert, an Audio Alert, or both. If you have a direct hit, the inner and outer proximities have not effect. If you have a hit in an inner proximity, the outer proximity has no effect.

   For the Inner Proximity and Outer Proximity columns, the hit must fall within the specified distance for that proximity. This is a radius with the incident as the center point.

   d. In the Sequence # column, specify a sort order sequence number for the new premise hazard type, or leave the default value of 999.

   The sequence number determines the sort order in which premise/hazard types are displayed on the CAD and Mobile client forms that display premise/hazard records for a particular location. For the CAD client, these include the Incident Initiation, Incident Management, Location Detail, and the Premise Hazard Search forms, and for the Mobile client, the Incident Summary Premise Hazard tab and the Incident Summary (Traffic Stop) Premise Hazard tab.

   Accepting the default value of 999 places the premise/hazard type at the bottom of the sorted list. If multiple premise/hazard types have the same sequence number, they are sorted alphabetically.

   You can use any sequence number between 1 and 999 to control sort order. For example, you can use sequence numbers of 10, 20, 30, and so on, to allow for future insertions in the sort order.

   The sort order can be further controlled by specifying an agency sort order. For details, see “Configuring Premise/Hazard Settings” on page 13-56.

5. Click the plus symbol to the right of the row to save the code and proximity information and to add a new line.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the code information, even after you click Save.

6. Click **Save**.

Configuring Premise/Hazard Settings

Premise/hazard settings include log settings and the incident address display order.

To configure premise/hazard records:

1. Access the form for configuring premise/hazard types. For instructions, see "Configuring Premise/Hazard Types and Proximities" on page 13-53.

   The Premise Hazard form appears with the Types & Proximities tab in focus (see Figure 13-26).

2. In the Premise Hazard form, select the Settings tab.

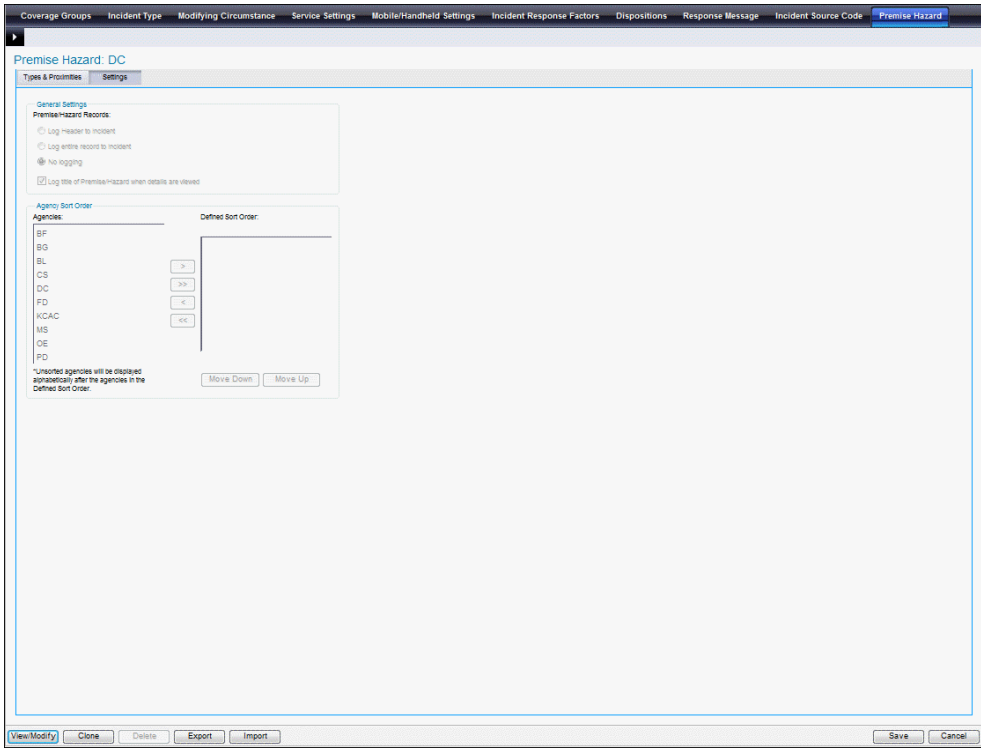


Figure 13-27 Premise Hazard Form – Settings Tab

3. In the General Settings section, select the premise/hazard information that you want to log to incidents when the record is viewed.

   - To log header information regarding the premise/hazard to an incident, select the **Log Header to Incident** button.
   - To log the entire premise/hazard record to an incident, select the **Log entire record to incident** button.
   - If you do not want any premise/hazard information logged to an incident, select **No logging.**
   - To log the title of a premise hazard record when the record is viewed, select the **Log title of Premise/Hazard when details are viewed** check box.

4. In the Agency Sort Order section, specify the default sort order in which trusted agencies' premise hazard records are displayed in the CAD and Mobile clients. Use the arrow buttons to move trusted agencies from the Agencies panel to the Defined Sort Order panel. Use the Move Down and Move Up buttons to reorder them.

   Premise/hazard records for agencies that are not moved to the Defined Sort Order panel are displayed alphabetically following the records for agencies in the Defined Sort Order.

5. Click **Save**.

Premise/Hazard Sort Order Rules

Premise Hazard Types, Settings, and Sort Order are defined in Provisioning under the Incident Management – Premise/Hazard item. When multiple locations are displayed within the Premise/Hazard Search Form, the records are first sorted by *Location* and *City* before applying the following Premise/Hazard Sort Order Rules:

1. The Proximity value for the corresponding Premise/Hazard record in ascending order.

   All Direct Hit records will appear first, followed by Inner Proximity records, and then by Outer Proximity records.

2. The Sort Order Sequence Number provisioned against the Premise/Hazard Type for the corresponding Premise/Hazard record in ascending order.

   All Premise/Hazard records with a Sort Order Sequence Number of 1 will appear first, followed sequentially by the next number in the sequence until Sort Order Sequence Number 999.

3. The Agency ID that owns the Premise/Hazard Type for the corresponding Premise/Hazard record based on the Agency Sort Order provisioned for the user's owning agency in their defined order.

   a. The agencies will be displayed in the provisioned Defined Sort Order.

   b. All agencies that are not included within the Defined Sort Order will be displayed alphabetically immediately after the agencies in the Defined Sort Order.

4. The Premise/Hazard Type assigned to the corresponding Premise/Hazard record in alphabetical order – when more than one Premise/Hazard Type has the same Sort Order Sequence Number within an agency.

5. The approximate distance between the Premise/Hazard record's location and the specified location in ascending order – when more than one Premise/Hazard Record exists within the same Premise/Hazard Type. This actually only applies to Inner and Outer Proximity records, since the approximate distance for Direct Hit records would be zero.

6. The Premise/Hazard Record Title in alphabetical order for Direct Hit records– when more than one Premise/Hazard Record exists for the same approximate distance value within the same Premise/Hazard Type.

Configuring Premise Hazard Records

Premise Hazard records have unique or special information regarding a specific location that could be useful to the officer responding to an incident at the location. Examples include gate codes, special entry information, VIP contact and protocol information, presence of toxic chemicals, or known drug dealers.

You configure individual premise hazard records by setting the following: Premise Hazard type, whether it is permanent or temporary, record title, address information, authorizing personnel, attachment information, purge date and time, owner and contact information, and any comments.

You can define or modify a premise hazard record using either a point location or a premise hazard area.

NOTE
If an update occurs to the GIS database that affects a premise hazard address, you must manually update the location.

You can add, create, modify, clone, delete, import, and export premise hazard records. For details on cloning modifying, deleting, importing, and exporting premise/hazard records, see "Working With Configuration Items" on page 2-9.

Adding Premise/Hazard Records

Add a premise/hazard record when you learn of a new hazard in the area covered by your agency or when you learn of new premise information about which your officers need to be aware, such as a new school, or the home of an ambassador.

To edit premise/hazard records, follow the same procedures as adding the records.

To add a premise/hazard record:

1. From the navigation panel, select **Incident Management**.
2. Select **Premise/Hazard**, and then select **Premise/Hazard Record**.

   The Premise Hazard Records form appears. A list of existing record titles displays on the left side of the form.

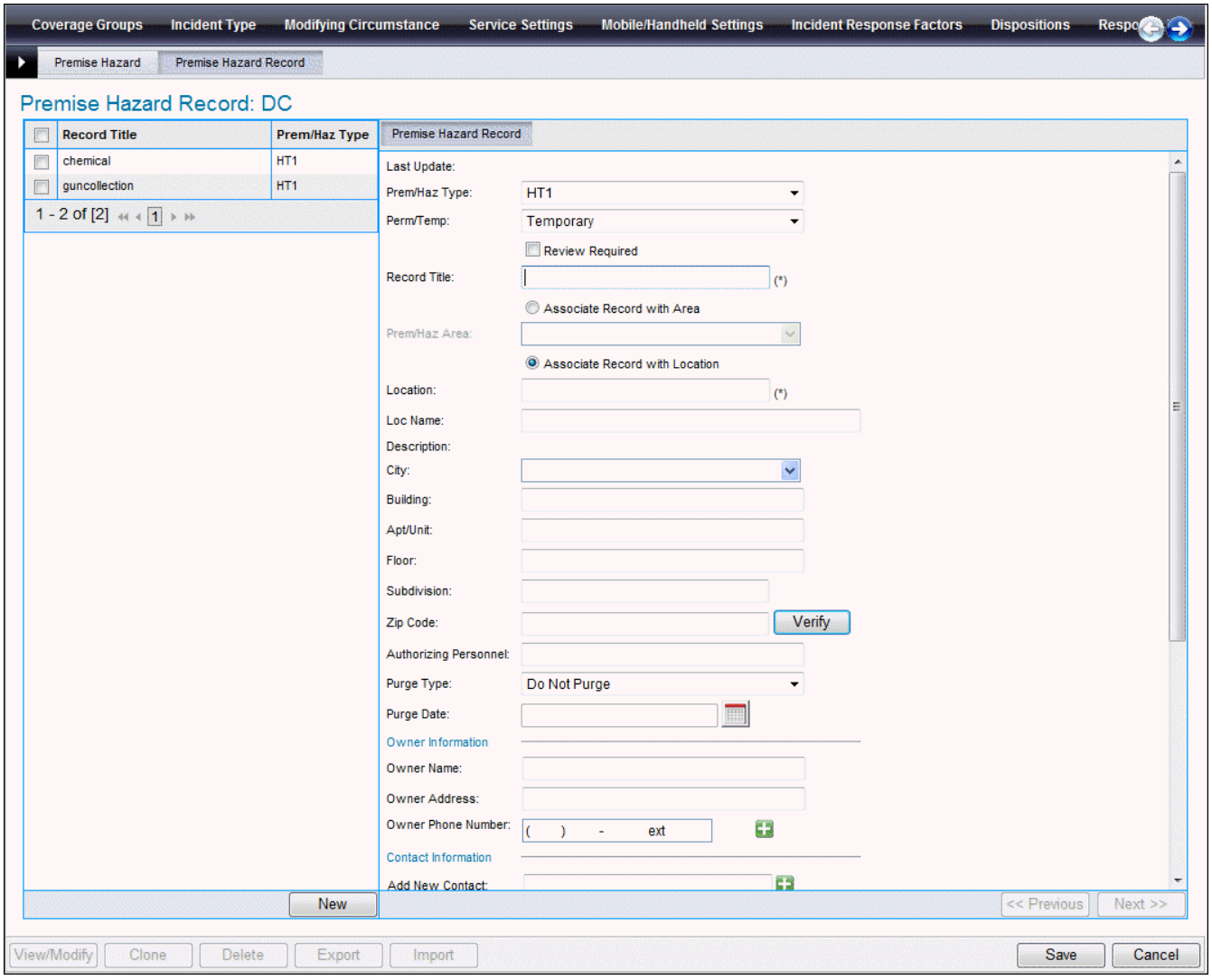


Figure 13-28 Premise Hazard Records Form

3. At the bottom of the Record Title list, click the **New** button.
4. From the Premise Hazard Type list, select a premise/hazard type or code. The options for this field are defined in the Premise/Hazard Codes and Proximities section of the Premise Hazard form.

For more information, see “Configuring Premise/Hazard Types and Proximities” on page 13-53.

NOTE

When a record is updated the following information displays: agency ID, user ID, last name, and first name of the user making the change, and date and time the record was updated.

5. From the Perm/Temp list, select whether you want this record to be permanent or temporary.

6. To require the record to be reviewed, select the **Review Required** check box.

   Premise/hazards records can be filtered by those that require review. Temporary records have **Review Required** checked automatically.

7. In the Record Title field, type a descriptive title for this premise hazard record.

   Titles do not have to be unique.

8. Do one of the following:

   Select **Associate record with area** if the premise/hazard is an area, and not a specific address. From the Premise Hazard Area list, select an area name.

   A Premise/hazard area is not a single location; it defines a geographic area as part of a GIS layer. An example is a gate code for an incident that has occurred within a gated community. The area can be modified, cloned, imported, and exported just as point locations can.

   - Select **Associate record with location** (default). This is an specific address for the premise/hazard location. Then complete the address fields to complete the record.

9. In the Address fields, type as much information as you have for the location of the premise or hazard information.

   Click **Verify** to verify the address.

   The location name will appear in the Loc Name field after you enter the street address, if the information is available.

Because titles do not have to be unique, location information is critical for differentiating one record from another during a search.

NOTE

The Location fields for existing records remain enabled. When GIS data is updated, the coordinates for an address may change. The GIS data change could cause the Lat/Long of an address to change, which in turn would no longer match the coordinates of existing Premise/Hazard records. This results in previous **Direct Hit** matches becoming **Proximity Hits**.

Street names might also be updated; for example BYERS RD might have been incorrectly entered as BYERS DR within GIS. Correcting this street name in GIS would cause the existing Premise/Hazard record to become unusable.

10. In the Authorizing Personnel field, type the name of the person who authorized the premise/hazard record.

11. From the Purge Type list, select the purge method:

    - To keep the record indefinitely, select **Do not purge**. You can change the purge type at a later time.
    - To purge the record on a specific date, select **Automatically** and then enter the purge date in the Purge Date field.
    - To purge the record manually, select **Purge Manually**.

12. In the Purge Date field, select or type the date you want to purge this record.

13. In the Owner Information fields, type the name, address, and phone number of the property owner.

    In the Owner Phone Number field, you can use any combination of 3-digit area code, 7-digit phone number, and/or 1-4 digit extension. If you are entering an international number, start with a + symbol, enter the country code, and then the rest of the phone number information. Entering the + symbol causes the area code/phone number/extension formatting to be removed.

    Click the plus symbol to the right of the Owner Phone Number field to save the owner information and to add additional phone numbers.

14. In the Contact Information section, you can use the address book to add ready reference information by clicking the Add Another Contact link. You can also add another contact name *and* phone number. After you type the name, click the plus symbol to the right of the Contact Name field. A field for the phone number appears.

    After you type the phone number in the Contact Phone Number field, click the plus symbol to the right of the Add New Contact field to save the contact information.

15. In the Comments field, type any comments about this premise/hazard record.

16. To add an attachment, such as a floor plan:

a. In the Attachment Name field, click **Browse** to navigate to the attachment.

b. Locate the record, and then click **Open**.

c. In the Attachment Description field, type a brief description of the attachment.

d. Click the plus symbol to the right of the Attachment Name field to save the attachment information and add another set of attachment fields.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the attachment information, even after you click Save.

17. Repeat the procedure for any other premise/hazard records you want to add.

    Each unsaved record appears in the Record title list on the left in blue text.

18. Click **Save**.

    The premise/hazard records you added appear in the Record Title list on the left in black text.

CHAPTER 14

Configuring Unit Recommendations

The Unit Recommendation configuration item contains the following items:

- Response Cards – Where you define the set of required resources that are needed by an agency for a particular situation. For details, see “Configuring Response Cards” on page 14-2.
- Response Category – Where you group similar unit capabilities together. Grouping capabilities together makes reviewing and maintaining a unit’s capabilities much more effective. For details, see “Configuring Response Categories” on page 14-36.
- Response Class – Where you can alter the standard unit recommendation made to a specific *location*. You can provision a response class for a specific address, an intersection, a street house number range, a common place, or a beat. Response classes are permanent adjustments. Response classes are referenced in run cards. For details, see “Configuring Response Classes” on page 14-13.
- Response Descriptor – Where you can manually alter the run card response while requesting recommendations. Response descriptors are referenced in run cards. For details, see “Configuring Response Descriptors” on page 14-17.
- Response ID – Where you can group Incident Response Factors (IRFs) by common response requirements. By grouping IRFs that have the same response requirements, your agency only has to provision the single response ID to get the same recommendations for all of the IRFs in the group. Response IDs are referenced in run cards. For details, see “Configuring Response IDs” on page 14-15.
- Response Mode – Where you can temporarily alter the standard unit recommendations made to a specified set of beats. This can be due to an unavoidable but definable situation such as a flood or a high winds. Response modes are removed when the situation no longer exists. Response modes are referenced in run cards. For details, see “Configuring Response Modes” on page 14-11.
- Run Card – Where you can define a set of fixed conditions that help identify the most appropriate units to dispatch to an incident with a specific jurisdiction. Run cards define where and in what order PremierOne looks to find units to dispatch. You can provision a different run card for each capability. For details, see “Configuring Run Cards” on page 14-19.

- Settings – Where you set how logging is done, sort order for capabilities, sort order of duty types, sort order of response categories, and maximum driving speed for vehicle types. For details, see "Configuring Unit Recommendations Settings" on page 14-27.

PremierOne recommends specific units automatically based on the incident's IRF, the units' availability, the units' location, and other factors. By using response modes, response classes, response IDs, response descriptors, run cards, and response categories you can alter the automatic recommendation.

Configuring Response Cards

Use the Response Card configuration item to view and administer response cards.

Response cards are used by an agency to define the set of required resources that are needed for a particular situation. In most cases, the required resources are the same throughout an agency's jurisdiction.

Examples:

A shooting at a public school requires a different response than a shooting at a residence.

A reported shoplifting incident requires a one-man police response.

Other factors or special conditions may also alter the normal responses. You can provision those conditions as part of a response card.

Adding Incident Response Factors to Response Cards

When you provision response cards, you enter information on one of two main tabs:

- Incident Response Factors
- Response ID

Each main tab has two subtabs:

- General – Where you indicate the response card name, set the incident response factors or the response ID, geographical level, day/time information, and subsequent dispatch options.
- Response – Where you indicate the initial and secondary capabilities, whether the capability is required, minimum number of personnel, quantity of personnel to recommend, response descriptor, how to search, how many additional units to obtain, whether to include ARL recommendations, and the order of the selected capabilities.

The general information and response requirements are the same whether you are provisioning response cards for IRFs or for response IDs.

Adding Response Cards for IRFs or Response IDs – General Subtab

Add a response card when the response cards you have do not meet your needs. Entering the information for the General and Response tabs is the same whether you are provisioning response cards for incident response factors (IRF) or response IDs.

To add general settings for a response card for IRFs or response IDs:

1. From the navigation panel, select **Unit Recommendation**, and then select **Response Card**.

The Incident Response Factor form appears with the General tab in focus.

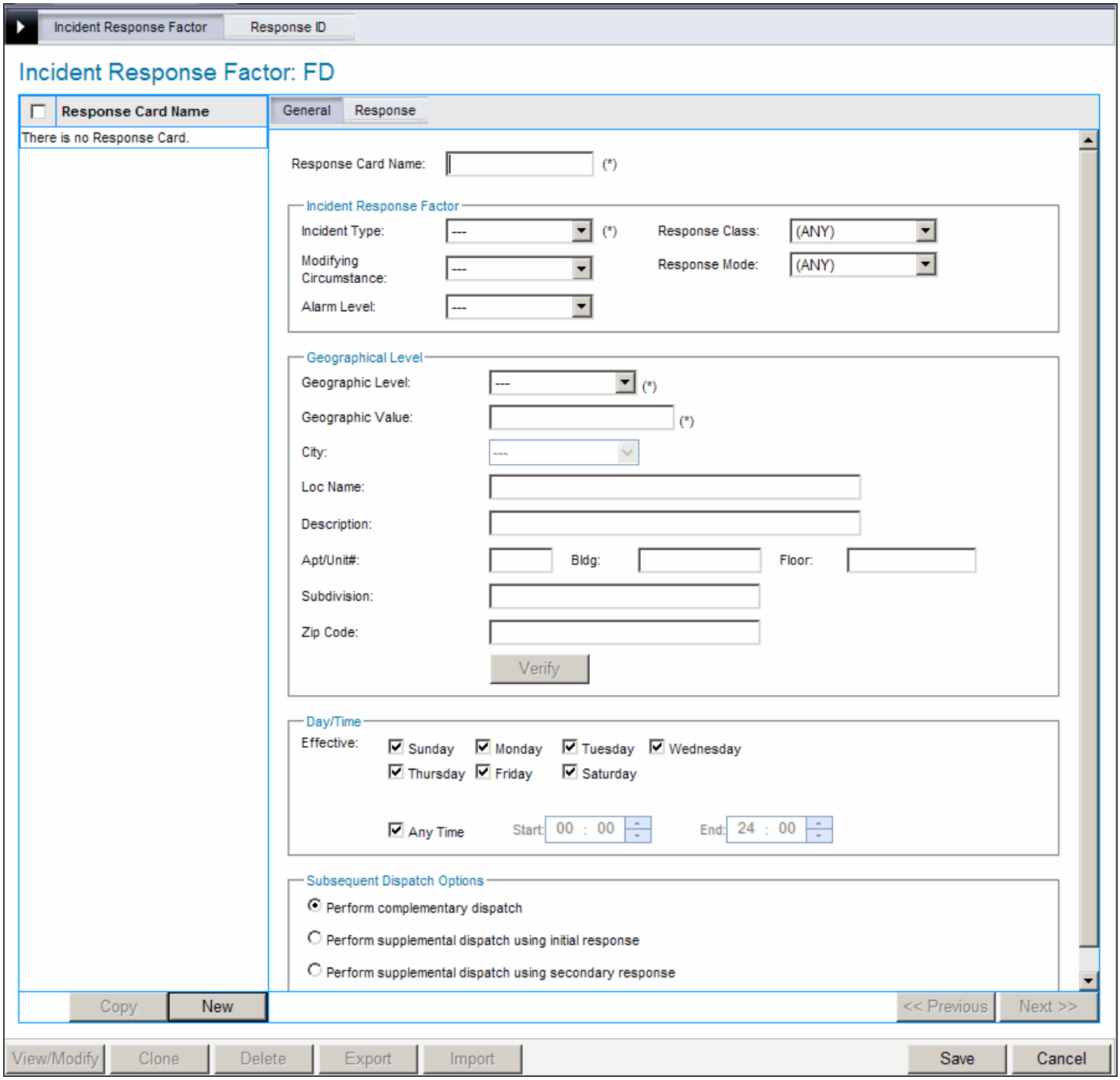


Figure 14-1 Unit Recommendations – Response Card – IRF Tab, General Subtab

2. From the General tab, click **New** at the bottom of the Response Card Name list.

   The Incident Response Factor form appears with the General tab in focus.

3. On the General tab, in the Response Card Name field, type a name for the new response card.

The name must be unique within your agency and can be up to 20 alphanumeric characters.

4. In the Incident Response Factor or the Response ID section, set your preferred values for your response card.

   At minimum, you must supply an IRF (incident type, modifying circumstance, and alarm level) for the Incident Response Factor section or a Response ID for the Response ID section.

5. In the Geographical Level section, select a value for the Geographic Level.

   - If you select **Agency**, PremierOne sets the Geographic Value to the provisioning agency. No other agency value is allowed.
   - If you select **Area**, you can select any valid area across all provisioned active and inactive plans for the Geographic Value field.
   - If you select **Beat**, you can select any valid beat for your provisioned agency for the Geographic Value field.
   - If you select **Location**, you can select any valid GIS location for the Geographic Value field, and select the City. If the location you select is a common place, PremierOne displays the common place name in the Location Name field.
   - If you select Sector, you can select any valid sector across all provisioned active and inactive plans for the Geographic Value field.

6. In the Day/Time section, do the following:

   - Select the day or days of the week that this response card will be effective.
   - Select **Any Time** or select a start and end time that the response card will be effective.

     Example:

     Any Time includes all undefined times. For example, you already have response cards set up for 7:00 AM to 8:00 AM and for 2:00 PM to 3:00 PM for a school zone. You could now set one up for **Any Time** which would cover all other times of the day and night.

7. In the Subsequent Dispatch Options section, select one of the following options for dispatching additional units after units are already assigned to the incident:

   - **Perform complementary dispatch** (default) to compare working capabilities of the units already assigned to the incident against the response card requirements and only recommend what is missing from the incident.
   - **Perform supplemental dispatch using initial response** to always recommend the full set of provisioned response requirements, regardless of the units that are currently assigned to the incident. This recommendation matches the initial response.

- **Perform supplemental dispatch using secondary response** to recommend a secondary response that is different than the initial response as defined by the response card.

  Example:

  A police agency is involved in an incident with an IRF of Death Investigation. The initial response requires one patrol unit and 1 supervisor. The supervisor is no longer needed and leaves the scene. The patrol unit requests a backup unit. In this case, another patrol unit can be sent; the supervisor is no longer required. Therefore, the supplemental dispatch has different response requirements than the initial dispatch.

  When you select **Perform supplemental dispatch using secondary response**, the Secondary sub-subtab becomes active on the Response tab.

Adding Response Cards for IRFs or Response IDs – Response Subtab

Add a response card for Incident Response IDs when the response cards you have do not meet your needs. Entering the information for the General and Response tabs is the same whether you are provisioning response cards for incident response factors (IRF) or response IDs.

To add response settings for IRFs or Response IDs:

1. Access the form for response cards. For instructions, see "Adding Incident Response Factors to Response Cards" on page 14-2.

   NOTE

   The Response tab can have one subtab - Initial, or two subtabs - Initial and Secondary. The Secondary subtab is available if you selected **Perform supplemental dispatch using secondary response** in the Subsequent Dispatch Options section on the General tab. The Initial and Secondary tabs contain the same fields.

2. Select the Response tab.

Fields for Response information display.

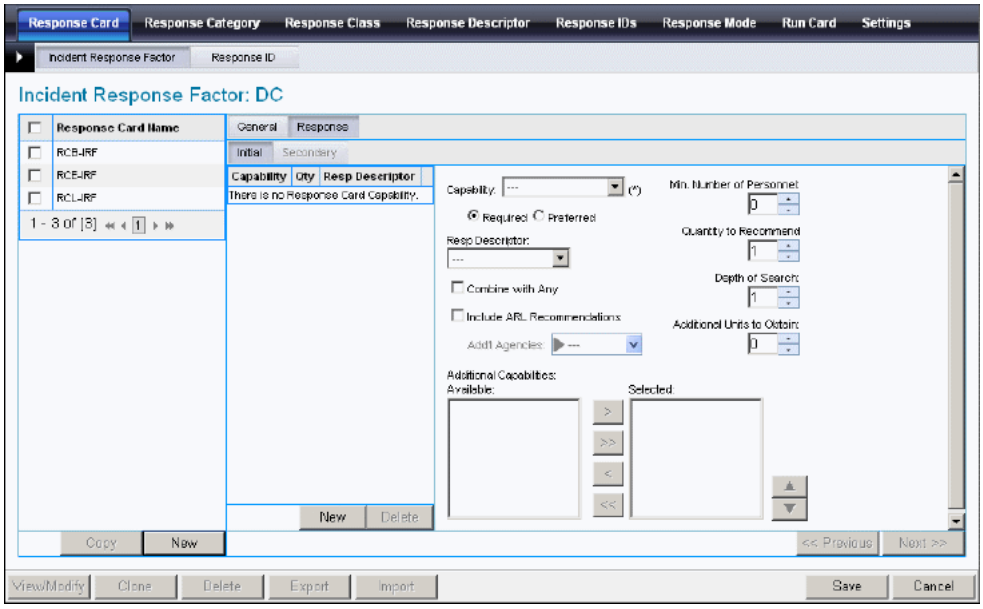


Figure 14-2 Unit Recommendations – Response Card – IRF Tab, Response ID Subtab

3. From the Capability list, select the capability you want to provision for this response card. This will be considered the primary capability if it is on the Initial subtab.

   All other response requirements are based on this value.

4. Set whether the capability is required or preferred.

   A required capability allows you to send one or more additional units if the additional units are closer to the incident.

   Example:

   With a required capability, you can send an additional BLS unit that is close to the incident so it can arrive before your required ALS unit.

   A preferred capability allows you to substitute a different capability if the substitute is closer.

   Example:

   With a preferred capability, you can substitute a BLS unit that is closer to the incident rather than sending the more distant ALS unit.

   If the capability you selected is provisioned as Allow Numeric Entry = Yes, the Required and Preferred options are disabled with the selected option being Required. For more information, see “Configuring Capabilities/Skills” on page 11-4.

   If you change the Capability prior to saving the record, the Required/Preferred option reverts to its default value of Required.

5. In the Min. Number of Personnel field, select the minimum number of people to recommend within the selected capability. A value of 0 means ignore this value.

   Setting the Min. Number of Personnel may result in a greater number of units than you requested.

   Example:

   You requested two engines with a minimum number of personnel of seven. The two engines that are available have only 6 personnel. Therefore, another unit must be recommended to meet the minimum number of personnel requirement.

   If the Capability is provisioned as Allow Numeric Entry = Yes, the Min. Number of Personnel field is disabled and set to 0. For more information, see "Configuring Capabilities/Skills" on page 11-4.

   Within each response card, there is only one Minimum Number of Personnel value that is stored for each unique capability. For example, if a response card has three instances of a capability of Engine, there is only one Minimum Number of Personnel value that is applied to each of these instances.

   If the Capability has been previously defined within the response card, the provisioned value is displayed on duplicate entries of that capability.

   An update to the Minimum Number of Personnel value becomes the new value for all instances of that Capability within the response card.

   If you change the Capability prior to saving the record, the Minimum Number of Personnel value reverts to its default value based on the above rules.

6. In the Quantity to Recommend field, select how many of the capabilities you want to recommend.

   If you change the Capability prior to saving the record, the Quantity value reverts to its default value of 1.

   Example:

   For this type of incident, you must have three units with ALS capability.

7. From the Response Descriptor list, select a response descriptor for this capability.

8. From the Depth of Search list, select a value from 1 to 99.

   When provisioning Preferred/Substitute or Required/Additional response combinations, the Depth of Search field allows you to indicate how deep into the run card order you are willing to search for the primary capability before considering a substitute or additional capability. If the primary capability cannot be found within the value in a run card, then a closer unit with some other capability can be recommended either in place of (Preferred/Substitute), or in addition to (Required/Additional) a unit with the primary capability.

   If the Capability is provisioned as Allow Numeric Entry = Yes, the Depth of search field is disabled and set to 1. For more information, see "Configuring Capabilities/Skills" on page 11-4.

If you change the Capability prior to saving the record, the Depth of Search value reverts to its default value of 1.

9. In the Combine with Any field, select the check box to if this capability can be combined with any of the units already found.

   If you change the Capability prior to saving the record, the Combine with Any value reverts to its default value of No (blank).

   Example:

   You need two engines and you need a diver. Select the check box if the diver can be considered part of the personnel/capabilities of the engine. Do not check the box if the personnel on the engines must be separate from the diver.

10. From the Include ARL Recommendations list, select the check box to include the search for this capability in ARL recommendations.

    Including ARL recommendations provides a secondary, more precise, set of recommendations.

    Example:

    An agency has a response requirement of 10 engines, 5 ladders, and 2 rescue units. The agency can itemize the required resources to enable ARL recommendations for only a portion of the resources, thereby gaining the flexibility of getting some of the critical units onto the scene as quickly as possible, but letting the supporting units arrive based on their standard (fixed) response.

    Table 14-1 Sample Response Requirement

Quantity	Capability	Enable ARL Recommendations
3	Engines	YES
7	Engines	NO
5	Ladders	NO
2	Rescue	YES

    In the table above, the agency elected to find only the closest three engines using ARL, complemented by another seven engines that were obtained from fixed recommendations (for a total of 10 engines). None of the five responding ladder units are to be recommended using ARL, but the two Rescue units should utilize ARL recommendations.

11. From the Additional Units to Obtain list, select a value from 1 to 99.

    If you change the Capability prior to saving the record, the Additional Units to Obtain value reverts to its default value of 0.

    These additional units are not recommended *for dispatch* but are shown in the recommendations. The dispatcher must select the addition units from the list to dispatch them.

If the Capability is provisioned as Allow Numeric Entry = Yes, the Additional Units to Obtain field is disabled and set to 0. For more information, see "Configuring Capabilities/Skills" on page 11-4.

12. In the Additional/Substitute Capabilities area, select secondary capabilities to support the primary capability. If the primary capability cannot be found within a predefined limit (Depth of Search field), then a closer unit with another capability can be recommended either in place of (if you selected Preferred in step 4) or in addition to (if you selected Required in step 4) a unit with the primary capability.

    If you selected **Required** in the Required/Preferred option, the Secondary Capabilities selection is labeled as Additional Capabilities.

    If you selected **Preferred** in the Required/Preferred option, the Secondary Capabilities selection is labeled as Substitute Capabilities.

    You can select capabilities from all capabilities provisioned for your agency with the following exceptions:

    - The capability that you selected as the primary capability.
    - All capabilities that are provisioned as Allow Numeric Entry = Yes.

    If your primary capability is provisioned as Allow Numeric Entry = Yes, the Additional/Substitute Capabilities area is disabled.

    If you change the primary Capability prior to saving the record, the Additional/Substitute Capabilities area reverts to its default value of none being selected.

13. You can add multiple primary capabilities to a single response card by repeating these steps.

Copying Response Cards

Copy a response card when you want to use an existing response card record as the default value for creating a new record. By retrieving an existing response card record and pressing the Copy button, PremierOne behaves as if you pressed the New button, but keeps all of the existing data within the Provisioning form intact with the exception of the Response Card Name field. All fields become editable.

To copy a response card:

1. Access one of the forms for response cards. For instructions, see "Adding Incident Response Factors to Response Cards" on page 14-2.

    The Incident Response Factor form or the Response ID form appears (see Figure 14-1) with the General tab in focus.

2. From the list of existing response cards, select the one you want to copy so it is highlighted, and then click **Copy**. You do not have to select the check box.

3. Make any changes necessary on the General and Response tabs.

4. Click **Save**.

Configuring Response Modes

Use the Response Mode configuration item to view and administer response modes and their descriptions.

Response modes temporarily alter the standard unit recommendations made to a specified set of beats. These conditions can be due to an unavoidable situation such as a flood or a high winds. Response modes are removed when the situation no longer exists.

Response mode codes must be unique within an agency but can be shared among agencies.

You can add, modify, export, import, and delete response modes. For details on modifying, exporting, importing, and deleting response modes, see “Working With Configuration Items” on page 2-9. You cannot change the response mode code name. If you want to change the code name, you must delete and re-add the record.

Adding Response Modes

Use the response mode configuration item to add a response mode. Response modes consist of the code for the response mode and a description.

To add a response mode:

1. From the navigation panel, select **Unit Recommendation**, and then select **Response Mode**.

The Response Mode form appears.

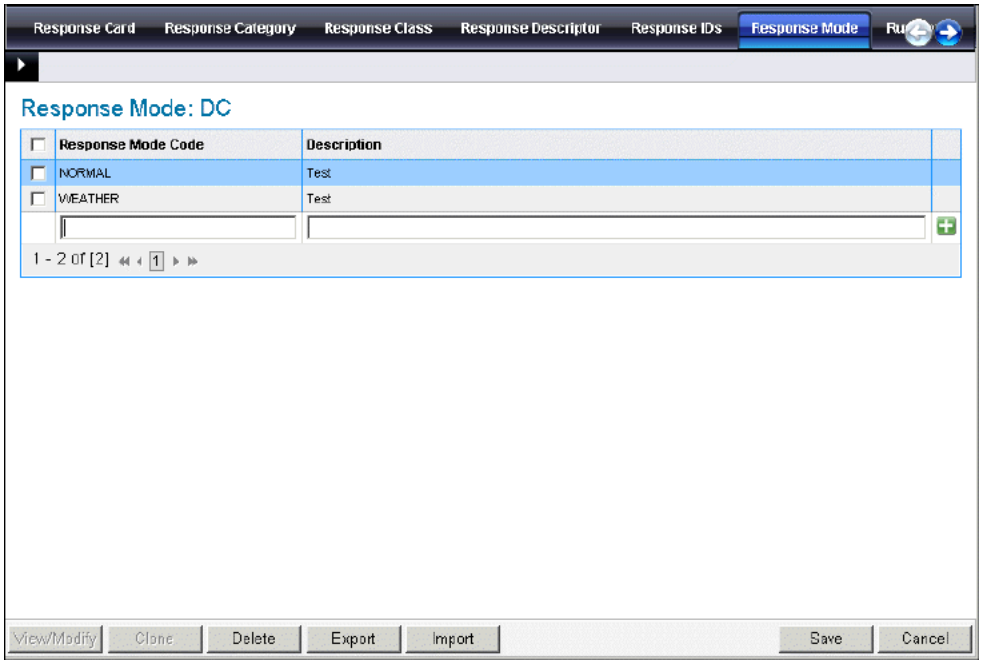


Figure 14-3 Response Mode Form

2. Click **View/Modify**.
3. In the blank Response Mode field, type a new response mode.
4. In the blank Description field, type a description for the response mode.
5. Click the plus symbol at the end of the row or press **Enter** to temporarily save the response mode and description and add another blank row.

   The new response mode and description display in blue to indication that they have not been permanently saved.
6. Repeat this procedure if you want to add more response modes.
7. Click **Save**.

   The new response modes and descriptions now display in black to indicate that they have been saved.

Configuring Response Classes

Use the response class configuration item to view, add, delete, export, and import response classes and their descriptions.

Response classes alter the standard unit recommendation made to a specific *location*. You can provision a response class for a specific address, an intersection, a street house number range, a common place, or a beat. Response classes are permanent adjustments.

Examples:

A beat does not contain a hydrant. The beat requires the addition of a tanker to the standard structure fire response recommendation. By separating the dry and wet regions and giving them different response classes, PremierOneCAD sends a tanker response automatically to the incident in the dry area.

You can provision PremierOneCAD to send additional specific units to hospitals. Use a response class to identify a hospital by its address.

Response class codes must be unique within an agency but do not have to be unique between agencies.

You can add, modify, export, import, and delete response classes. For details on modifying, exporting, importing, and deleting response classes, see “Working With Configuration Items” on page 2-9. You cannot change the response class code. If you want to change the code name, you must delete and re-add the record.

Adding Response Classes

Use the response class configuration item to add a response class. Response classes consist of the code for the response classes and a description.

Because response classes alter the standard unit recommendation made to a specific *location*, you must define a location for each response class you are going to add. The location can be an address, an intersection, a common place, a street range, or a jurisdictional location (beat, sector, or area).

To add a response class:

1. From the navigation panel, select **Unit Recommendation**, and then select **Response Class**.

The Response Class form appears.

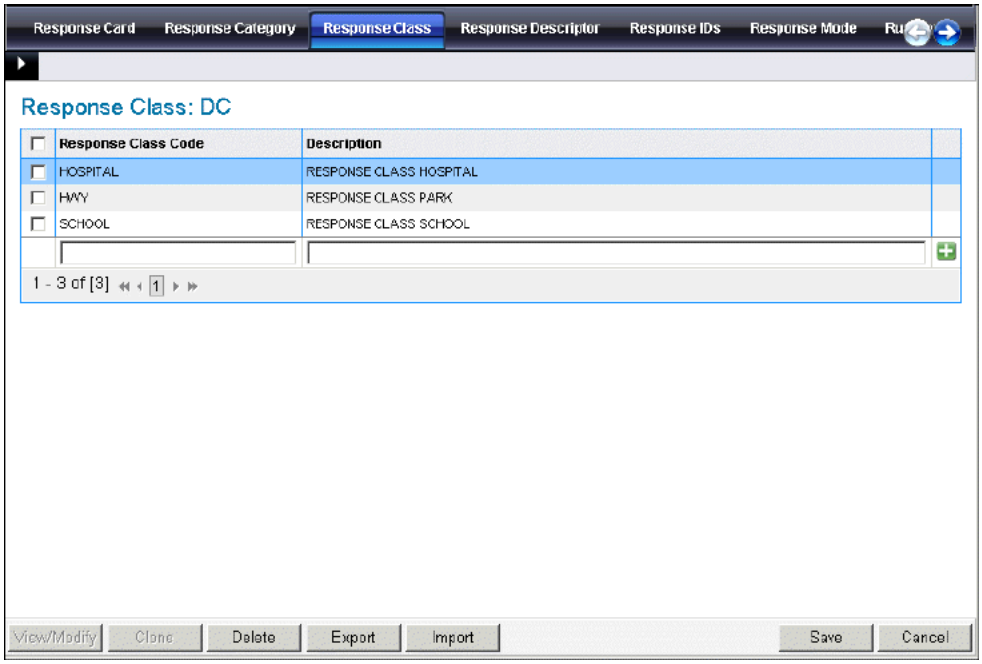


Figure 14-4 Response Class Form

2. Click **View/Modify**.
3. In the blank Response Class field, type a new response class.
4. In the blank Description field, type a description for the response class.
5. Click the plus symbol at the end of the row or press **Enter** to temporarily save the response mode and description and add another blank row.

   The new response class and description display in blue to indication that they have not been permanently saved.
6. Repeat this procedure if you want to add more response classes.
7. Click **Save**.

   The new response classes and descriptions now display in black to indicate that they have been saved.

Configuring Response IDs

Response IDs allow Incident Response Factors (IRFs) to be grouped by common response requirements. By grouping IRFs that have the same response requirements, your agency only has to provision the single response ID to get the same recommendations for all of the IRFs in the group.

You provision response IDs at the Agency Type level.

You can add, modify, export, import, and delete response IDs. For details on modifying, exporting, importing, and deleting response IDs, see “Working With Configuration Items” on page 2-9. You cannot change the response ID code name. If you want to change the response ID code name, you must delete and re-add the record.

Adding Response IDs

Use the response ID configuration item to add a response ID. Response IDs consists of the code for the response ID and a description.

To add a response ID:

1. From the navigation panel, select **Unit Recommendation**, and then select **Response ID**.

The Response ID form appears.

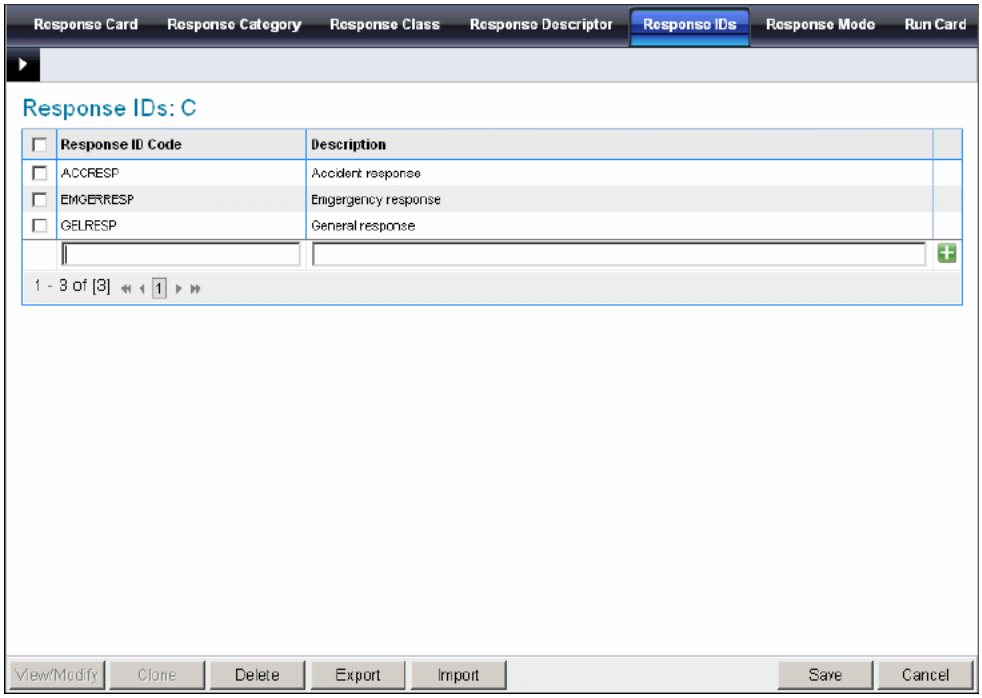


Figure 14-5 Response ID Form

2. Click **View/Modify**.

   You can now edit the fields in the last row.

3. In the blank Response ID field, type a new response ID.

4. In the blank Description field, type a description for the response ID.

5. Click the plus symbol at the end of the row or press **Enter** to temporarily save the response ID and description and add another blank row.

   The new response ID and description display in blue to indication that they have not been permanently saved.

6. Repeat this procedure if you want to add more response IDs.

7. Click **Save**.

   The new response IDs and descriptions now display in black to indicate that they have been saved.

Configuring Response Descriptors

Use the Response Descriptor configuration item to view and administer response descriptors and their descriptions.

A response descriptor manually alters the run card response while requesting recommendations.

Example

A beat can have separate run cards provisioned for Northbound (NB), Southbound (SB), Eastbound (EB), and Westbound (WB). A unit arriving on the scene of an accident needs assistance, but realizes that the accident has created a traffic jam in the southbound lanes. The normal response would have units traveling the southbound lanes, delaying their response. Therefore, the unit can ask the dispatcher to send a northbound Engine, rather than the normal southbound response Engine. The dispatcher can enter an Incident Dispatch command requesting 1 Engine with a response descriptor = NB.

You can add, modify, export, import, and delete response descriptors. For details on modifying exporting, importing, and deleting response descriptors, see “Working With Configuration Items” on page 2-9. You cannot change the response descriptor code name. If you want to change the code name, you must delete and re-add the record.

Adding Response Descriptors

Use the response descriptor configuration item to add a response descriptor. Response descriptors consist of the code for the response descriptor and a description.

To add a response descriptor:

1. From the navigation panel, select **Unit Recommendation**, and then select **Response Descriptor**.

The Response Class Descriptor form appears.

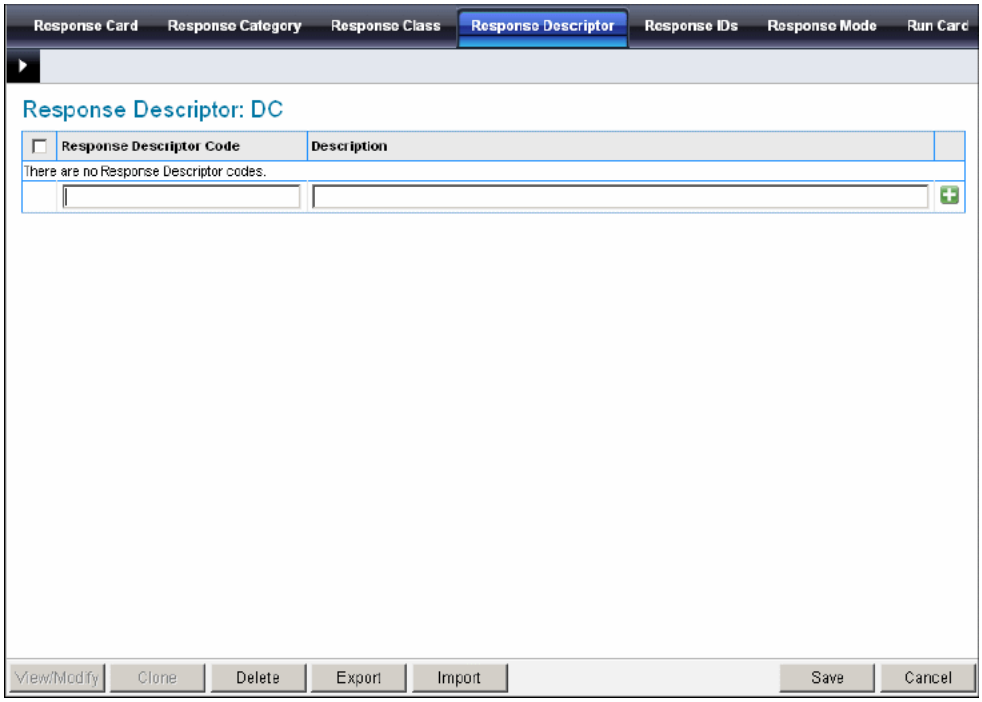


Figure 14-6 Response Descriptor Form

2. Click **View/Modify**.

   You can now edit the fields in the last row.

3. In the blank Response Descriptor Code field, type a new response descriptor code.

   Try to ensure that your response descriptor codes describe how the usual response is being altered.

   Example:

   WB describes that the response is being altered to go in a westbound direction rather than the usual direction.

4. In the blank Description field, type a description for the response descriptor.

5. Click the plus symbol at the end of the row or press **Enter** to temporarily save the response descriptor and description and add another blank row.

   The new response descriptor and description display in blue to indication that they have not been permanently saved.

6. Repeat this procedure if you want to add more response descriptors.

7. Click **Save**.

   The new response descriptors and descriptions now display in black to indicate that they have been saved.

Configuring Run Cards

Use the Run Card configuration item to view and administer run cards at the agency level.

Run cards allow you to define a set of fixed conditions that help identify the most appropriate units to dispatch to an incident with a specific jurisdiction. Run cards define where and in what order PremierOne looks to find units to dispatch. You can provision a different run card for each capability.

You can add, modify, export, import, delete, and copy run cards. For details on exporting, importing, and deleting run cards, see "Working With Configuration Items" on page 2-9. For details on copying run cards, see "Copying Run Cards" on page 14-26.

Searching for Run Cards

To search run cards, use the Run Card filter for existing run cards.

To search for run cards:

1. From the navigation panel, select **Unit Recommendation**, and then select **Run Card**.

   The Run Card filter area appears.

2. Select **Existing**.

   The Run Card search fields appear: Geographic Level, Geographic Value, Sequence #, Order Type, and Order Type Value.

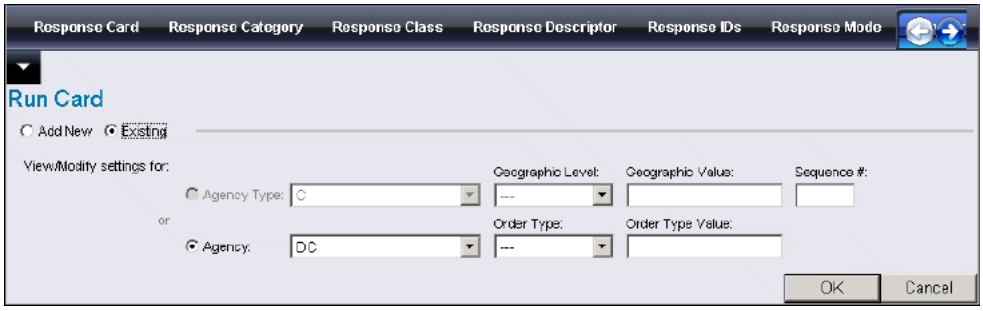


Figure 14-7 Run Card Filter Showing Search Fields

3. Select information for or enter information in as many of the search fields as you can.

   The more valid information you enter, the fewer results you will receive.

If you know the Geographic Level, such as Agency, Area, Beat, Location, or Sector, that you want to search for, select it in the Geographic Level field and type the value in the Geographic Value field.

If you know the sequence number, type that in the Sequence # field. The Sequence # is automatically assigned by PremierOne when you create the Run Card.

If you know the Order Type, such as Area, Beat, Jurisdiction, Section, Station, or Unit, that you want to search for, select it in the Order Type field, and type the value in the Order Type Value field.

4. Click **OK**.

Adding Run Cards

Use the run card configuration item to add a run card. When you add a run card, you enter information on three tabs of the Run Card form:

- Run Card Order – Where you enter the geographic level, the geographic value, the city, and the run card order information, including the order type and order value.
- Run Card Resp ID – Where you enter the run card conditions including the response ID, response class, response mode, response descriptor, and capability, as well as the days of the week and times that this run card is valid.
- Run Card IRF – Where you enter run card conditions for incident response factors (IRFs) including incident type, modifying circumstance, alarm level, response class, response mode, response descriptor, and capability, as well as the days of the week and times that this run card is valid.

When you add a run card, PremierOne automatically adds a new sequence number, based on the jurisdiction, to the run card. The sequence number value cannot be edited.

Adding Run Card Order Information

Run order information includes the geographic level and value and the run card order.

To add run card run order information:

1. From the navigation panel, select **Unit Recommendation**, and then select **Run Card**.

The Run Card form appears with a list of existing run cards on the left side of the form. If you typed specific information in the Geographic Level and Value or Sequence # fields in the filter, the run card you specified appears in the form with no other run cards.

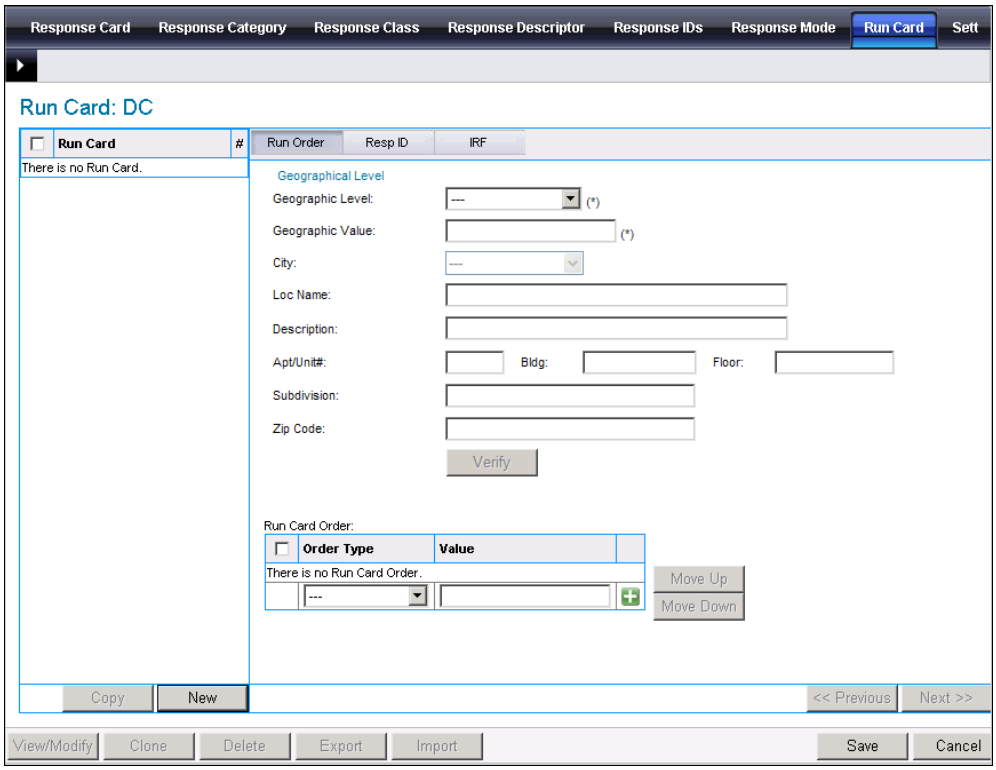


Figure 14-8 Run Card Form

2. At the bottom of the Run Card list, click the **New** button.
3. In the Geographic Level field, select the geographic level. (Required field)

   The default value is `Null` or ---; however, you must select a value from the list.
4. In the Geographic Value field, type a value for the geographic level.

   - If you selected `Agency` in the Geographic Level, PremierOne sets this field to the agency that is provisioning this record. No other agency value is allowed.
   - If you selected `Area` in the Geographic Level, you can enter any valid area across all provisioned active and inactive plans.
   - If you selected `Beat` in the Geographic Level, you can enter any valid beat for the provisioning agency.
   - If you selected `Location` in the Geographic Level, you can enter any valid GIS Location including Addresses, Intersections, and Common Places.

You can also enter the city or a partial city value in the City field to verify the address.

- If you selected Sector in the Geographic Level, you can enter any valid sector across all provisioned active and inactive plans for the provisioning agency.

5. For each entity, select the Order Type in the Run Card Order section. Valid values for the order type are: Area, Beat, Jurisdiction, Sector, Station, and Unit. The Order Type identifies the order in which PremierOne should search for the appropriate units to recommend.

   The default value is Null or ---; however, you must select a value from the list.

6. In the Value field, type a value for the entity.

   The default value is Null or ---, regardless of Order Type.

   - If you selected Area from the Order Type list, you can enter any valid Agency ID/Area across all provisioned active and inactive plans.
   - If you selected Beat from the Order Type list, you can enter any valid Agency ID/Beat.
   - If you selected Jurisdiction from the Order Type list, you must select one of these values from the list: Area, Beat, or Sector.
   - If you selected Sector the from the Order Type list you can enter any valid Agency ID/Sector across all provisioned active and inactive plans.
   - If you selected Station from the Order Type list, you can enter any valid Agency ID/Station provisioned for the agency.
   - If you selected Unit from the Order Type list, you can enter any Agency ID/ Unit ID.
     - To allow for the entry of wildcard characters, PremierOne does not validate the Unit ID entries in this field, even when your agency is provisioned: to validate unit IDs.
     - You can enter a question mark within the Unit ID to represent a single-character wildcard value. For example, enter 1?1 to represent Unit IDs 1A1, 1B1, 1C1, and so on.
     - You can enter an asterisk within the Unit ID to represent a multi-character wildcard value. For example, enter 1*1 to represent 1A1, 1B1, 1C1, 130A1, 1ANYTHING1, and so on.

   After each type and value selection, click the plus symbol at the end of the row to temporarily save your selection and add an additional row.

7. Add as many run cards as you need. To change the run card order, select a row by clicking the check box to the left of the Order Type, and then click the **Move Up** or **Move Down** buttons next to the Run Card Order table.

The Order Type and Order Type Entity value must be unique among the run cards.

> **NOTE**
> The order of the run cards is important. Run cards are evaluated from the top to the bottom of the list.

8. Click **Save**.

Adding Run Card Response ID Information

Response ID information includes the run card conditions of response ID, response class, response mode, response descriptor, and capability, as well as the days of the week and times that this run card is valid.

To add run card response ID information:

1. Access the form for run cards. For instructions, see "Adding Run Card Order Information" on page 14-20.

   The Run Card form appears (see Figure 14-8). A list of existing run cards displays on the left side of the form.

2. Select the Resp ID tab.

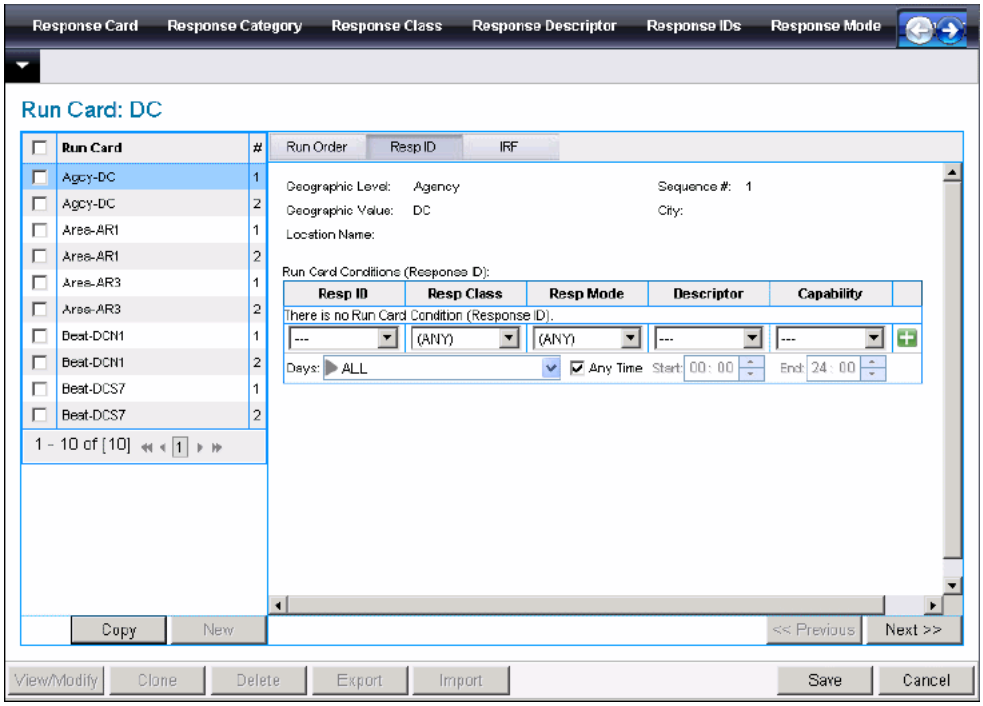


Figure 14-9 Run Card Form – Resp ID Tab

3. Click **View/Modify**.

   You can now edit the fields in the Run Card Conditions area.

4. In the Run Card Conditions area, select a value for each field.

   These fields are required for response ID: Resp ID and Capability. The others are optional.

   The default value for each field is Null or ---. You can select any valid value for the Agency Type of the provisioning agency or you can select (ANY).

5. In the Days field, select a day or leave at the default of ALL.

6. In the Start field, do one of the following:

   - Accept the default of Any Time.

     Any Time means any time other than the value in the Start and End time fields.

     Example:

     A school is in session from 9:00 AM until 3:00 PM. Any Time is any time other than 9:00 AM to 3:00 PM.

   - Enter values in the Start and End fields to indicate start and end times for the day or days of the week you selected.

     The Start and End fields accept values in the 24 hour time format from 00:00 to 24:00.

     PremierOne prevents overlaps in Days of Week and Time Range entries.

7. Click the plus symbol at the end of the row to add another blank row, and then continue adding values.

   The combination of values you set in this procedure must be unique within the same run card and ideally should be unique across all run cards with the same Run Card Identification user-entered values.

8. Click **Save**.

Adding Run Card IRF Information

IRF information includes the run card conditions of incident type, modifying circumstance, alarm level, response class, response mode, response descriptor, capability, and the days of the week and times that this run card is valid.

To add run card IRF information:

1. Access the form for run cards. For instructions, see “Adding Run Cards” on page 14-20.

   The Run Card form appears (see Figure 14-8). A list of existing run cards displays on the left side of the form.

2. Select the IRF tab.

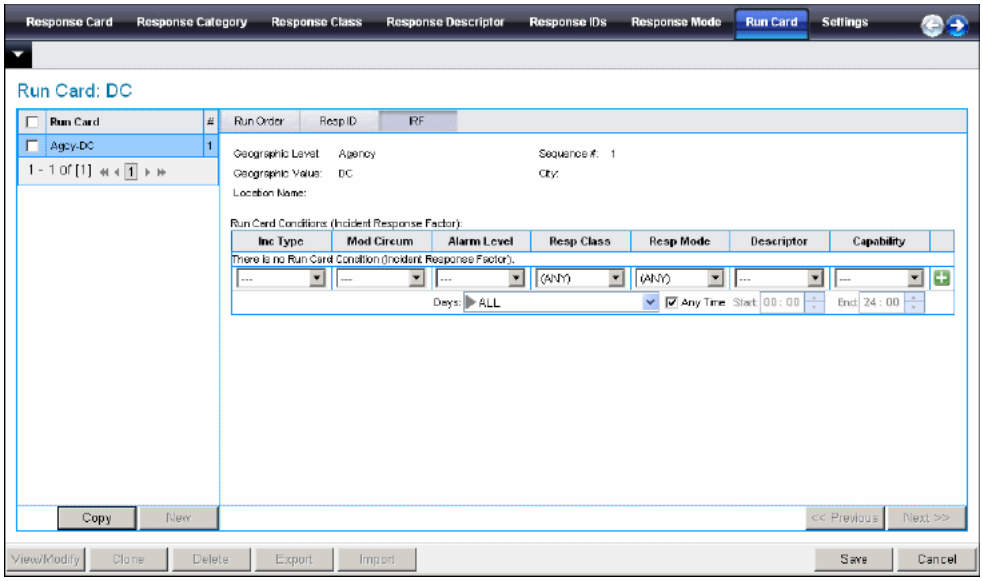


Figure 14-10 Run Card Form – IRF Form

3. Click **View/Modify**.

   You can now edit the fields in the Run Card Conditions area.

4. In the Run Card Conditions area, select a value for each field.

   These fields are required for incident response factor: Inc Type and Capability. The others are optional.

   The default value for each field is Null or ---. You can select any valid value for the Agency Type of the provisioning agency or you can select (ANY).

5. In the Days field, select a day or leave at the default of ALL.

6. In the Start field, do one of the following:

   - Accept the default of Any Time.
   - Enter values in the Start and End fields to indicate start and end times for the day or days of the week you selected.

     The Start and End fields accept values in the 24 hour time format from 00:00 to 24:00.

     PremierOne prevents overlaps in Days of Week and Time Range entries.

7. Click the plus symbol at the end of the row to add another blank row, and then continue adding values.

   The combination of values you set in this procedure must be unique within the same run card and ideally should be unique across all run cards with the same Run Card Identification user-entered values.

8. Click **Save**.

Copying Run Cards

Copy a run card when you want to use an existing run card record as the default value for creating a new run card. By retrieving an existing run card and pressing the Copy button, PremierOne behaves as if you pressed the New button but keeps all of the existing data within the Provisioning form intact. All fields become editable.

Example:

The run card order for neighboring fire beats share the same 50 stations in their run card order, but the first two stations in the order are reversed. Beat 101's Run Card Order is: STN1, STN2, STN3, STN4, ..., STN50, and Beat 102's run card order is: STN2, STN1, STN3, STN4, ..., STN50. The run card conditions are also the same for these two beats.

Therefore, what the administrator needs is the ability to copy the properties once for Beat 101, and copy it to Beat 102. At this point, the administrator only has to change the run card IDs Geographic Level (Beat =102), and the first two stations in the run card order and save the record.

To copy a run card:

1. Access the form for run cards. For instructions, see "Adding Run Cards" on page 14-20.

   The Run Card form appears (see Figure 14-8). A list of existing run cards displays on the left side of the form.

2. From the list of existing run cards, select the one you want to copy so it is highlighted. You do not have to select the check box, and then click **Copy**.

   The information from the run card you selected appears in the Run Order tab.

3. Make any changes necessary on the Run Order, Resp ID, and IRF tabs.

4. Click **Save**.

Breaking Ties on a Run Card

There are times when PremierOne CAD finds multiple units at the same location that satisfy a given item on a run card. When this happens, PremierOne uses the following rules, in order, to select the unit:

1. The unit or combination of units that satisfies the greatest number of combined capabilities.

2. The unit or combination of units that result in the fewest number of people being sent to still satisfy the required number of people.

3. Rotational sub-search. Rotational sub-search uses the following rules:

    a. Preferred Unit Order. If two or more units with the same capabilities reside in the same station, then units are selected in the preferred unit order provisioned for that station. The preferred unit order only considers units when they are within their home station.

    b. Unit Longest in Clear Status. If no preferred unit order is provisioned or if the units are not located in the same station, then the unit that has been in a clear status the longest is selected.

    c. Alphabetically by Unit ID.

Configuring Unit Recommendations Settings

The Unit Recommendations Settings configuration item contains the following tabs:

- General – Where you set how logging of recommended units to Incident History should be done.
- Capability – Where you provision the sort order of capabilities.
- Duty Type – Where you provision the sort order of duty types.
- Vehicle Type – Where you set the maximum driving speed for vehicle types.

Logging Unit Recommendations

Use the General subtab to provision how logging of recommended units to Incident History should be done: whenever recommendations are requested; when units are dispatched or when recommendations are requested and no units are returned; or *only* when recommendations are requested and no units are returned.

This feature provides your agency with the opportunity to compare the units that were recommended for an incident against the units that were actually dispatched to the incident. The feature allows your agency to evaluate:

- Your recommendation schemes to ensure that the most appropriate units are being recommended
- Your dispatchers to ensure that they are dispatching the most appropriate units to the incident

This feature also allows your agency to automatically log to an incident's history the fact that no units were recommendable at the time of dispatch. This incident history record helps to provide evidence that a delay in responding to an incident was caused by the lack of available resources.

To log unit recommendations:

1. From the Navigation panel, select **Unit Recommendation**, and then select **Settings**.

   The Settings form appears with the General subtab in focus.

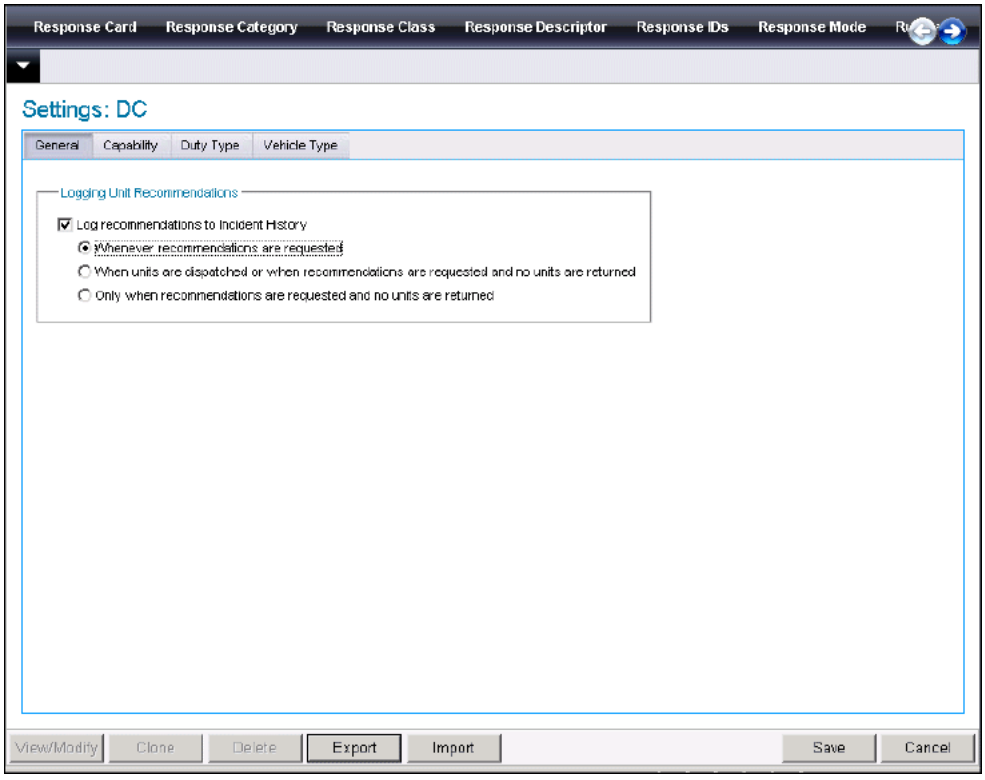


Figure 14-11 Settings – General Subtab

2. To use Unit Recommendations logging at the agency level, select the Log recommendations to Incident History check box, and then select one of the following options:

   a. Whenever recommendations are requested – to log unit recommendations to Incident History each time recommendations are requested

      This option includes logging an Incident History transaction when no recommended units are found, or when no response card is provisioned for the incident's Incident Response Factor (IRF) or Response ID.

   b. When units are dispatched or when recommendations are requested and no units are returned – to log unit recommendations to Incident History only when the requested recommendation is associated with a dispatch, or when no recommendable units were returned

      This option allows logging in two different scenarios: when units are dispatched *and* when recommendations are requested and no units are returned.

      This option also includes logging an Incident History transaction when no recommended units are found, or when no response card is provisioned for the incident's IRF or Response ID.

   c. Only when recommendations are requested and no units are returned – to log unit recommendations to Incident History only when recommendations are requested but no recommendable units were returned

      This option is different from the second option. This option allows logging *only* when recommendations are requested and no units are returned. The only other instances where an Incident History transaction is logged are when no recommended units are found, or when no response card is provisioned for the incident's IRF or Response ID.

      Units would not be logged that were dispatched or that were requested and recommended.

3. Click **Save**.

Recommendation requests can be performed in CAD using the Request button in the Dispatch form or using the ID command from the command line to display the Dispatch form.

Holding Units for Dispatch

This feature is planned for a future release.

Use the General subtab to set whether units recommended for dispatch are held for dispatch and, if so, the length of time the units are held.

In some agencies, especially fire agencies, multiple dispatchers can be responsible for the same set of units. To prevent a unit from being recommended for different incidents at the same time, an agency can enable holding the unit upon its first recommendation so that the unit will not be recommended while it is being held.

When you enable this feature, you must also specify the amount of time (in seconds) the recommended units will be held for an incident that belongs to that agency. This way, if a dispatcher leaves an Incident Dispatch form displayed for an extended period of time, the units that are recommended within the form will be released from their held state after the provisioned amount of time, and can now be recommended for another incident.

To hold units for dispatch:

1. From the navigation panel, select **Unit Recommendation**, and then select **Settings**.

   The Settings form appears with the General subtab in focus.

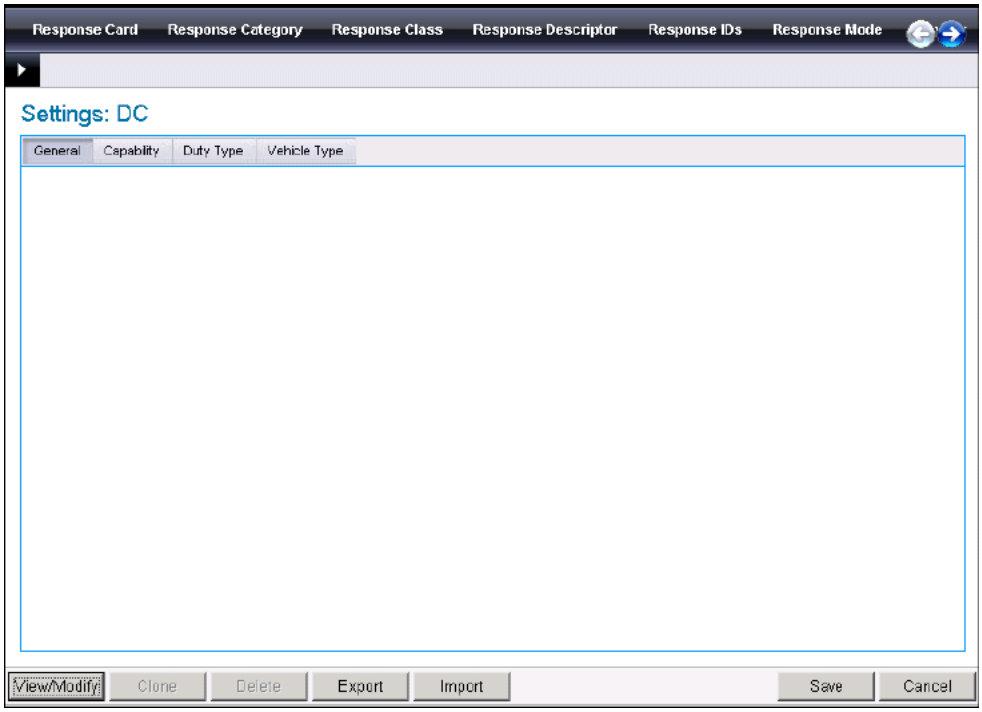


Figure 14-12 Settings – General Subtab

2. Click **View/Modify**.

3. To hold units for dispatch, select the check box next to the Hold units recommended for dispatch field.

4. In the seconds field, select the length of time to hold the units.

5. Click **Save**.

Setting the Sort Order for Capabilities

Use the Capability subtab to set the capability sort order so the dispatcher can quickly identify the relationship between each recommended unit and that unit's recommended capability. This allows the dispatcher to evaluate the effects of dispatching the recommended units based on their recommended capabilities.

Example:

Three Ladder units were recommended as substitutes for the three Engines that are needed for an incident. The dispatcher wonders whether he or she should dispatch all of the Ladder units (making them unavailable for a potentially more serious incident that may require a Ladder), or should he or she dispatch two Ladder units and an Engine that is a little further away?

If the agency uses the sort order for capabilities, and has sorted it to show Capability = Engine first, followed by Capability = Ladder, the dispatcher's decision will be easier because the units identified for each unit capability will be listed in the order of recommendation.

To set the sort order for capabilities:

1. Access the Settings form.

   The Settings form displays with the General subtab in focus (see Figure 14-12).

2. Select the Capability subtab.

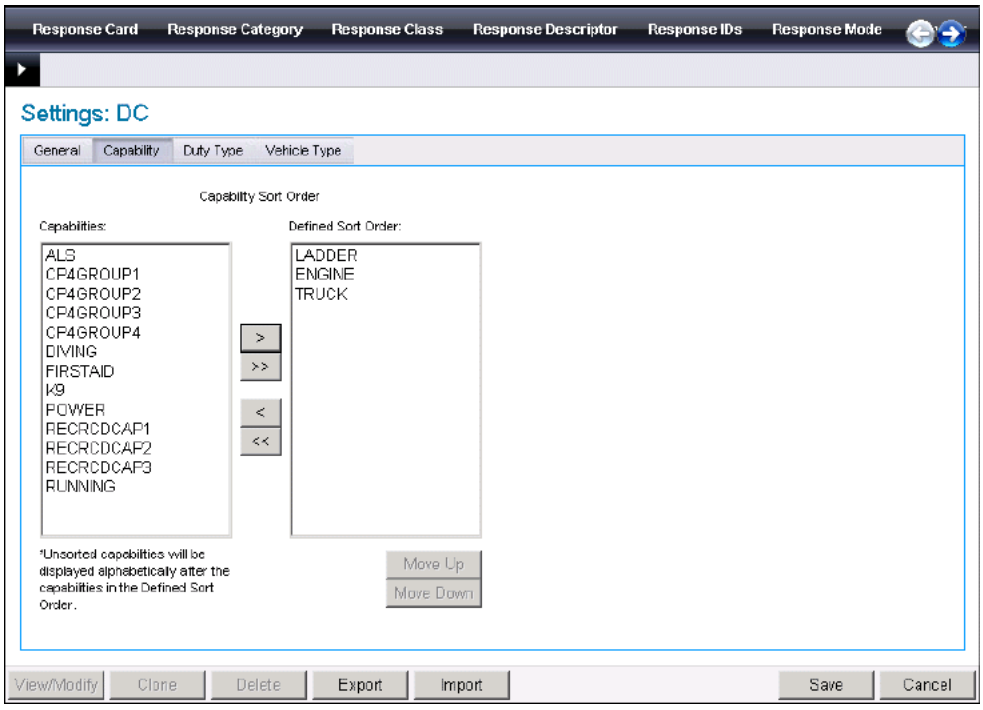


Figure 14-13 Settings – Capability Subtab

3. Click **View/Modify**.

4. From the Capabilities list, select the capabilities you want to sort and move them to the Defined Sort Order list.

5. Use the **Move Up** and **Move Down** buttons to sort the capabilities in the Defined Sort Order list.

   Any capabilities that you do not sort will be displayed alphabetically after the sorted capabilities in the Defined Sort Order.

6. Click **Save**.

Setting the Sort Order for Duty Types

Use the Duty Type subtab to set the sort order for duty types so that a dispatcher can broadcast the units in a specific order based on the duty type assigned to each unit.

Example:

A fire dispatcher is getting ready to dispatch the following units onto an incident based on the incident's response requirements:

Response Requirements	Units to Be Dispatched
1-Battalion Chief	BC1
1-Division Chief	DC1
3-Engines	E101, Q17, L14
2-Ladders	L3, Q33
2-Rescue	E215, AMB11

The duty types assigned to each of these units is as follows:

Duty Type	Units
BATCHIEF	BC1
DIVCHIEF	DC3
ENGINE	E101, E215
LADDER	L3, L14
QUINT	Q17, Q33
RESCUE	AMB11

The recommended units within each duty type are grouped together in the order of recommendation. All remaining units assigned to duty types that are not identified within the Duty Types Sort Order are listed in the order of recommendation following the provisioned sort order.

For this agency, the dispatcher would be required to broadcast the units being dispatched onto the incident in the following duty type order: ENGINE, LADDER, QUINT; BATCHIEF.

The actual dispatch of these units would need to be ordered based on the above duty type order, followed by the remaining units in the order of recommendation. Therefore, the units would be displayed in the Incident Management form as follows:

Order of Units to be Dispatch	E101. E215	L14. L3	Q17. Q33	BC1	AMB11	DC3
Duty Types	ENGINE	LADDER	QUINT	BATCHIEF	N/A	N/A

Provisioning the duty types sort order allows an agency to define the order in which units are to be broadcast when dispatched onto an incident. The agency does not have to order all of their duty types, only those that need to be broadcast in a specific order.

To set the sort order for duty types:

1. Access the Settings form.

   The Settings form displays with the General subtab in focus (see Figure 14-12).

2. Select the Duty Type subtab.

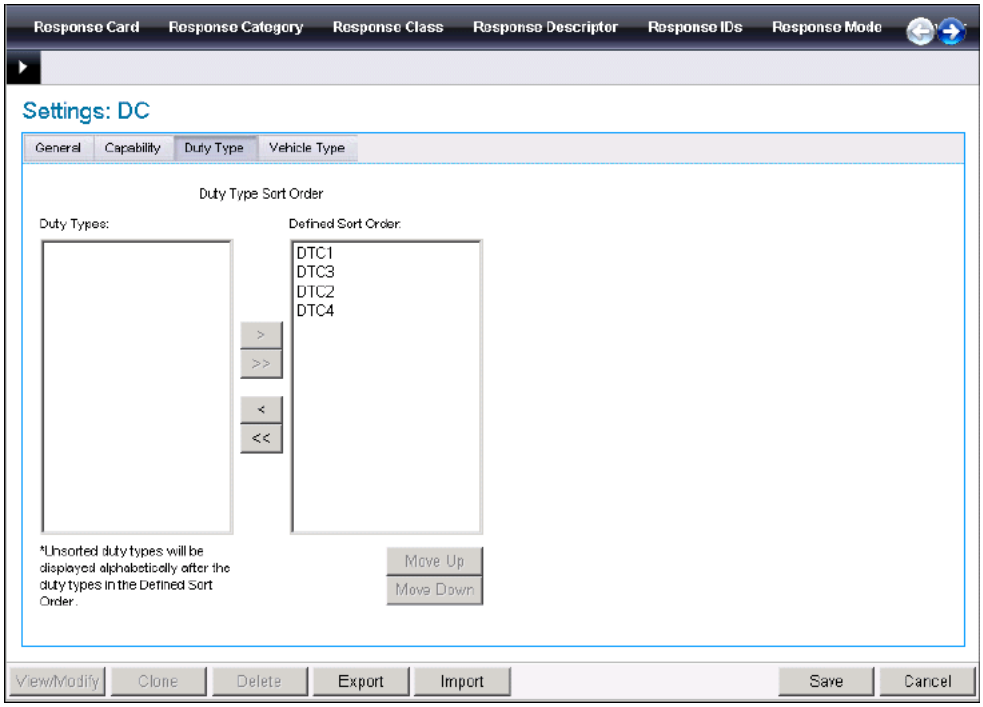


Figure 14-14 Settings – Duty Type Subtab

3. Click **View/Modify**.

4. From the Duty Types list, select the duty types you want to sort and move them to the Defined Sort Order list.

5. Use the **Move Up** and **Move Down** buttons to sort the capabilities in the Defined Sort Order list.

   Any duty types that you do not sort will be displayed alphabetically after the sorted duty types in the Defined Sort Order.

6. Click **Save**.

Setting the Maximum Speed for ARL Recommendations for a Vehicle Type

Use the Vehicle Type subtab to set the maximum driving speed for ARL (Automated Resource Locator) recommendations for a specific vehicle type.

Each ARL-equipped vehicle type that is provisioned for your agency must have a maximum driving speed (in miles per hour) associated with it. During the ARL recommendations process, this value is applied to each unit's straight line distance and can potentially reduce the number of ETA (estimated time of arrival) calculations that are required.

NOTE
You cannot disable the Maximum Driving Speed value. Make sure the speed is not set to zero or you will not get valid recommendations.

To set the maximum driving speed for ARL recommendations for a vehicle type:

1. Access the Settings form.

   The Settings form displays with the General subtab in focus (see Figure 14-12).

2. Select the Vehicle Type subtab.

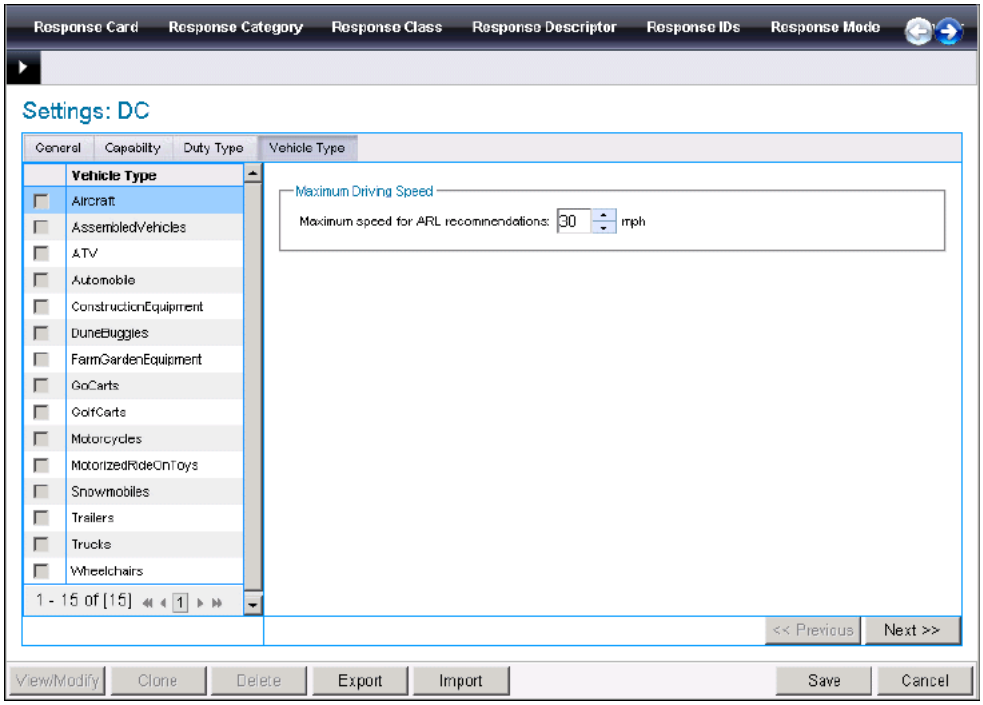


Figure 14-15 Settings – Vehicle Type Subtab

3. Click **View/Modify**.

4. From the list of vehicle types on the left, select the type of vehicle for which you want to set a maximum speed for ARL recommendations. You do not have to select the check box.

5. Select the maximum speed to use for recommendations when ARL is enabled.

   The default value is 30. The maximum value is 99.

6. Repeat these steps for any other vehicle types for which you want to set speeds.

7. Click **Save**.

Configuring Response Categories

Use the Response Category configuration item to view and administer response categories and their descriptions.

Response categories allow an agency to group similar unit capabilities together. Grouping capabilities together makes reviewing and maintaining a unit's capabilities much more effective. For more information about unit capabilities, see "Capabilities Overview" on page 11-4.

You can add, modify, export, import, and delete response categories. For details on modifying, exporting, importing, and deleting response categories, see "Working With Configuration Items" on page 2-9. You cannot change the response category name. If you want to change the response category name, you must delete and re-add the record.

Adding Response Categories

Use the response category configuration item to add a response category. Response categories consist of the code for the response category, a description, and capability settings.

To add a response category:

1. From the navigation panel, select **Unit Recommendation**, and then select **Response Category**.

The Response Category form appears with a list of existing response category codes on the left side of the form.

NOTE

SKILL is a reserved category for each agency and is always listed. You cannot change, update, or delete the SKILL category.

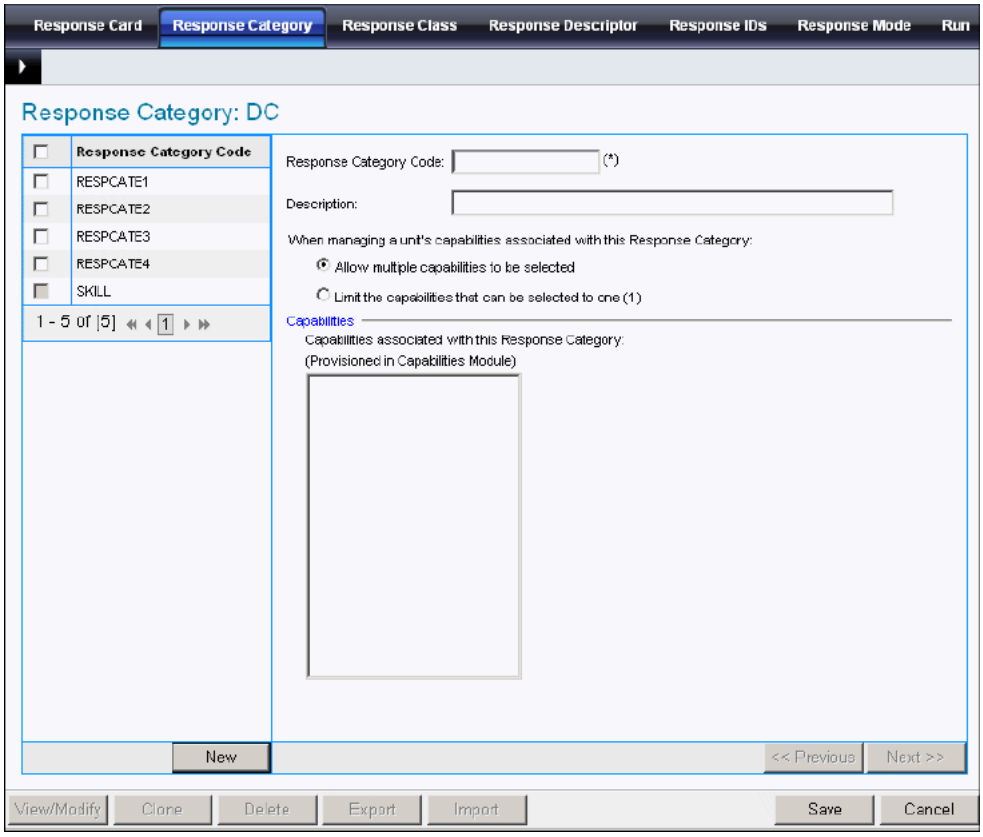


Figure 14-16 Response Category Form

2. Click **New**.
3. In the Response Category Code field, type the name of your new response category.
4. In the Description field, type a description for the response category.
5. In the next section, indicate whether multiple capabilities can be selected simultaneously (Allow multiple capabilities to be selected) or whether capabilities are mutually exclusive (Limit the capabilities that can be selected to one (1)).

   Example:

   An example of a response category that limits the capabilities than can be selected to one is Medical Response where you can select either ALS (Advanced Life Support) *or* BLS (Basic Life Support), but not both.

However, if you want to allow a unit to respond to both ALS *and* BLS calls, select Allow multiple capabilities to be selected.

6. Click **Save**.

CHAPTER 15

Configuring Contractor Rotation

The Contractor Rotation configuration item contains the following items:

- General – Where you configure contractor types, capabilities, and action codes. For details, see “Configuring General Contractor Information” on page 15-2.
- Contractors – Where you configure contractors. For details, see “Configuring Individual Contractors Information” on page 15-8.
- Rotations – Where you set up contractor rotations. For details, see “Configuring Contractor Rotations” on page 15-16.

The Contractor Rotation feature provides CAD users a means of assigning support providers and equipment to an incident on a rotational basis. Such providers might include towing companies, judges, or detectives, as well as utility services such as sewer, water, and street repair. Rotational assignment of these providers ensures fair distribution of business opportunities for the individual contractors.

You can assign permissions for use of the Contractor Rotation (CR) command per provisioned role. For more information, see “Configuring Role Permissions” on page 8-1.

Configuring General Contractor Information

Enter general contractor information when your agency wants to start using a new category of support provider. When you add general information, you enter information on three tabs of the General form:

- Contractor Types – Where you set general information, such as contractor type, capabilities, and action codes.
- Capabilities – Where you define, at the agency level, all the valid contractor capabilities used for a particular agency.
- Action Codes – Where you define codes for contractor actions such as Contractor accepted, Contractor declined, Contractor withdrew acceptance, and so on.

You can add, modify, import, export, clone, and delete contractor information. For details on modifying, importing, exporting, cloning, and deleting, see "Working With Configuration Items" on page 2-9. You cannot change an existing contractor type name. If you want to change the name, you must delete and re-add the record.

Adding Contractor Types

Contractor Types are used to distinguish different categories of contractors, such as Towing or Judges. CAD users must first select a contractor type when making a contractor request.

You can provision a default contractor type for each agency that will appear when a CAD user is requesting a contractor from the command line. For more information, see "Configuring Commands" on page 21-1.

To add a contractor type:

1. From the navigation panel, select **Contractor Rotation** and then select **General**.

The General form for the selected agency appears in the work area, with the Contractor Types tab in focus.

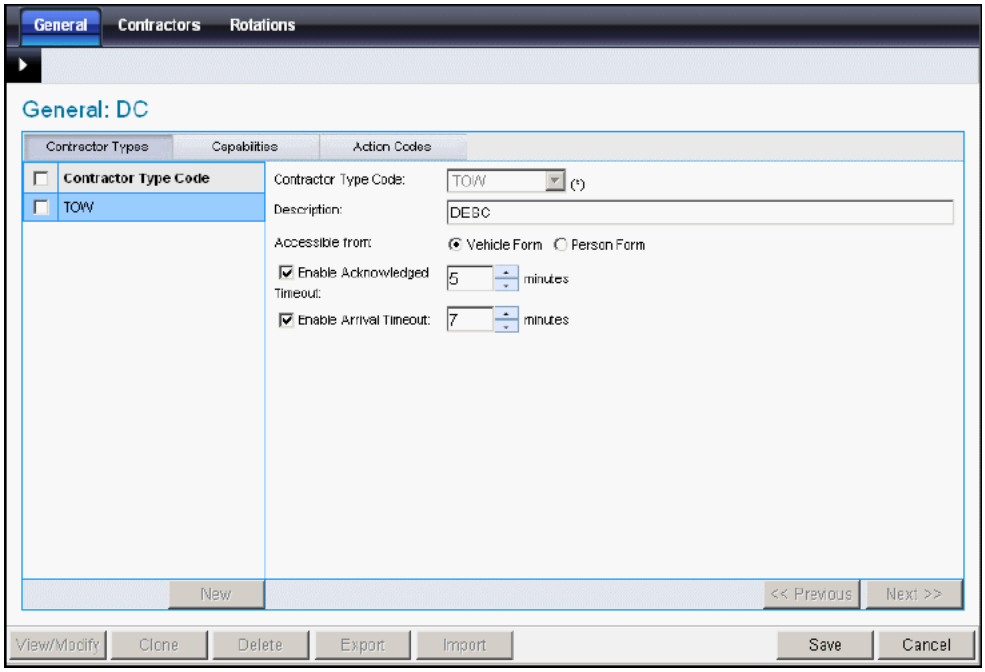


Figure 15-1 Contractor Rotation General Form

2. At the bottom of the Contractor Type list, click **New**.

   The Contractor Type form refreshes, with all fields enabled for entry.

> **NOTE**
> The New button is enabled only as long as there are contractor type codes that are not used.

3. From the Contractor Type Code list, select the code for the contractor type.

   The code must be unique within the specified agency, but need not be unique across different agencies.

   Contractor type codes are defined at the mapping layer by your GIS administrator.

4. In the Description field, type a description of the new contractor type, such as Towing, or Judges.

5. In the Accessible from field, select the appropriate button to indicate which Incident Management tab, Vehicle or Person, you want the contractor information to display in.

   - If the Contractor Type is Towing, select **Vehicle Form**.
   - If the Contractor Type is Judges, select **Person Form**.

6. In the Enable Acknowledged Timeout field, enter the number of minutes a contractor of this type will have to acknowledge a request for service. If this timer expires, the dispatcher is notified and the dispatcher can assign another contractor to the incident.

   To enter an acknowledgement timeout, select the Enable Acknowledged Timeout check box and then enter the minutes in the adjacent field.

7. In the Enable Arrival Timeout field, enter the number of minutes a contractor of this type will have to arrive on the scene of a request for service. The default value is 30 minutes. If this timer expires, the dispatcher is notified and can assign another contractor to the incident.

   To enter an arrival timeout, select the Enable Arrival Timeout check box and then enter the minutes in the adjacent field.

8. To add another contractor type, click **New** again.

9. Click **Save**.

   The contractor types you added appear in the Contractor Type list, and a success message displays in the Status Message area.

Adding Contractor Capabilities

Use the Contractor capabilities tab to define all the valid contractor capabilities used for a particular agency. Contractor capabilities allow users to make contractor requests that require specific abilities or equipment, such as large capacity tow trucks or motorcycle tow trucks.

You can add, modify, import, export, and delete contractor capabilities. For details on modifying, importing, exporting, and deleting capabilities, see “Working With Configuration Items” on page 2-9. You cannot change the capability name. If you want to change a capability name, you must delete and then re-add the code.

To add a contractor capability:

1. Access the Contractor Rotation General form for the appropriate agency. For instructions, see “Adding Contractor Types” on page 15-2.

2. Click the Capabilities tab.

The Capabilities form appears in the work area.

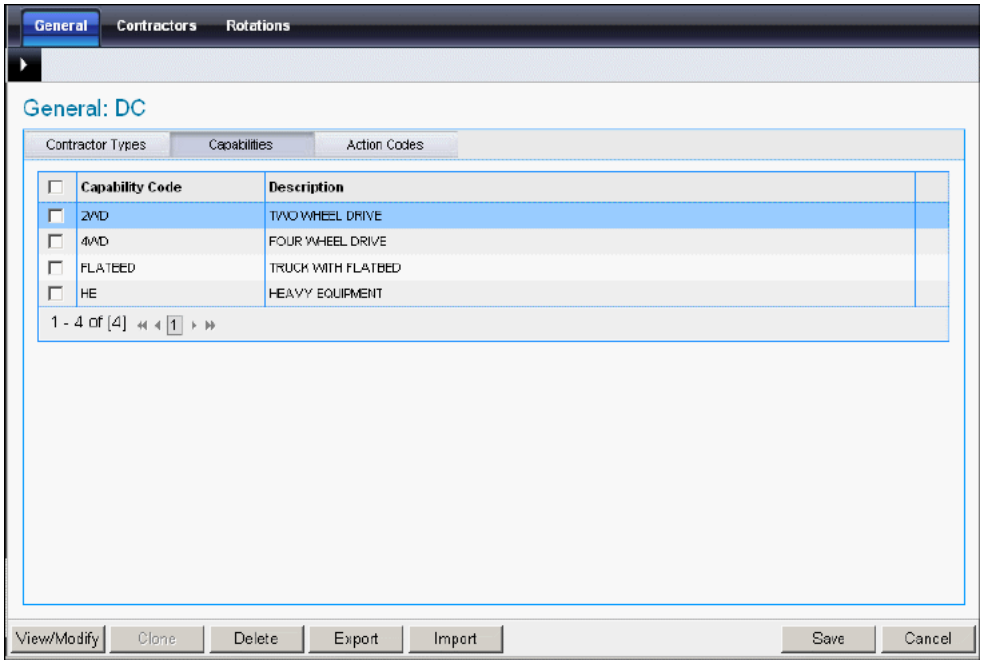


Figure 15-2 Contractor Capabilities Form

3. Click **View/Modify**.

   The Capabilities form refreshes. The first existing capability in the table is highlighted and the Description field becomes editable.

   Additionally, a new row appears at the bottom of the table.

4. In the new field at the bottom of the Capability Code column, type a code for the new capability.

5. In the new field at the bottom of the Description column, type a description for the new capability.

6. Click the plus icon (+) to the right of the Description field.

   The new capability is added to the table, and a new blank row for adding another capability appears at the bottom of the table.

7. Repeat this procedure to add other capabilities.

8. Click **Save**.

Modifying Contractor Action Codes

PremierOne is installed with a default set of actions that might occur in response to a contractor request. Each action has a corresponding default action code. You can modify the action codes to meet the preferences of a particular agency, but you cannot change the default contractor actions.

CAD users can select an action code on the Contractor Request form to define the response to a request.

The default contractor actions include the following:

- CA – Contractor accepted
- CD – Contractor declined
- CP – Contractor paged
- CU – Contractor could not be contacted
- N – Show next company
- CW – Contractor withdrew acceptance
- AW – Agency withdrew request
- ST – Stop timer
- RT – Reset timer

To modify a contractor action code:

1. Access the Contractor Rotation General form. For instructions, see “Adding Contractor Types” on page 15-2.

   The General form appears in the work area.

2. Click the **Action Codes** tab.

The Action Codes form appears.

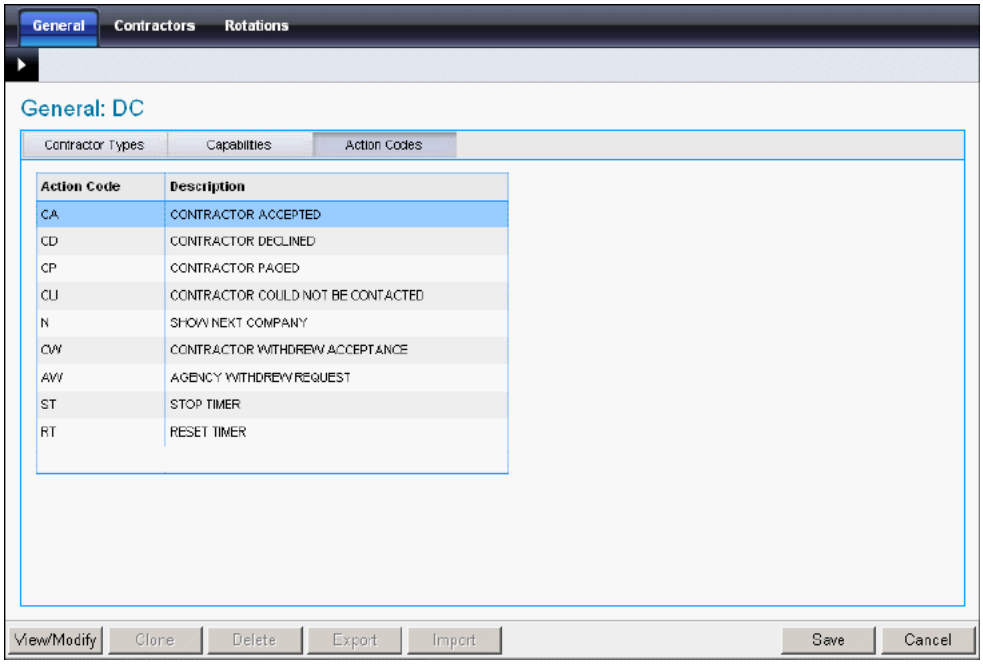


Figure 15-3 Action Codes Form

3. To modify an action code, click the code to select it.
4. Click **View/Modify**.

   The Action Code field for the selected action code becomes editable.
5. Type a new action code for the action.
6. Click **Save**.

Provisioning Auto Club Affiliations and Payment Methods

Use the List and Statute Management form to provision contractors' auto club affiliations and payment methods. CAD users can select these values on the Contractor Request form. For details on lists, see "Configuring Lists and Codes" on page 6-1.

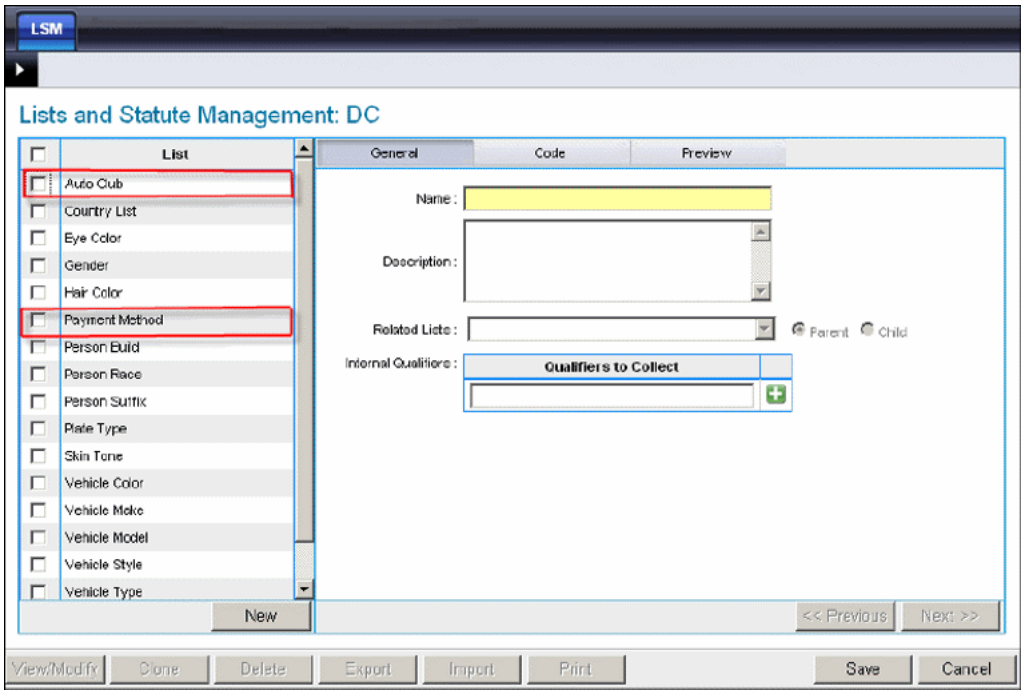


Figure 15-4 Lists And Statute Management Form

Configuring Individual Contractors Information

Use the Contractors form when your agency wants to add or modify information about a new or existing support provider. When you add contractor information, you enter information on three tabs of the Contractors form:

- General – Where you enter general information, such as contractor name, ID code, capabilities, and contact phone numbers.
- Addresses – Where you enter address information for contractors, including email addresses.
- Contractor Types – Where you associate contractors to the appropriate Contractor Types defined for the agency.

You can add, modify, import, export, clone, and delete contractor information. For details on importing, exporting, cloning, and deleting, see “Working With Configuration Items” on page 2-9.

Adding New Contractors

Service providers that you add as new contractors can be businesses, such as towing companies or taxi services, or persons, such as judges or detectives. Once entered in the system, contractors can be added to rotation lists.

Contact information added for contractor rotation is also automatically available in the PremierOne global address book. For information on address books, see “Configuring Address Books” on page 18-1.

Adding General Contractor Contact Information

The General form displays different fields for Business and Person contractors. When adding a new contractor, click the New Business or New Person button to display the proper fields.

Adding Business Contractor Contact Information

Use the Business Contractor form to add service providers that are businesses, such as towing companies or taxi services.

To add a business contractor:

1. From the navigation panel, select **Contractor Rotation** and then select **Contractors**.

The Contractors form for the selected agency appears in the work area, with the General tab in focus. A list of existing contractors displays on the left side of the form.

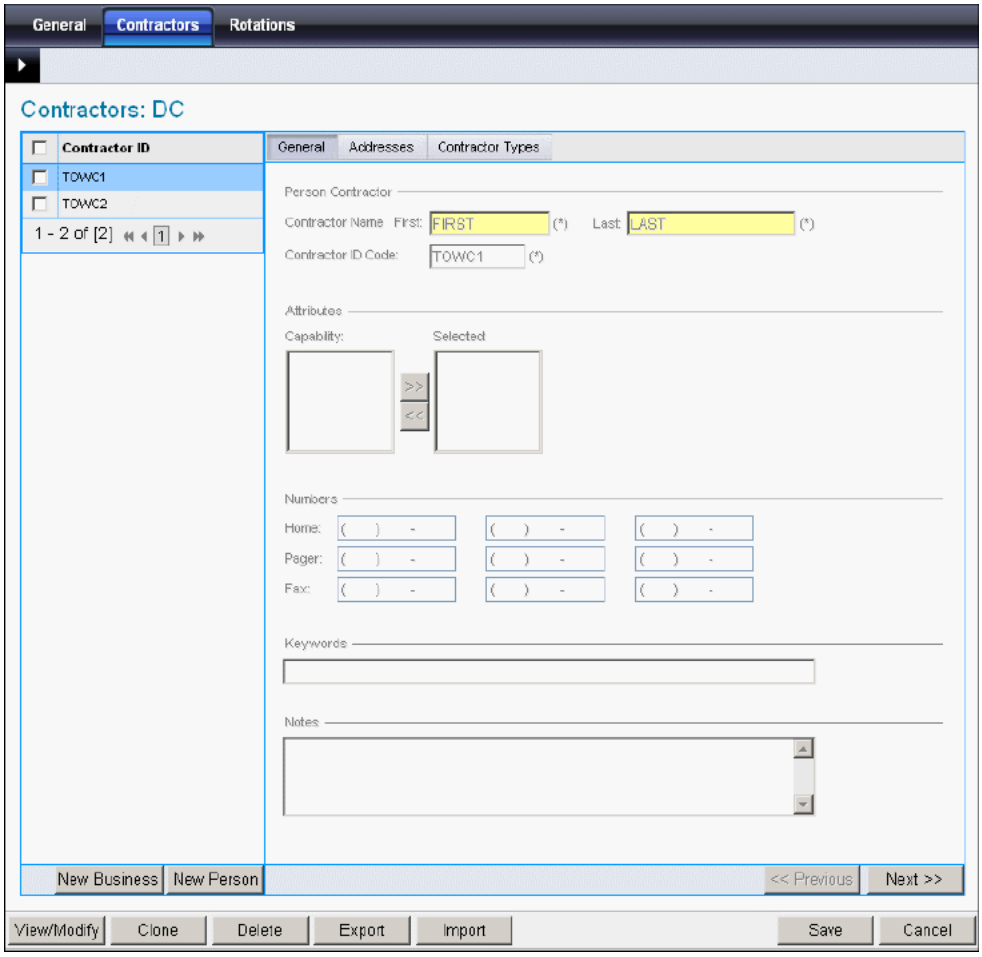


Figure 15-5 Contractor Rotation — Contractors Form

2. Click **New Business**.

The General tab refreshes and the contact information fields become editable. Business Contractor displays at the top of the Primary Work Area.

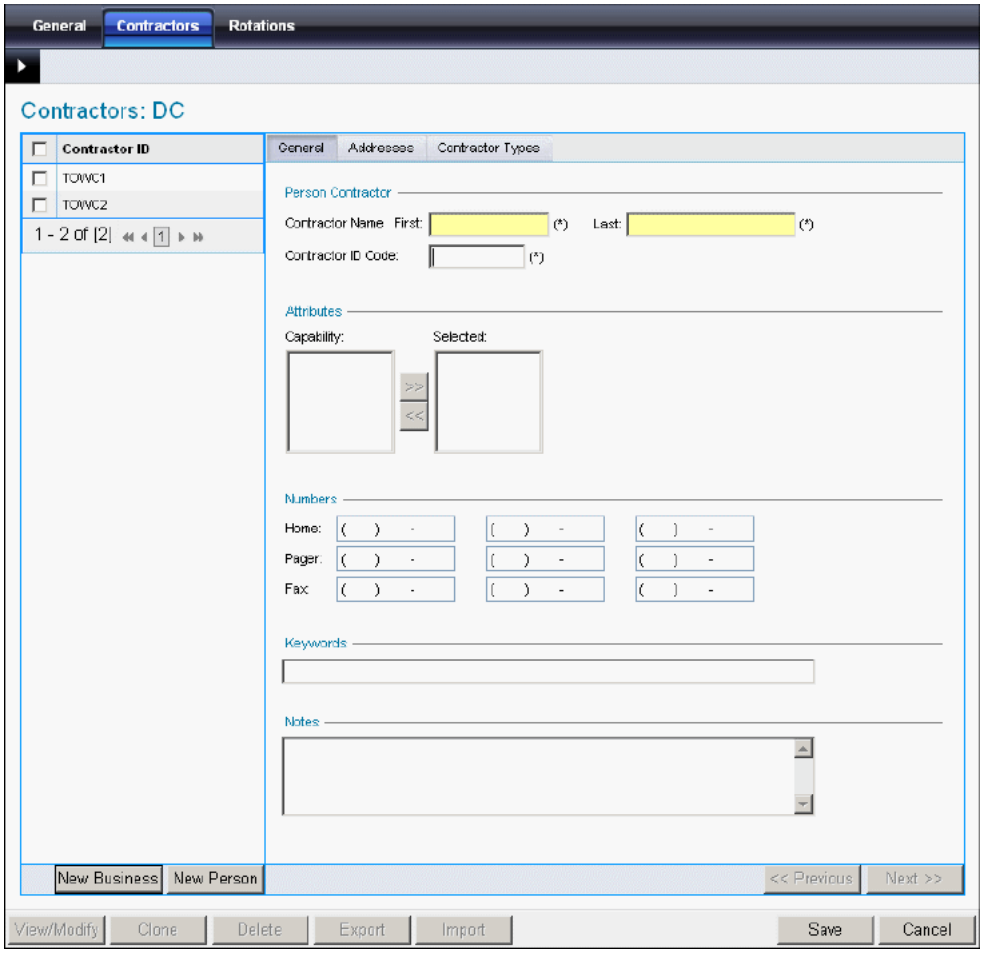


Figure 15-6 Contractors Form — General Tab for New Business Contractor

3. In the Contractor Name field, type the contractor business name.

4. In the Contractor ID Code field, type a unique code for this contractor.

5. In the Owner's Name fields, type the first and last name of the business owner.

6. In the Attributes section, select the Capabilities, Auto Club Affiliations, and Payment Methods that apply to this contractor.

   Capabilities are provisioned on the General tab of the Contractor Rotation form (see "Adding Contractor Capabilities" on page 15-4). Auto club affiliations and payment methods are provisioned on the List and Statute Management form (see "Provisioning Auto Club Affiliations and Payment Methods" on page 15-8).

   To select an item, click its entry in the left box to highlight it, and then use the arrow keys to move it to the Selected box. You can select multiple items by using the Shift-click and Ctrl-click combinations.

7. Continue with "Adding Business Contractor Address Information" on page 15-13.

Adding Person Contractor Contact Information

Use the Person Contractor form to add service providers that are persons, such as judges or detectives.

To add a person contractor:

1. Access the Contractor Rotation Contractors form for the appropriate agency. For instructions, see "Adding Business Contractor Contact Information" on page 15-9.

2. Click **New Person**.

   The General tab refreshes and the contact information fields become editable. Person Contractor displays at the top of the Primary Work Area.

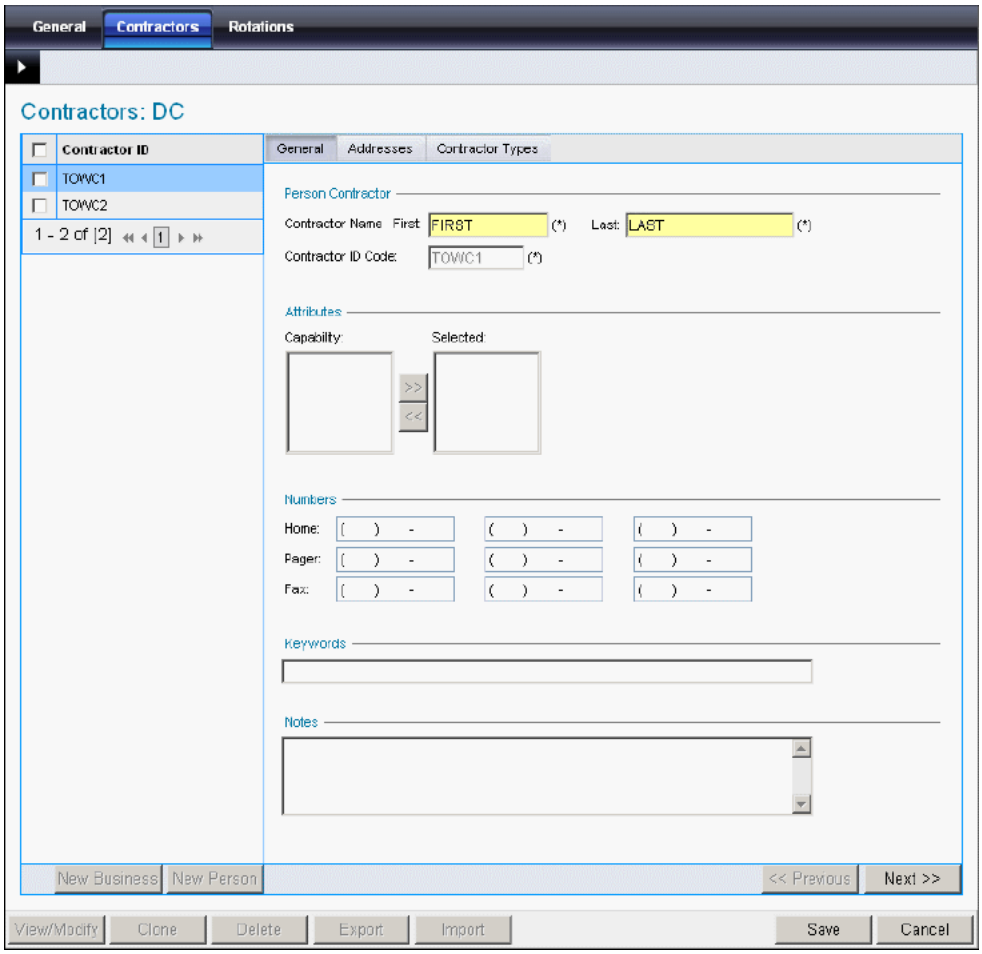


Figure 15-7 Contractors Form — General Tab for New Person Contractor

3. In the Contractor Name fields, type the first and last name of the new contractor.

4. In the Contractor ID Code field, enter a unique code to identify this contractor.

5. In the Capability box, select the appropriate capabilities for this contractor and use the arrow to move them to the Selected box.

6. In the Numbers section, type the contact phone, pager, and fax numbers for this contractor.

7. In the Keywords field, type any unique words that can be used to search for this person.

   Contact information added for contractor rotation is also automatically available in the PremierOne global address book. CAD users can enter these keywords to search for entries in the global address book.

8. Continue with "Adding Person Contractor Address Information" on page 15-14.

Adding Contractor Address Information

Like the General contractor contact information form, the Addresses form displays different fields for Business and Person contractors.

Adding Business Contractor Address Information

To add address information for a business contractor:

1. Complete the contact information on the General tab of the Contractors form. For details, see "Adding Business Contractor Contact Information" on page 15-9.

2. Click the **Addresses** tab.

   The Business Address form appears.

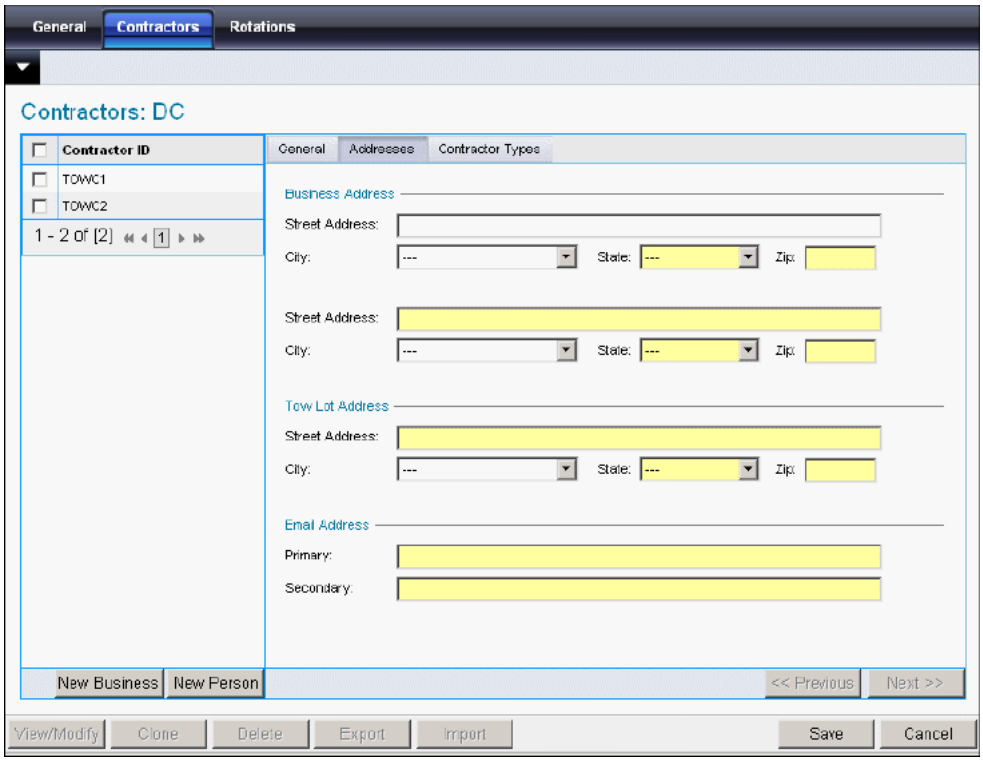


Figure 15-8 Contractors Form — Addresses Tab for New Business Contractor

3. In the Business Address section, type or select the primary Street Address, City, State, and Zip information for the new contractor.

4. In the Business Address section, type or select secondary Street Address, City, State, and Zip information for the new contractor.

5. In the Tow Lot Address section, type or select the Street Address, City, State, and Zip information for the tow lot of the new contractor, if applicable.

6. In the Email Address section, type a primary and secondary email address for the new contractor.

7. Continue with "Setting Contractor Type and Availability" on page 15-15.

Adding Person Contractor Address Information

To add address information for a person contractor:

1. Complete the contact information on the General tab of the Contractors form. For details, see "Adding Person Contractor Contact Information" on page 15-12.

2. Click the **Addresses** tab.

   The Person Address form appears.

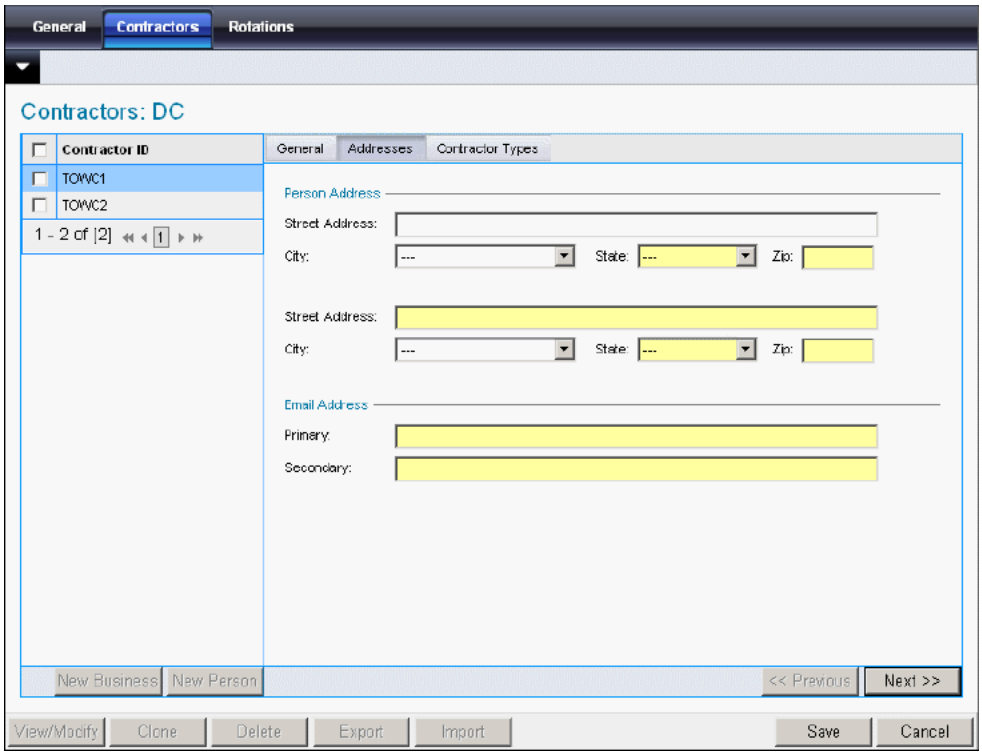


Figure 15-9 Contractors Form — Addresses Tab for New Person Contractor

3. In the Person Address section, type or select the primary Street Address, City, State, and Zip information for the new contractor.

4. In the Person Address section, type or select secondary Street Address, City, State, and Zip information for the new contractor.

5. In the Email Address section, type a primary and secondary email address for the new contractor.

6. Continue with "Setting Contractor Type and Availability" on page 15-15.

Setting Contractor Type and Availability

Use the Contractor Types tab to associate a contractor with one of the Contractor Types defined for the selected agency, and to specify the contractor's days and hours of availability. Use this form for both Business and Person contractors.

To associate a contractor with a Contractor Type:

1. Access the Contractor Rotation Contractors form. For instructions, see "Adding Business Contractor Contact Information" on page 15-9.

2. Click the **Contractor Types** tab.

   The Contractor Types form appears.

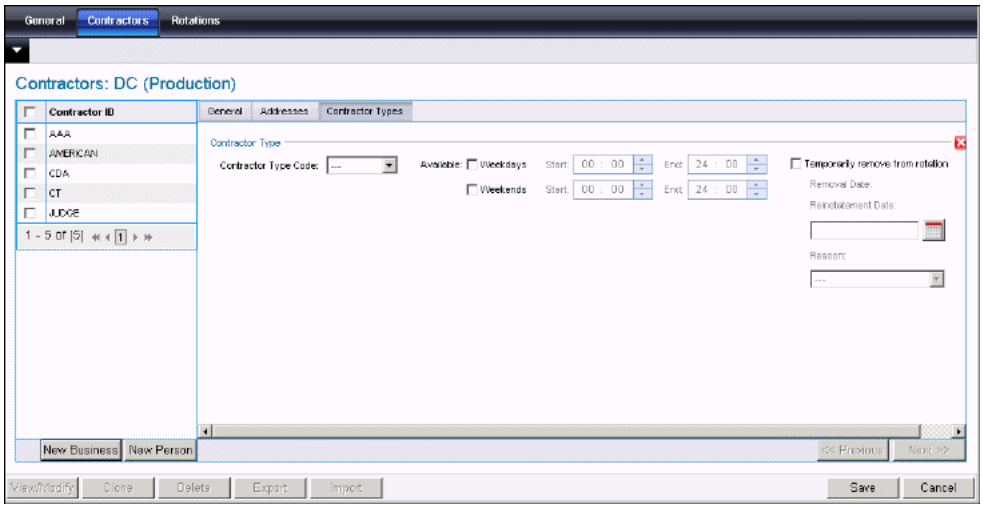


Figure 15-10 Contractors Form — Contractor Types Tab

3. From the Contractor Type Code list, select the appropriate Code for the new contractor.

> **NOTE**
> Contractor type codes are added from the GIS data.

4. In the Available fields, indicate the contractor's availability by selecting the check box for Weekdays, Weekends, or both.

5. In the Start and End fields, select the starting and ending times that the contractor is available on the selected days. These fields use a 24-hour clock.

6. Select the **Temporarily remove from rotation** check box if you need to remove a contractor from the rotation for a period of time.

7. In the Reinstatement Date field, type or select the date when the contractor will again be available to rejoin the rotation.

8. From the Reason list, select the reason for the contractor's temporary removal from the rotation. Options are Suspended and Unavailable.

9. Click **Save**.

NOTE

After you click Save, the Removal Date field displays the date of the contractor's removal from the rotation. This field is read-only.

Configuring Contractor Rotations

Use the Rotations form when your agency wants to add or modify information about a new or existing contractor rotation list. When you provision contractor rotations, you enter information on the Rotations form.

CAD users can select a contractor from the rotation list that displays on the Contractor Request form.

You can add, modify, import, export, clone, and delete contractor rotation information. For details on importing, exporting, cloning, and deleting, see "Working With Configuration Items" on page 2-9.

Adding New Rotations

You can create an ordered list of contractors who are available to provide service for a specific geographic area.

To add a rotation:

1. From the navigation panel, select **Contractor Rotation** and then select **Rotations**.

The Rotations form for the selected agency appears in the work area, with existing rotations displayed in the left panel.

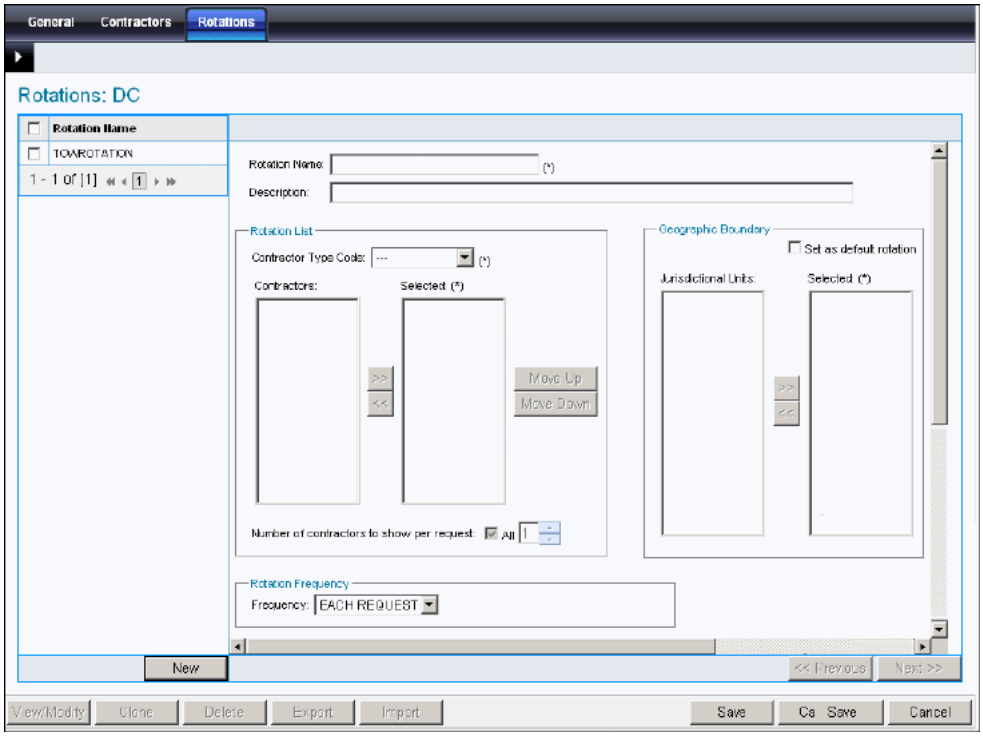


Figure 15-11 Contractor Rotations Form

2. At the bottom of the Rotation Name column, click **New**.

   The Rotations form appears (see Figure 15-11).

3. In the Rotation Name field, type a name for this rotation.

4. In the Description field, type a description of this rotation.

5. From the Contractor Type Code list, select the Contractor Type Code for this rotation list.

In the Rotation List section, the Contractors box displays contractors with the selected Contractor Type Code. In the Geographic Boundary section, the Jurisdictional Units box displays (in alphabetical order) all the jurisdictional units that have been defined in GIS for the selected contractor type.

NOTE

With the exception of the default rotation, each rotation must be assigned to at least one jurisdictional boundary.

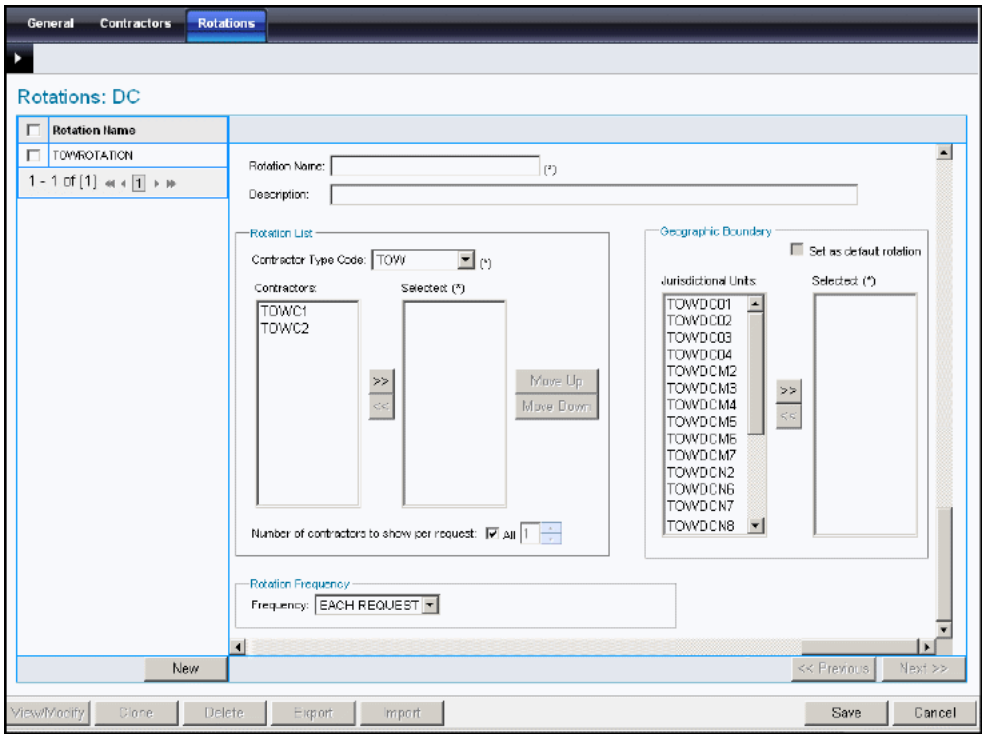


Figure 15-12 Contractor Rotations Form — Contractor Type Code Selected

6. In the Contractors box, select each contractor that you want to add to the rotation and use the arrow to move the contractor to the Selected box.

   You can select multiple contractors by using the Shift-click and Ctrl-click combinations.

   In the Selected box, you can re-order the list by clicking a contractor and then using the Move Up or Move Down buttons to change the highlighted contractor's position in the list.

7. In the Number of contractors to show per request field, set the number of contractors you want the system to display for each contractor request, or click the **All** check box to display all contractors on the list for each request.

8. In the Jurisdictional Units box, click the jurisdictional units that you want the rotation list to include and use the arrow button to move the jurisdictional units to the Selected box.

9. In the Rotation Frequency section, set the Frequency field to indicate how often this list should rotate: Each Request, Daily, Weekly, Monthly, Yearly, or Static.

   Depending on your selection, additional fields display for defining the rotation frequency as follows:

   a. Each Request – No additional fields. The list rotates for each request.

   b. Daily – Complete the following:

      - Time: Using 24-hour (military) format, enter the time of day that the list should rotate.
      - Every __ day(s): Enter the number of days between rotations.
      - For example, every *2* days.
      - Every weekday: Select this check box to rotate the list each weekday.

   c. Weekly – Complete the following:

      - Time: Using 24-hour (military) format, enter the time of day that the list should rotate.
      - Recur every __ week(s) on: Enter the number of weeks between rotations.

        For example, every *2* weeks.
      - Day check boxes: Select the day of the week on which to rotate the list.

   d. Monthly – Complete the following:

      - Time: Using 24-hour (military) format, enter the time of day that the list should rotate using military time.
      - Day __ of every __ month(s): Enter the day of the month to rotate the list and the number of months between rotations.

        For example, day *5* of every *2* months.
      - The __ __ of every __ month(s): Select a specific day of the week and week of the month for the list to rotate, and the number of months between rotations.

        For example, the *first Monday* of every *2* months.

   e. Yearly – Complete the following:

      - Time: Using 24-hour (military) format, enter the time of day that the list should rotate using military time.
      - Every __ __: Select the month and the day of the month to rotate the list.

For example, every *February 5*.

- The __ __ of __: Select a specific day of the week, week of the month, and month for the list to rotate.

  For example, the *first Monday* of *March*.

f. Static – No additional fields. The list does not rotate.

10. Click **Save**.

Creating Default Rotations

For each contractor type you can create a rotation list that will display by default when a geographical beat cannot be found for the location of a contractor request. This might occur when the incident address cannot be verified, or if a contractor request is needed outside of the agency's jurisdiction. Unlike other contractor rotations, the default rotation is not associated with any geographical boundaries.

To create a default rotation:

1. Create a new rotation list as described in "Adding New Rotations" on page 15-16.
2. In the Geographic Boundary section, click the **Set as default rotation** check box.

   The Jurisdictional Units list becomes unavailable.

   NOTE
   You can only have one default rotation per contractor type.

3. Click **Save**.

CHAPTER 16

Customizing the User Interface

The Customization configuration item contains the following items:

- Mobile – Where you customize the Mobile service areas, Action bar, Options menu, Navigation bar, Status bar, logos, and Command line. For details, see “Configuring the Mobile Interface” on page 16-2.
- Mobile Speech – Where you specify the fields that are enabled for text-to-speech. For details, see “Configuring Mobile Text-to-Speech” on page 16-18.
- Function Keys – Where you customize the function keys for both CAD and Mobile. For details, see “Configuring Function Keys for CAD and Mobile” on page 16-28.
- Data Elements – Where you customize the labels that appear on the PremierOne application interfaces, such as Area, Beat, City, and so on. For details, see “Configuring Data Elements” on page 16-34.

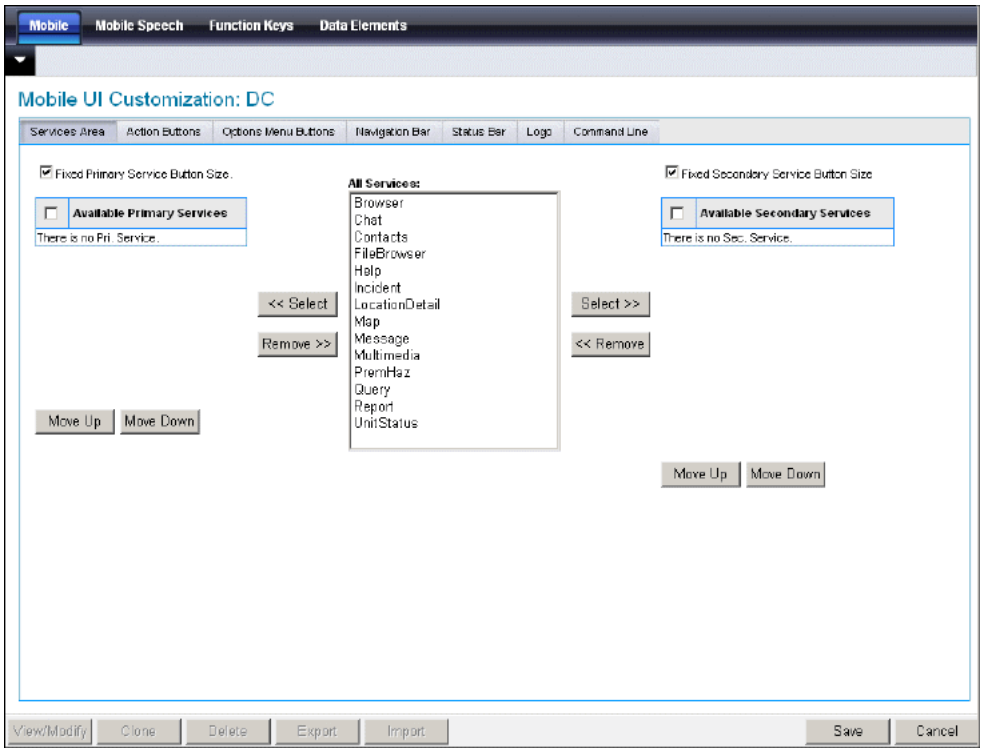


Figure 16-1 Mobile UI Customization Form

Configuring the Mobile Interface

Use the Mobile UI Customization form to configure Primary and Secondary services, the Action bar, the Navigation bar, the Status bar, the Options buttons, the Login logo, and the Command line for the Mobile interface. For details see the *PremierOne Mobile User Guide*. Configuration settings do not take affect until the Mobile client is synchronized with the Mobile server.

The Mobile UI Customization form contains seven sub-tabs to configure the Mobile user interface. The tabs are:

- Services Area – Used to specify the buttons that are used in the primary and secondary services areas in the Mobile interface.
- Action Buttons – Used to specify the action buttons that are used in the Mobile interface.
- Options Menu Buttons – Used to specify the Option Menu buttons that are used in the Mobile interface.
- Navigation Bar – Used to specify the items that are on the Navigation bar in the Mobile interface.
- Status Bar – Used to specify the items that are on the Status bar in the Mobile interface.
- Logo – Used to specify the logos for the Mobile Address book and the Login icons.
- Command Line – Used to enable or disable a command line on the Mobile interface.

Mobile Interface Window Example

You can customize the Mobile user interface to meet your needs. The following figure shows a Mobile window configured with many of the items that you can configure. For more information see the *PremierOne Mobile User Guide*.

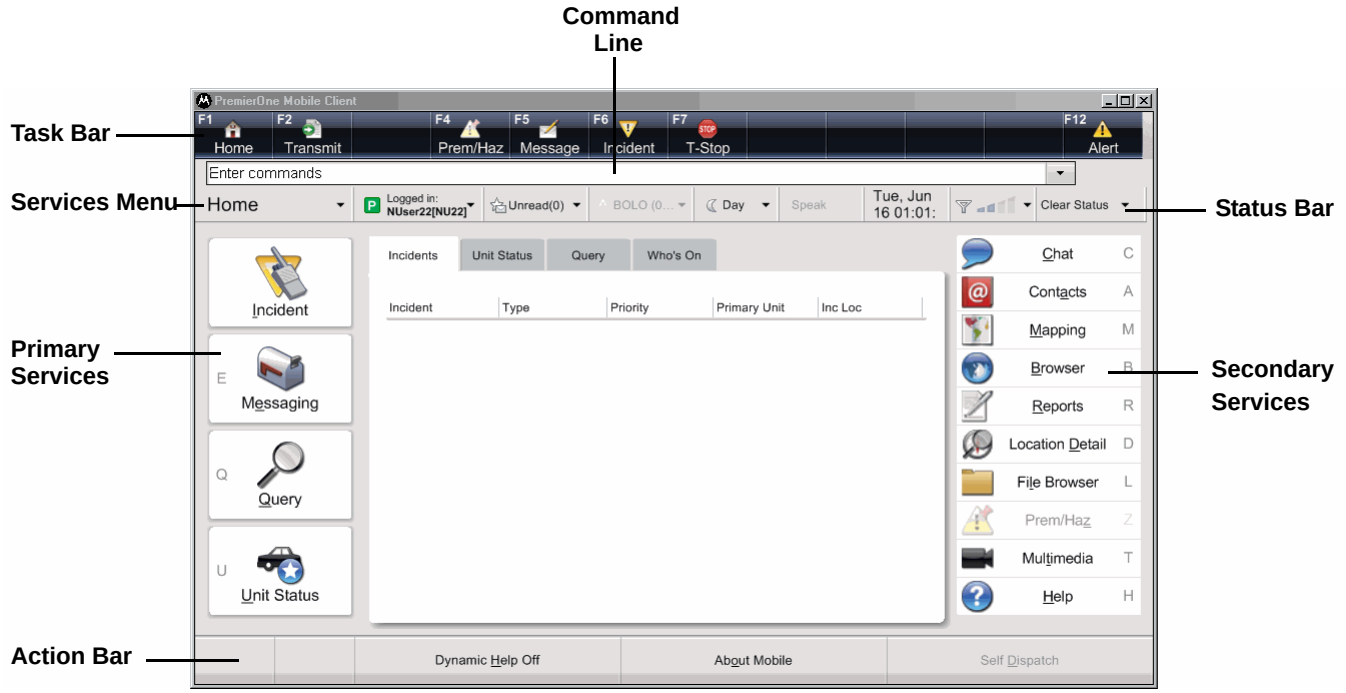


Figure 16-2 Mobile Window

Configuring the Mobile Services Areas

Use the Services Area subtab to configure the primary and secondary service buttons on the Mobile window. You can add buttons, remove buttons, and arrange the button order for the Primary or Secondary services.

If no provisioning has been done, a default set of menus displays in the Mobile client, and a notification box states that the default values are being used.

For the location of primary services in the Mobile window, see "Configuring the Mobile Interface" on page 16-2.

To configure the Primary Services area of the Mobile window:

1. From the navigation panel, select **Customization**, and then select **Mobile**.

   The Mobile UI Customization form appears with the fields and buttons dimmed.

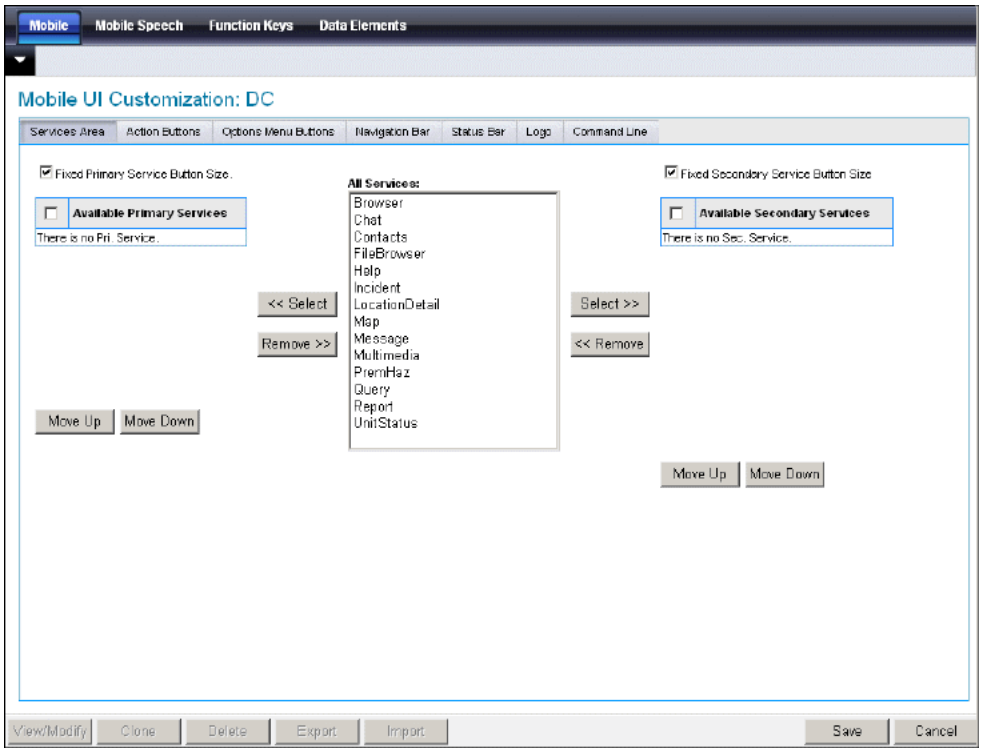


Figure 16-3 Mobile UI Customization form – Services Area Tab

2. Click the **View/Modify** button.

3. From the All Services list, select a service, such as **Incident**, and then click the **Select** button.

   The selected service is added to the Available Primary Services list.

4. Continue to add services as required.

You are limited to four primary services for the Mobile window if the **Fixed Primary Service Button Size** check box is selected. If the fixed primary service button size is not selected, the button is automatically sized to fill the entire area of the total number of buttons is less than four.

Selecting the check box fixes the button size so that the buttons are easily selected using the touch screen feature in Mobile.

5. To set the order of the primary services, select the service that you want to move. Do not select the check box.

6. Click the **Move Up** or **Move Down** button to move the service to the new location.

To configure secondary services:

1. From the All Services list, select a service, such as **File Browser**, and then click the **Select** button located to the right of the All Services list.

   File Browser is added to the Available Secondary Services list.

2. Continue to add services as required.

   You are limited to nine secondary services for the Mobile window if the **Fixed Secondary Service Button Size** check box is selected. If the fixed secondary service button size is not selected, the button is automatically sized to fill the entire area of the total number of buttons is less than four.

3. To set the order of the secondary services, select the service that you want to move. Do not use the check box.

4. Click the **Move Up** or **Move Down** button to move the service to the new location.

5. Click **Save**.

Configuring the Mobile Action Bar

Use the Actions subtab of the Customization form to configure the Action bar buttons on the Mobile window. You can add buttons, remove buttons, and arrange the button order for the Action bar.

The items available on the Mobile Action bar are based on the services and pages that are selected. For example, if an Incident is selected as the current service, and the View Incident window is active, the list of actions that can be performed is different from those that could be performed if a Message is active while viewing a new BOLO message. You can configure which items are available for each Primary or Secondary service.

The Action bar in the Mobile window is located by default at the bottom of the Mobile window. For the location of the Action bar on the Mobile window, see “Configuring the Mobile Interface” on page 16-2.

To configure the Mobile Action bar:

1. Access the form for Mobile Customization. For instructions, see "Configuring the Mobile Services Areas" on page 16-4.

2. In the Mobile UI Customization form, select the Action Buttons tab.

   The Actions form appears.

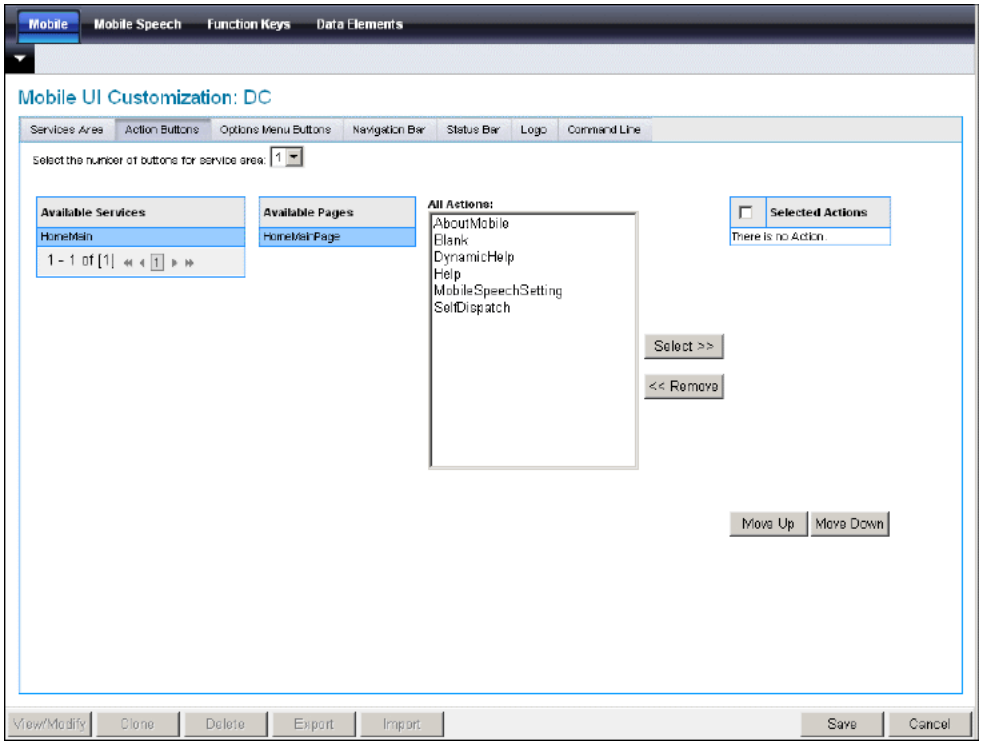


Figure 16-4 Mobile UI Customization form – Actions Tab

3. If the fields and buttons are all dimmed, click the **View/Modify** button.

4. From the Select the number of buttons for the action bar list, select the number of buttons you want to display in the Mobile Action bar. The maximum number is eight.

5. In the Available Services list, select a service, such as an Incident.

   If you have not configured the Services Area tab information, there may be no available services, as this is a listing of the Primary and Secondary services available on the Mobile window.

   The list of available pages for the selected service displays in the Available Pages list. This list changes based on the service that was selected.

NOTE

To enable MVX Integration with Mobile, select Incident – Incident: Main Assign– Send to MVX.

6. In the Available Pages list, select a page, such as ViewIncident.

   The list of actions that are available for the combination of the service and page that you selected display in the All Actions list.

7. In the All Actions list, select an action, and then click the **Select** button.

   The action you chose is added to the Selected Actions list. In this example, LocateOnMap, Print, and ClearIncident were selected.

> **NOTE**
> The default set of Action buttons do not appear in the Selected Actions list. If you want to remove a button that is not on the list (default button), you must first add it to the Selected Actions list, and then remove it.

8. To reorder the actions, select an action and click the **Move Up** or **Move Down** button to move the action as needed. Top to bottom here corresponds to left to right on the Mobile Action bar.

9. Continue to add action as needed for each service. Remember, you can have a maximum of eight action buttons for each service and page combination. If more than eight are selected, only the first eight are displayed.

10. When you have the actions you want and have put them in the order you want, click **Save**.

A Mobile client synchronization must be done before the changes take place in the Mobile client.

Configuring Mobile Option Buttons

Use the Options subtab of the Customization form to configure the options that are available from the Options buttons on the Mobile window. You can add buttons, remove buttons, and arrange the button order for the Options button area.

> **NOTE**
> In the Mobile client, if there are no configured Option buttons, the Option button does not appear on the Action bar. However, when you configure (add) the first Option button, the Options button automatically appears in the right-most location on the Action bar. If eight Action buttons are already configured for the Action bar, when you add the first Option button, the last (right) Action button is replaced by the Options button.

Example of Mobile Options Buttons

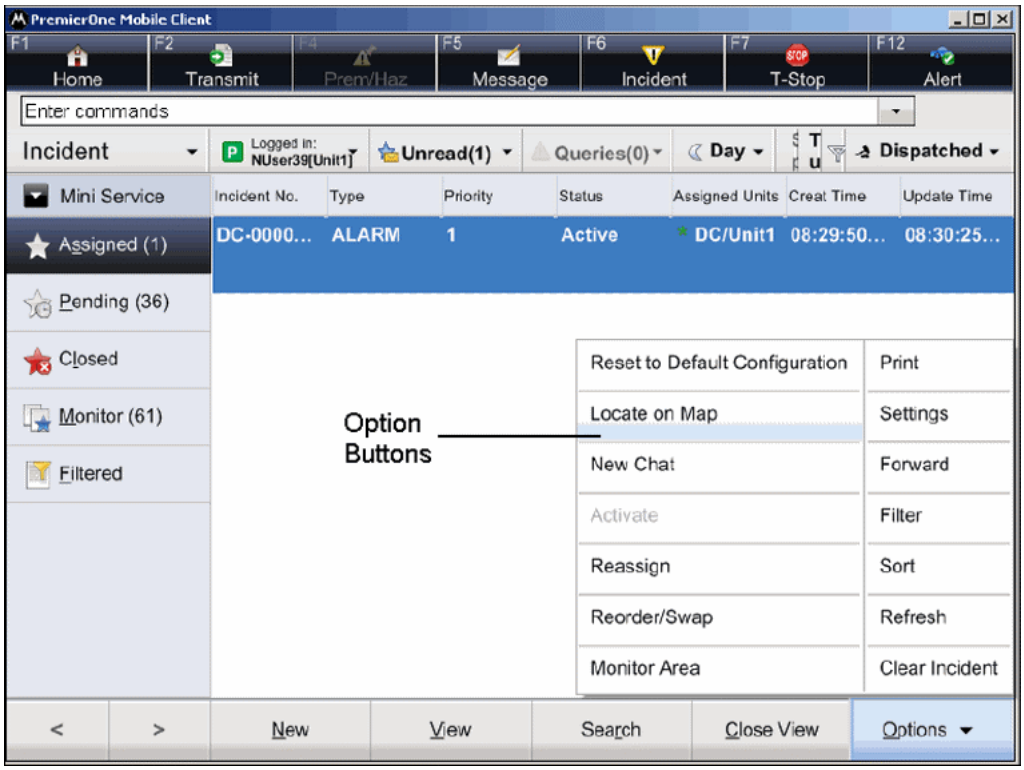


Figure 16-5 Mobile Window – Option Buttons

To select options for inclusion on the Mobile Options Menu Button area:

1. Access the form for Mobile Customization. For instructions, see "Configuring the Mobile Services Areas" on page 16-4.

2. Select the Options Menu Buttons tab.

   The Options Configuration form appears.

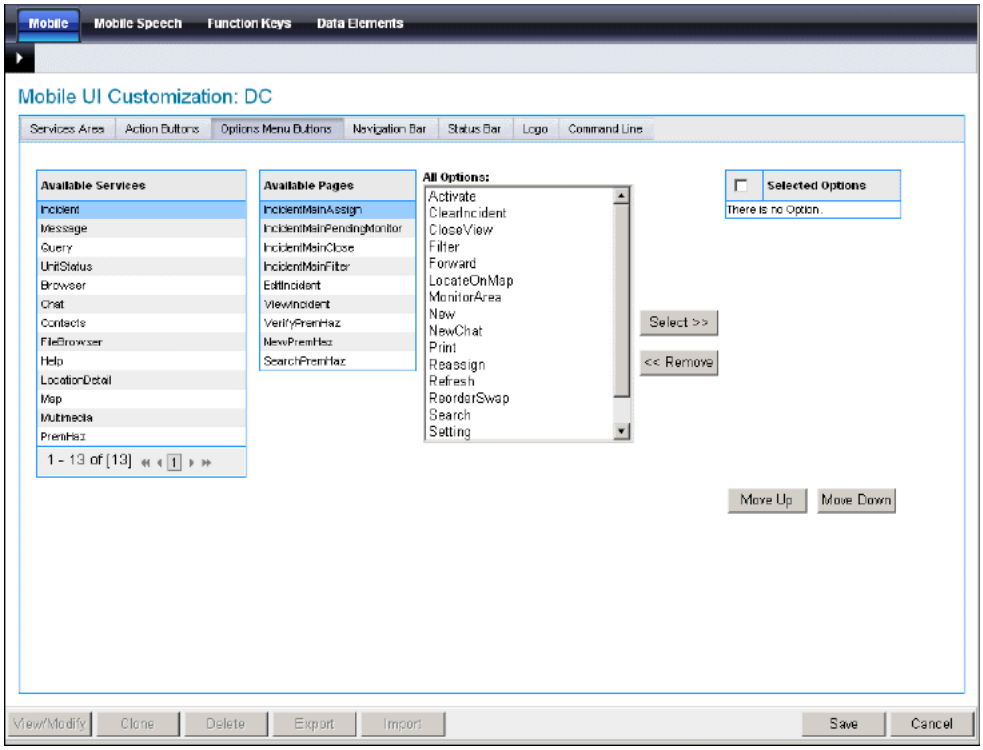


Figure 16-6 Mobile UI Customization Form – Options Menu Button Tab

3. If the fields and buttons are all dimmed, click the **View/Modify** button.

4. In the Available Services list, select a service. This is a listing of the Primary and Secondary services available on the Mobile window.

   The list of available pages that can display for a service are shown in the Available Pages list.

5. In the Available Pages list, select a page.

   The list of options that is available for the combination of the service and page that you selected display in the All Options list.

6. In the All Options list, select an option and then click the **Select** button. You can put up to 24 options for each page. The options display in three columns of eight.

   The option you chose is added to the Selected Options list.

7. To reorder the options, select the option that you want to move, and then click the **Move Up** or **Move Down** button to move the buttons as needed.

   The order from top to bottom in the Selected Options list results in the following order in the Mobile window options area, where 1 is at the top of the list in the Selected Options list.

24	16	1
23	15	2
22	14	3
21	13	4
20	12	5
19	11	6
18	10	7
17	9	8

Figure 16-7 Options Button Order In The Mobile Window

8. Continue to add options as needed for each service.

> **NOTE**
> If no options are configured, the Options button does not display on the Actions bar. The result is that one more Action button position is available on the Action bar.
>
> The default set of Options buttons do not appear in the Selected Options list. If you want to remove a default button, you must first add it to the Selected Options list, and then remove it.

9. Click **Save**.

Configuring the Mobile Navigation Bar

Use the Navigation subtab of the Mobile form to configure the Navigation bar on the Mobile interface. You can add buttons, remove buttons, and arrange the button order on the Mobile Navigation bar. For Navigation bar location details, see “Configuring the Mobile Interface” on page 16-2.

The Navigation buttons in the Mobile window are located by default at the left side of the Mobile window, and are displayed after a primary or secondary service is selected. Which buttons display in the Navigation bar are dependent upon the primary or secondary service that was selected in the Mobile window. Therefore, you must configure navigation buttons for each service.

Example of Mobile Navigation Bar

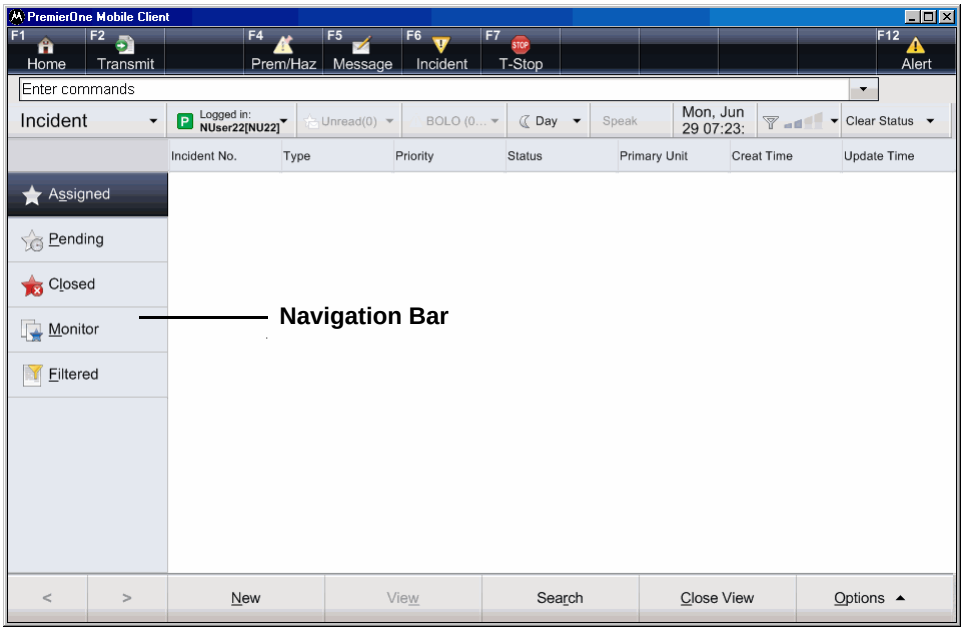


Figure 16-8 Mobile User Interface – Navigation Bar

To select Navigation bar items for the Mobile Navigation bar:

1. Access the form for Mobile Customization. For instructions, see "Configuring the Mobile Services Areas" on page 16-4.

2. Select the Navigation Bar tab.

   The Navigation Bar Configuration form appears.

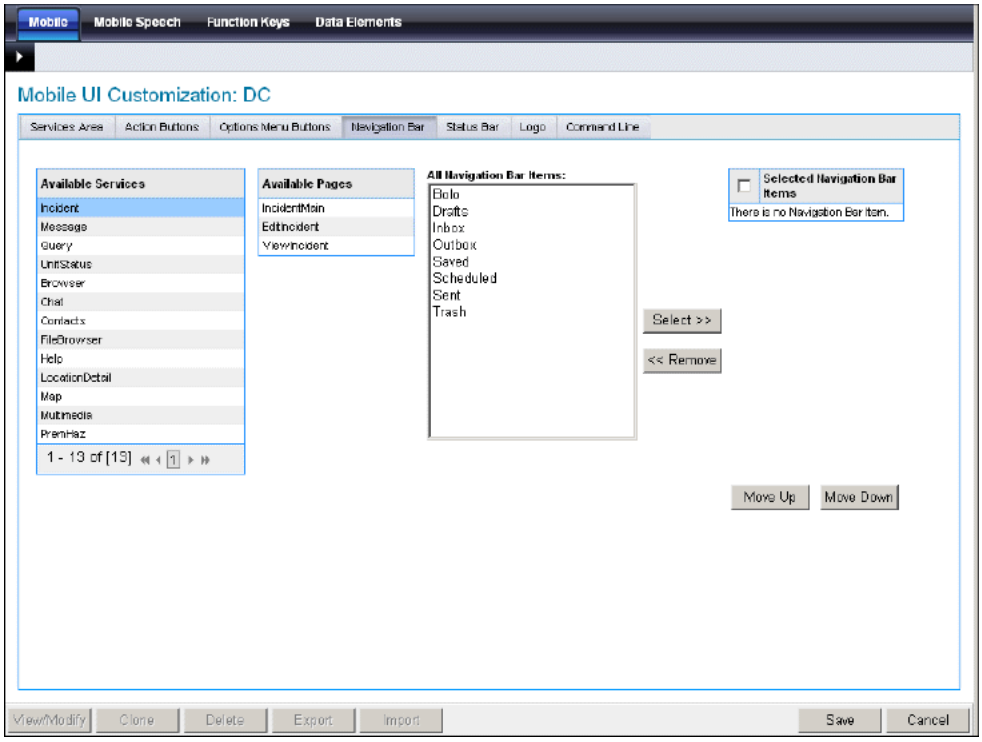


Figure 16-9 Navigation Bar Form

3. If the fields and buttons are all dimmed, click the **View/Modify** button.

4. In the Available Services list, select a service. This is a listing of the Primary and Secondary services available on the Mobile window.

   The list of available pages that can display for a service are shown in the Available Pages list.

5. In the Available Pages list, select a page.

   The list of Navigation bar items that is available for the combination of the service and page that you selected display in the All Navigation Bar Items list.

NOTE

For Incident Services, place the Summary tab at the top of the list of selected Navigation items so it will be available by default when incident forms, including traffic stop, are opened.

6. In the All Navigation Bar Items list, select an item and then click the **Select** button.

   The item you chose is added to the Selected Navigation Bar Items list.

7. To reorder the Navigation items, select the item that you want to move, and then click the **Move Up** or **Move Down** button to move the item as needed.

8. Continue to add items as needed for each service.

9. Click **Save**.

NOTES

At the present time, only Messaging and Incidents support Navigation bar customization.

The default set of Action buttons by default do not appear in the Selected Actions list. If you want to remove a default button, you must first add it to the Selected Actions list, and then remove it.

Configuring the Mobile Status Bar

Use the Status subtab of the Customization form to configure the Status bar for the Mobile window. You can add buttons, remove buttons, and arrange the button order for the Mobile Status bar. For Status bar location details, see “Configuring the Mobile Interface” on page 16-2.

To configure the Mobile Status bar:

1. Access the form for Mobile Customization. For instructions, see “Configuring the Mobile Services Areas” on page 16-4.

2. Select the Status Bar tab.

The Status Bar Configuration form appears.

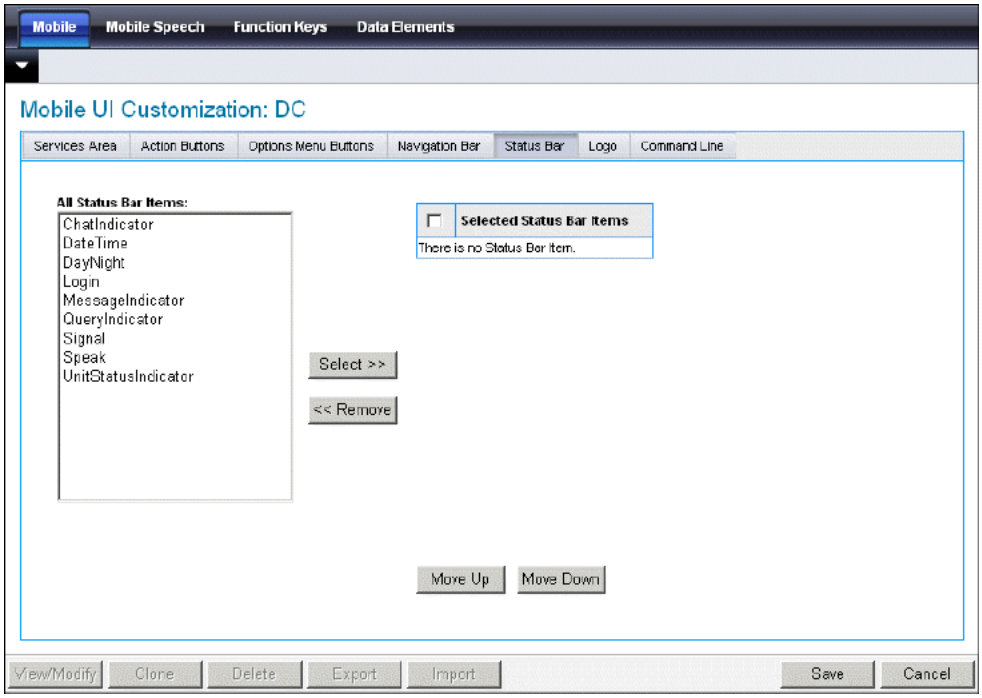


Figure 16-10 Mobile UI Customization form – Status Bar Tab

3. If the fields and buttons are all dimmed, click the **View/Modify** button.
4. From the All Status Bar Items list, select an item, and then click the **Select** button.

   The item you chose is added to the Selected Status Bar Items list.
5. Continue to add items as needed.
6. To reorder the Mobile Status bar items, select the item that you want to move, and then click the **Move Up** or **Move Down** button to move the items as needed.
7. Click **Save**.

Configuring the Mobile Address Book and Login Icons

Use the Mobile Customization Logo subtab to configure the Mobile Address Book icon and the Login icon.

To configure the login icon:

1. Access the form for Mobile Customization. For instructions, see "Configuring the Mobile Services Areas" on page 16-4.

2. Select the Logo tab.

   The Logo Customization form appears.

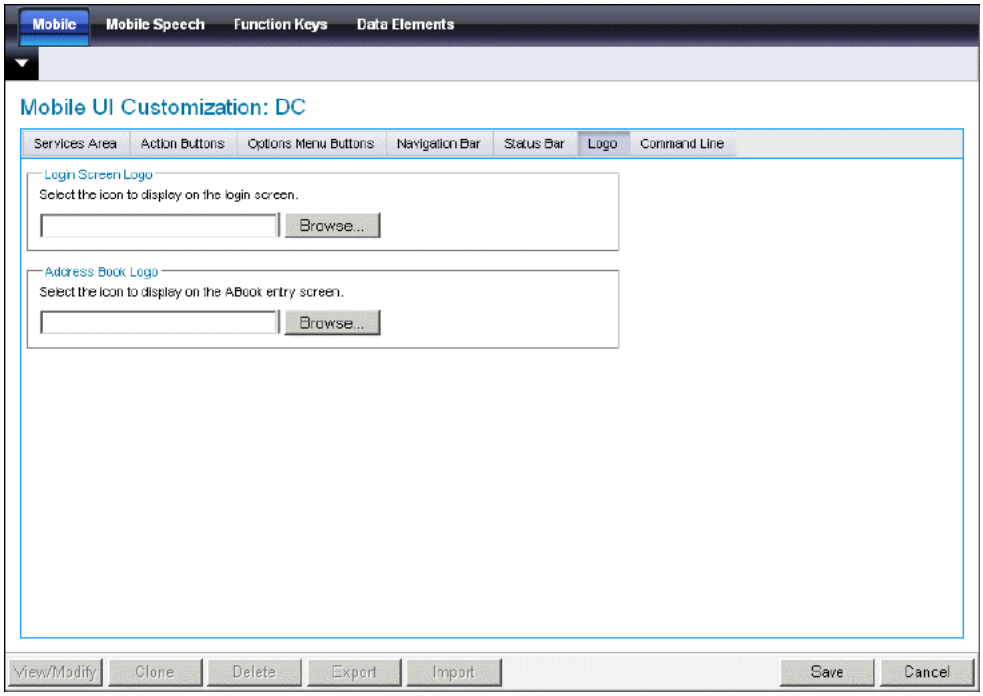


Figure 16-11 Mobile UI Customization form – Logo Tab

3. If the fields and buttons are all dimmed, click the **View/Modify** button.

4. In the Login Screen Logo area, click the **Browse** button to navigate and select the icon you want to display on the Mobile login dialog field.

   For the best results, the icon should have the following characteristics:

   - Format – jpg, png, gif.
   - Size – 150 by 150 pixels

If the size and resolution are not optimized for the Mobile window, the icon is converted to fit. However, converting and resizing bitmap graphics results in a lower quality appearance. The icons are displayed in 150 by 150 pixels. To get the best resolution results, you should create icons with that resolution.

NOTE
The icons must be pre-loaded to:

`C:\Program Files\Motorola\PremierOne\MobileClient\uixml\Default\image\LoginLogo` in the Mobile client.

5. Click **Save**.

To configure the logo:

1. Access the form for Mobile UI Customization. For instructions, see "Configuring the Mobile Services Areas" on page 16-4.
2. Select the Logo tab.

   The Logo Customization form appears (see Figure 16-11).
3. If the fields and buttons are all dimmed, click the **View/Modify** button.
4. In the Address Book Logo area, click the **Browse** button to navigate and select the icon you want to display.

   For the best results, the icon should have the following characteristics:

   - Format – jpg, png, gif.
   - Size – 150 by 150 pixels

   If the size and resolution are not optimized for the Mobile window, the icon is converted to fit. However, converting and resizing bitmap graphics results in a lower quality appearance. The icons are displayed in 150 by 150 pixels. To get the best resolution results, you should create icons with that resolution.

NOTE
The icons must be pre-loaded to:
`C:\Program Files\Motorola\PremierOne\MobileClient\uixml\Default\image\ABookEntryIcon` in the Mobile client.

5. Click **Save**.

Configuring the Mobile Command Line

The command line can be used to enter commands on the Mobile window. This is often faster than using the buttons on the Mobile user interface to accomplish tasks. You can choose to enable or disable the use of the command line.

To enable or disable the command line:

1. Access the form for Mobile Customization. For instructions, see "Configuring the Mobile Services Areas" on page 16-4.

2. Select the Command Line tab.

   The Command Line form appears.

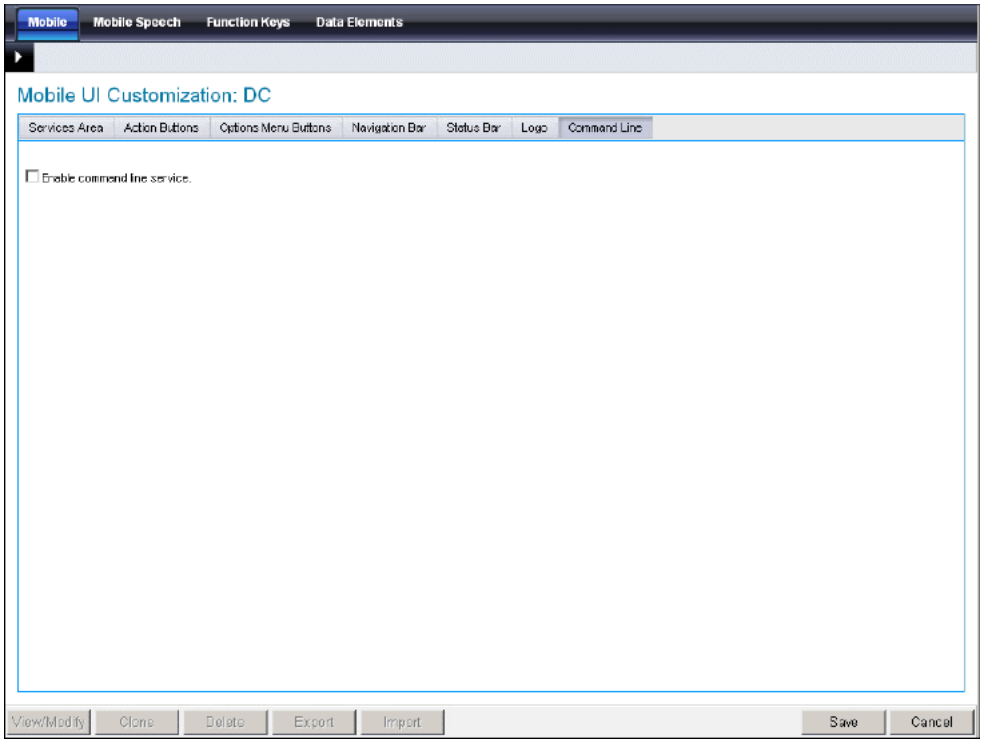


Figure 16-12 Mobile Command Line Form

3. Click the **View/Modify** button.

4. Select or clear the **Enable command line service** check box to enable or disable the service.

5. Click **Save**.

Configuring Mobile Text-to-Speech

Use the Mobile Speech configuration item to enable the Text-to-Speech feature and to select the fields that you want to be played as text-to-speech. The Text-to-Speech feature speaks all selected fields when the Mobile user enables Text-to-Speech.

This window also has a list where you select the voice that speaks when text-to-speak is used.

When you configure mobile speech, you enter information on four tabs of the Mobile Speech form:

- Query – Where you select specific query fields from the listed query types that you want to be played as text-to-speech.
- Incident Management – Where you select the incident fields that you want to be played as text-to-speech.
- Messaging – Where you select the messaging fields that you want to be played as text-to-speech.
- BOLO – Where you select the BOLO fields that you want to be played as text-to-speech.

Configuration settings do not take affect until the Mobile client is synchronized with the Mobile server.

Enabling Text-To-Speech

You access the Mobile Speech form from the navigation panel.

To enable text-to-speech:

1. From the navigation panel, select **Customization**, and then select **Mobile speech**.

   The Mobile Speech form appears. The top of the form is where you enable text-to-speech.

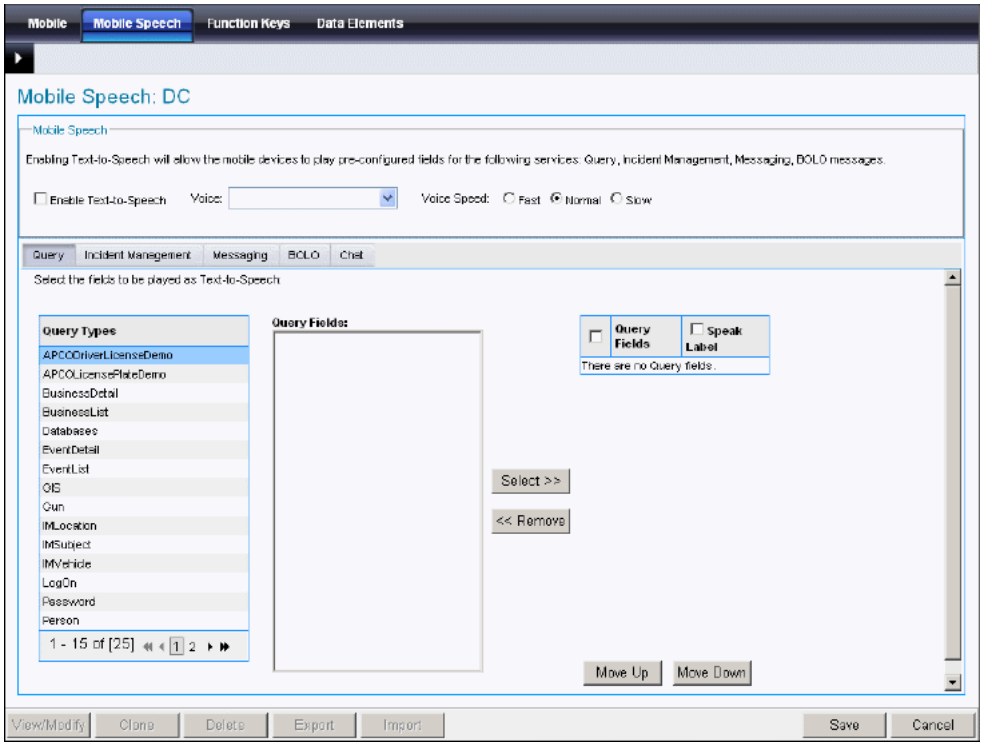


Figure 16-13 Mobile Speech Form

2. Click **View/Modify**.
3. In the Mobile Speech section, select the **Enable Text-to-Speech** check box.
4. Click **Save**.

Selecting the Speaking Voice

If you want to select a voice other than the default for text-to-speech windows, use the following procedure.

To select the speaking voice:

1. From the navigation panel, select **Customization**, and then select **Mobile speech**.

   The Mobile Speech form appears. The top of the form is where you select the voice that speaks during text-to-speech.

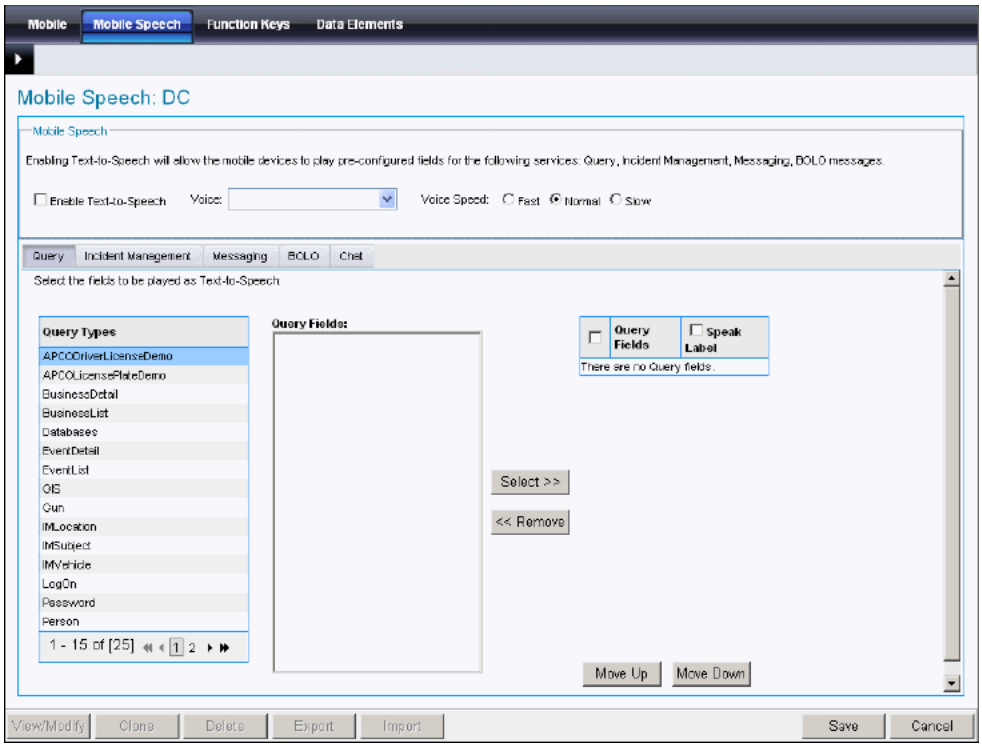


Figure 16-14 Mobile Speech Form

2. Click **View/Modify**.

3. In the Mobile Speech section, select the **voice** from the Voice list.

4. If the list does not contain the voice you want, you must add it. See "Adding Voices" on page 16-21.

5. In the Voice Speed area, select the speed that you want.

6. Click **Save**.

Adding Voices

If the speaking voice is not available from the Voices list, you must add the voice to make it appear on the list.

NOTE

If the Speech SDK is not installed on the client, and you configure a voice in Provisioning other than the default voice, the default is used in the client.

To add voices to the Voices list on the server:

1. Before you begin, the Microsoft speech SDK must be installed on the Mobile clients to provide the voices. See the following link for installation instructions.

   http://www.microsoft.com/downloads/en/details.aspx?FamilyId=5E86EC97-40A7-453F-B0EE-6583171B4530&displaylang=en

2. Open and edit the following XML file on the server.

   ```
   C:\Program
   Files\Motorola\PremierOne\PremierOneAdminConsole\bin\
   Config\MobileSpeechConfig.xml
   ```

3. Edit the **voices** section in the XML file to add voices.

   Example:

   ```
   <?xml version="1.0" encoding="utf-8"?>

   <TextToSpeechConfig xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
   XMLSchema">

     <Voices>

       <Item name="Microsoft Sam"></Item>

       <Item name="LH Michael" ></Item>

       <Item name="LH Michelle" ></Item>

     </Voices>

   </TextToSpeechConfig>
   ```

4. Save the file and exit.

Selecting Query Fields

Use the Query tab to choose which fields from each query type that you want to be played as text-to-speech.

To select query fields:

1. Access the form for Mobile Text-To-Speech. For instructions, see "Configuring Mobile Text-to-Speech" on page 16-18.

   The Mobile Speech form appears (see Figure 16-14).

2. Select the Query subtab.

3. In the Query Types box, select a query type.

   The fields associated with that query type appear in the Query Fields box.

4. From the Query Fields box, select one or more query fields to be played as text-to-speech. You can select more than one field by holding down the **Ctrl** key while you click each field. When you have selected all the fields you need, click **Select**.

   The fields you selected appear in the Query Fields list on the right.

5. To have the speech reader read both the field label and the value of the field, select the **Speak Label** check box for each field.

6. To change the order in which the fields will be read by the speech reader, select a field from the Query Fields list, and then click **Move Up** or **Move Down**. Repeat this step until the fields are in the order you want them read.

   You may need to scroll down to see the Move Up and Move Down buttons.

7. Repeat this procedure for each query type you want to configure for text-to-speech.

8. Click **Save**.

Selecting Incident Management Fields

Use the Incident Management subtab to choose the incident fields you want to be played as text-to-speech.

To select incident management fields:

1. Access the form for Mobile Text-To-Speech. For instructions, see "Configuring Mobile Text-to-Speech" on page 16-18.

   The Mobile Speech form appears.

2. Select the Incident Management tab.

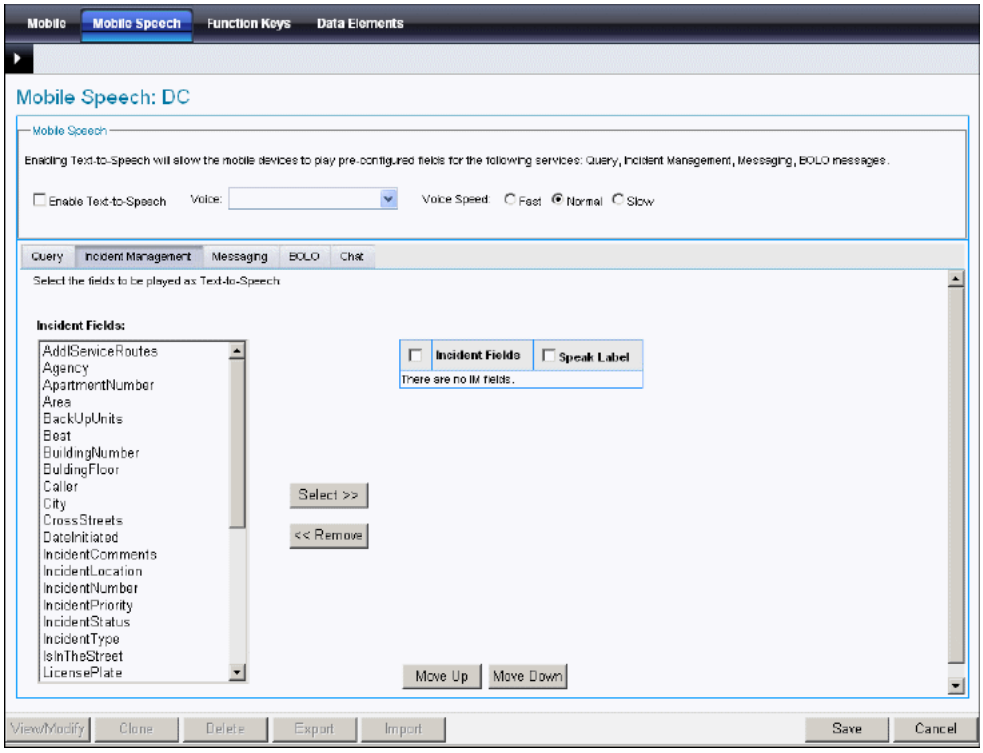


Figure 16-15 Mobile Speech – Incident Management Tab

3. In the Incident Fields box, select one or more incident fields to be played as text-to-speech. You can select more than one field by holding down the **Ctrl** key while you click each field. When you have selected all the fields you need, click **Select**.

   The fields you selected appear in the Incident Fields list on the right.

4. To have the speech reader read the field label and the value of the field, select the **Speak Label** check box for each field.

5. To change the order in which the fields will be read by the speech reader, select a field from the Incident Fields list, and then click **Move Up** or **Move Down**. Repeat this step until the fields are in the order you want them read.

   You may need to scroll down to see the Move Up and Move Down buttons.

6. Click **Save**.

Selecting Messaging Fields

Use the Messaging tab to choose the messaging fields you want to be played as text-to-speech.

To select messaging fields:

1. Access the form for Mobile Text-To-Speech. For instructions, see "Configuring Mobile Text-to-Speech" on page 16-18.

   The Mobile Speech form appears.

2. Select the Messaging tab.

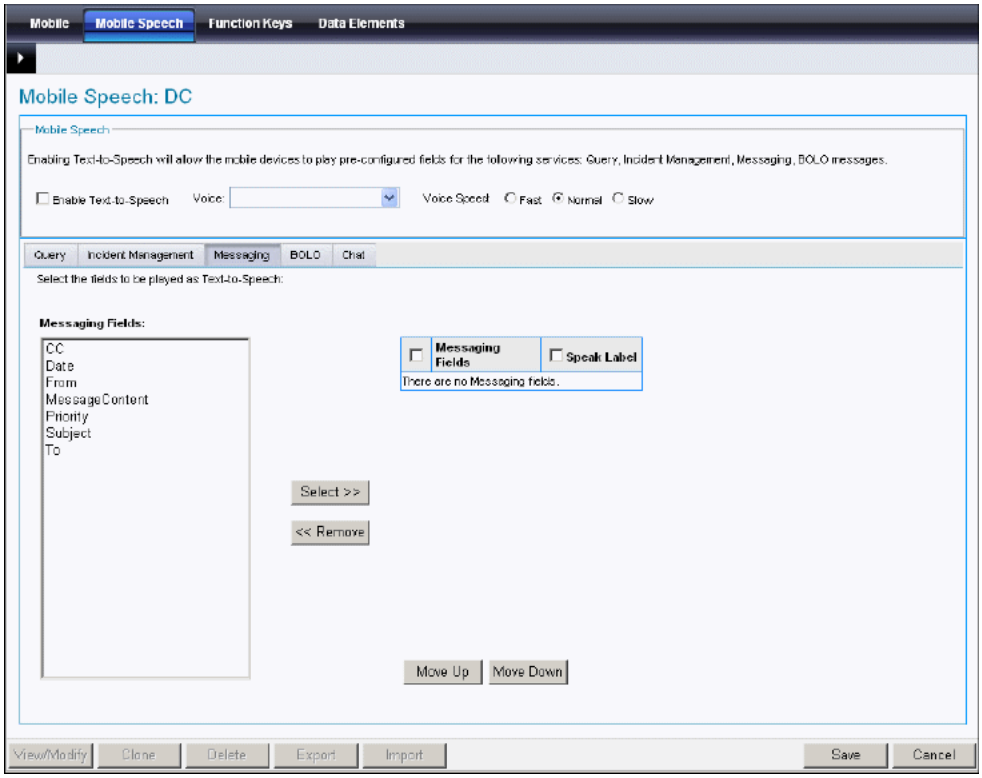


Figure 16-16 Mobile Speech – Messaging Tab

3. In the Messaging Fields box, select one or more messaging fields to be played as text-to-speech. You can select more than one field by holding down the **Ctrl** key while you click each field. When you have selected all the fields you need, click **Select**.

   The fields you selected appear in the Messaging Fields list on the right.

4. To have the speech reader read the field label and the value of the field, select the **Speak Label** check box for each field.

5. To change the order in which the fields will be read by the speech reader, select a field from the Messaging Fields list, and then click **Move Up** or **Move Down**. Repeat this step until the fields are in the order you want them read.

   You may need to scroll down to see the Move Up and Move Down buttons.

6. Click **Save**.

Selecting BOLO Fields

Use the BOLO tab to choose the fields you want to be played as text-to-speech.

To select BOLO fields:

1. Access the form for Mobile Text-To-Speech. For instructions, see "Configuring Mobile Text-to-Speech" on page 16-18.

   The Mobile Speech form appears.

2. Select the BOLO tab.

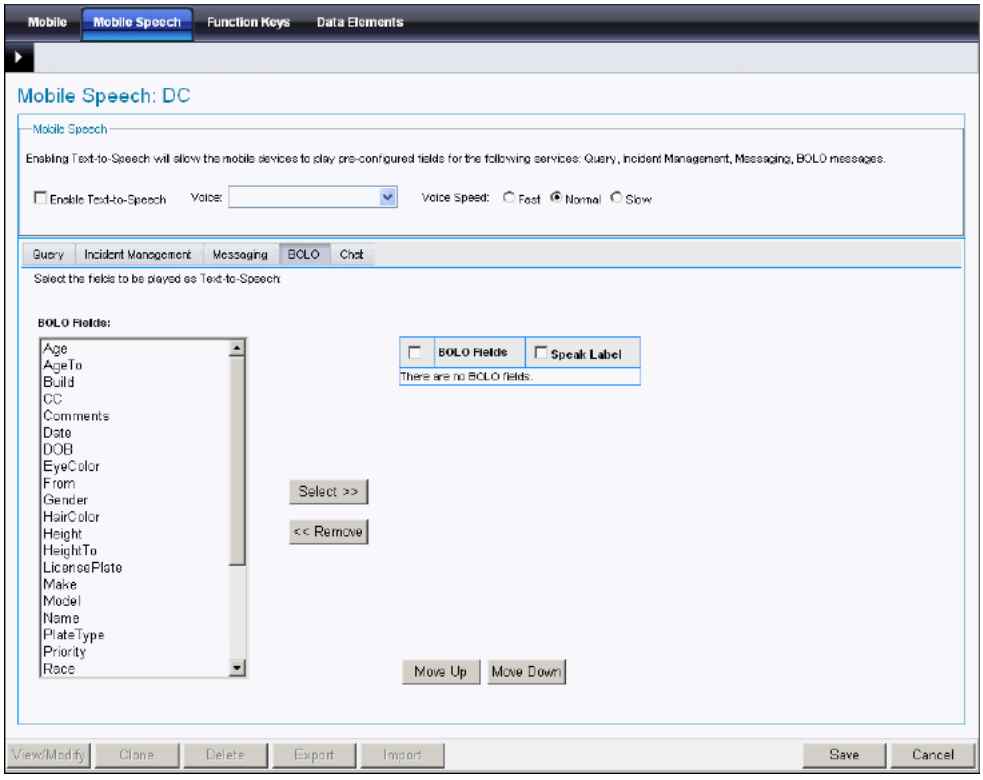


Figure 16-17 Mobile Speech – BOLO Tab

3. In the BOLO Fields box, select one or more incident fields to be played as text-to-speech. You can select more than one field by holding down the **Ctrl** key while you click each field. When you have selected all the fields you need, click **Select**.

   The fields you selected appear in the BOLO list on the right.

4. To have the speech reader read the field label and the value of the field, select the **Speak Label** check box for each field.

5. To change the order in which the fields will be read by the speech reader, select a field from the BOLO Fields list, and then click **Move Up** or **Move Down**. Repeat this step until the fields are in the order you want them read.

   You may need to scroll down to see the Move Up and Move Down buttons.

6. Click **Save**.

Selecting Chat Text-To-Speech Fields

Use the Chat subtab to choose the fields you want to be played as text-to-speech.

To select Chat fields:

1. Access the form for Mobile Text-To-Speech. For instructions, see "Configuring Mobile Text-to-Speech" on page 16-18.

   The Mobile Speech form appears.

2. Select the Chat tab.

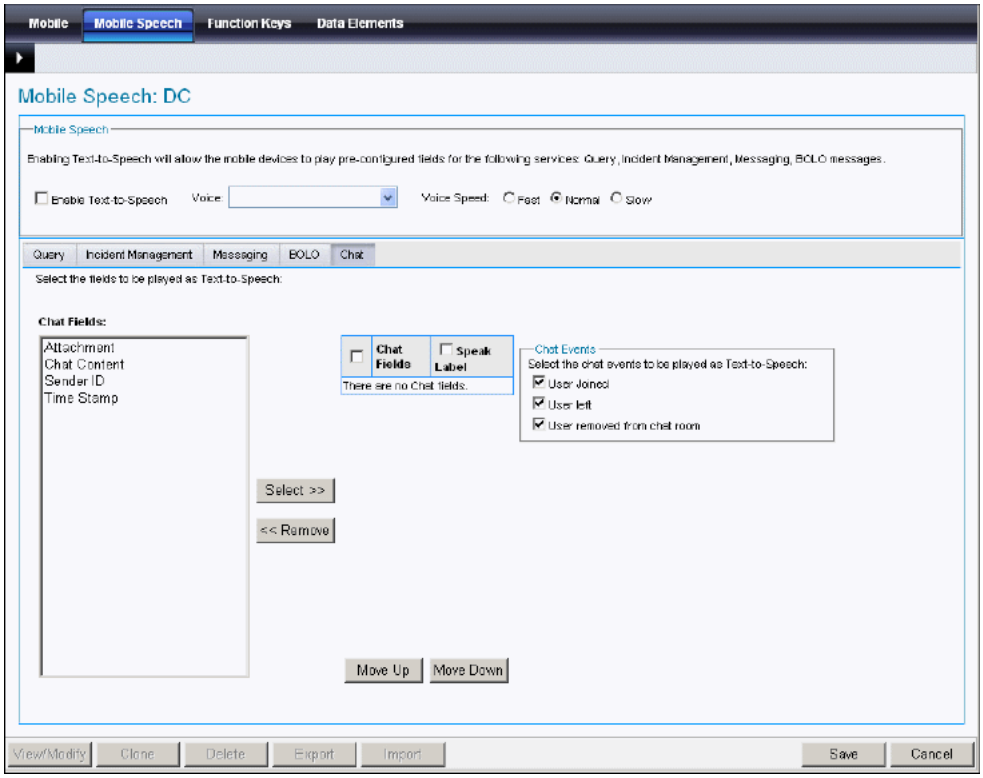


Figure 16-18 Mobile Speech – Chat Tab

3. In the Chat Fields box, select one or more fields that will play as text-to-speech. You can select more than one field by holding down the **Ctrl** key while you click each field. When you have selected all the fields you need, click **Select**.

   The fields you selected appear in the Chat Fields list.

4. To have the speech reader read the field label and the value of the field, select the **Speak Label** check box for each field.

5. To change the order in which the fields will be read by the speech reader, select a field from the BOLO Fields list, and then click **Move Up** or **Move Down**. Repeat this step until the fields are in the order you want them read.

   You may need to scroll down to see the Move Up and Move Down buttons.

6. In the Chat Events area, select the chat events you want to play as text-to-speech.

7. Click **Save**.

Configuring Function Keys for CAD and Mobile

Modify function keys for when you need to change an association between a function key and a common task. You must do this for both Mobile and CAD.

When you configure function keys, you enter information on two tabs of the Function Keys form:

- CAD – Where you assign function keys to common CAD tasks.
- Mobile – Where you assign function keys and icons to common Mobile tasks.

Configuring Function Keys for CAD

Modify function keys for CAD when you need to change an association between a function key and a common CAD task.

NOTE
Do not use the function key combination Shift+F10. This is a default Windows key combination that displays a context sensitive menu for the selected item.

To configure function keys for CAD:

1. From the navigation panel, select **Customization**, and then select **Function Keys**.

The Function Keys tab appears with the CAD tab selected.

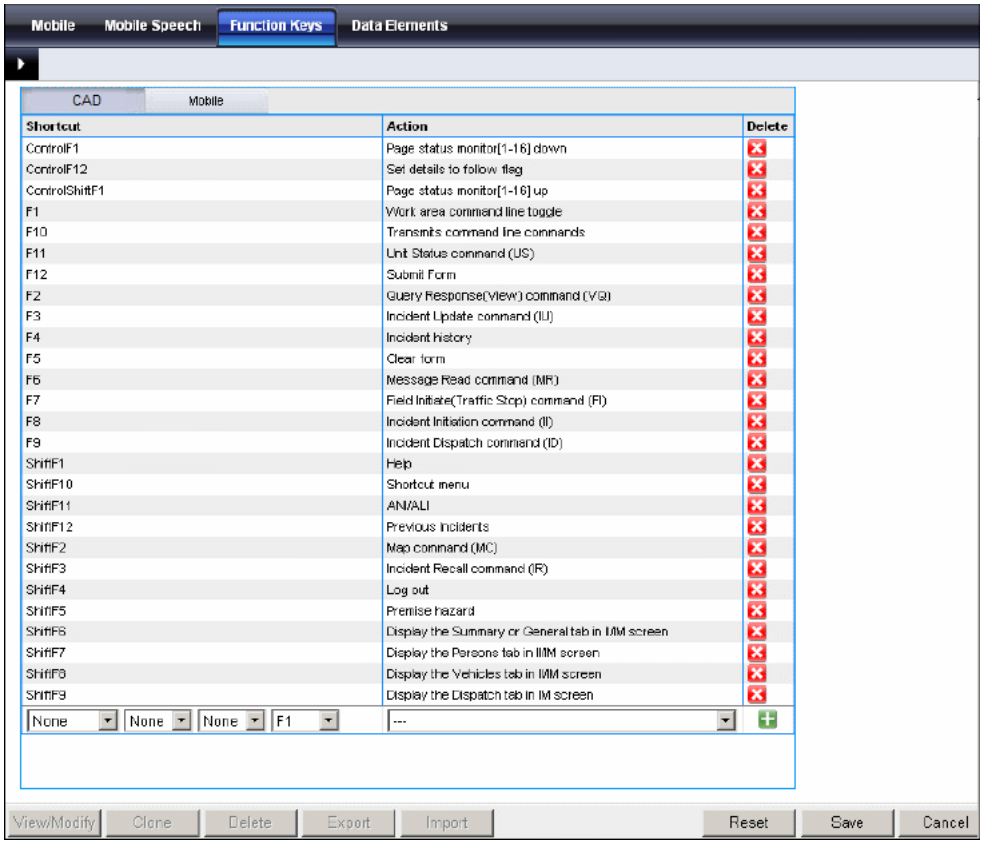


Figure 16-19 Function Keys – CAD Tab

2. Click **View/Modify**.
3. Select the shortcut you want to modify.

   You can now modify the Shortcut and the Action fields.
4. From the Shortcut list, select the function or shortcut key using the lists to define the shortcut you want.
5. From the Action list, select the action.
6. Click **Save**.

Configuring the Soft Function Keys for Mobile

Modify function keys for Mobile when you need to change an association between a function key and a common Mobile task. You can name the button, assign the tasks, select an icon, and select a button size. For Unit Status buttons only, you can also select the background color of the button based on the button status for both day and night mode.

You can now configure the hardware buttons on the Motorola MW810 to initiate PremierOne commands when running PremierOne Mobile. For details, see “Configuring Motorola MW810 Programmable Buttons” on page 16-32.

To configure function keys for Mobile:

1. Access the Function Keys form. For details, see “Configuring Function Keys for CAD” on page 16-28.

2. Select the Mobile tab.

   The Function Keys form appears.

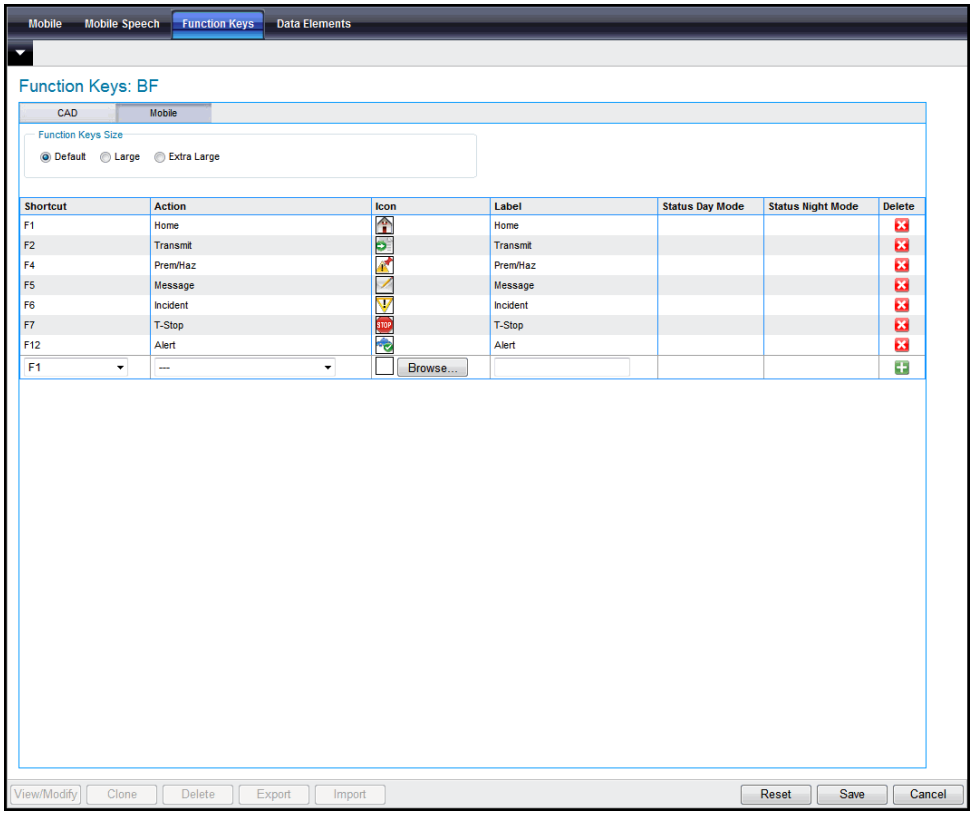
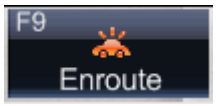


Figure 16-20 Function Keys Form – Mobile Tab

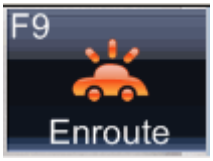
3. Click **View/Modify**.

4. In the Function Keys Size area, select a button size. Button width is determined by the number of buttons that you create. The number of buttons is limited to twelve.

Default



Large – 75 pixels high



Extra Large – 110 pixels high

5. Select the function key or shortcut you want to create or modify (F1- F12).

   You can now modify the Shortcut, Action, Icon, Label, and color fields.

6. From the Shortcut list, select the function or shortcut key.

   The form changes to put the selected shortcut row in focus with selections you can make.

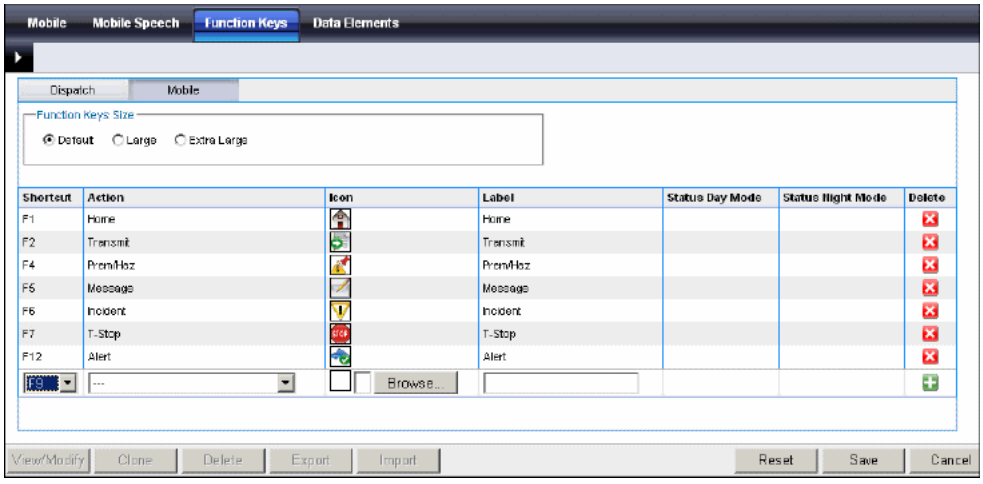


Figure 16-21 Editing Function Keys for Mobile

7. From the Action list, select an action you want to happen when the Shortcut key is activated.

8. In the Icon field, browse for the icon you want to use.

> **NOTE**
> If you create custom icons must be at least 60 x 60 pixels. The application will resize the icons based on the button size selected. Icons for mobile are located on the Mobile client application at:
>
> `C:\ProgramFiles\Motorola\PremierOne\MobileClient\uixml\Default\image\FunctionKeyIcon`

9. From the Label list, type the label you want to use for the button.
10. From the Status Day Mode column, select the button.

    The Color selection dialog box appears. The color picker is available only when selecting Unit Status information.
11. Select the color you want for the unit status you selected to appear on the button for day mode.
12. From the Status Night Mode column, select the button.

    The Color selection dialog box appears.
13. Select the color you want for the unit status you selected to appear on the button for night mode.

    The button configuration is complete.
14. Click **Save**.

    To reset the function keys and icons to the Motorola defaults, click **Reset**.

Configuring Motorola MW810 Programmable Buttons

When you install the PremierOne Mobile client on a Motorola MW810 device, you can configure the six or eight programmable hardware buttons on the MW810 device display to execute PremierOne actions. You can also configure the Emergency button on the MW810 (located on the top-left of the device display), to create a PremierOne Emergency alert or perform any of the other available PremierOne actions allowed.

You can assign the actions that are executed for the MW810 buttons, but you cannot change the button size, label, or the color.

The same PremierOne function can be assigned to a PremierOne Mobile Client (soft) button and a MW810 programmable button.

To configure MW810 hardware buttons:

1. Access the Function Keys form. For details, see "Configuring Function Keys for CAD" on page 16-28.

2. Select the Mobile tab.

   The Function Keys form for Mobile appears.

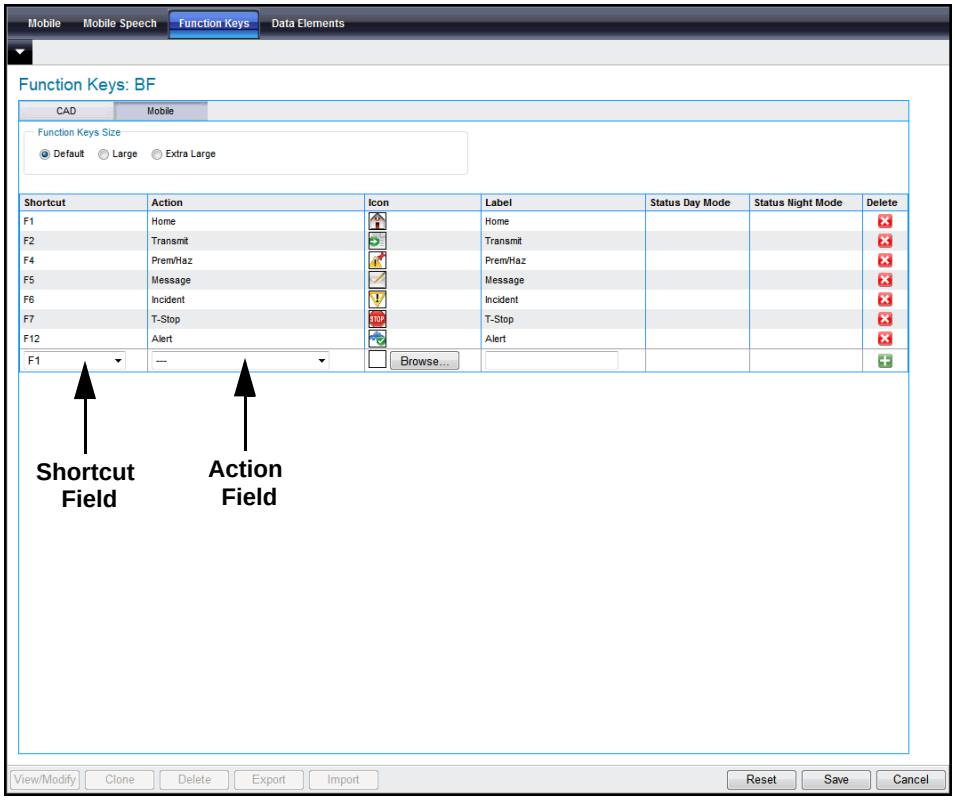


Figure 16-22 Function Keys Form – Mobile Tab

3. Click **View/Modify**.

4. Add and configure the MW810 buttons:

   a. In the Shortcut field, select the MW810 button that you want.

   b. In the Action field, select the action you want for the button.

   c. Click the green **Plus** icon to add the button to the list.

   d. Repeat this for each hardware button on the MW810 that you want to configure.

   The button configuration is complete.

5. Click **Save**.

   To reset the function keys and icons to the Motorola defaults, click **Reset**.

Configuring Data Elements

Use the Data Elements configuration item to modify the labels that appear on the PremierOne application interfaces, such as Area, Beat, City, and so on.

Data elements are the field labels that appear in the PremierOne applications, such as Area, Beat, City, and so on. You can modify some of these labels. For example, your agency may use the term *District* rather than Agency and the term *Reporting District* rather than Beat. You would enter these terms in the Updated Label field on the Data Elements form.

You can modify these labels and clone data elements. For details on cloning, see "Working With Configuration Items" on page 2-9.

You access the Data Elements settings form from the navigation panel. For details on using the filter display to access the form, see "Using Filters" on page 2-7.

To modify data elements:

1. From the navigation panel, select **Customization**, and then select **Data Elements**.

   The Data Elements form appears showing the data elements.

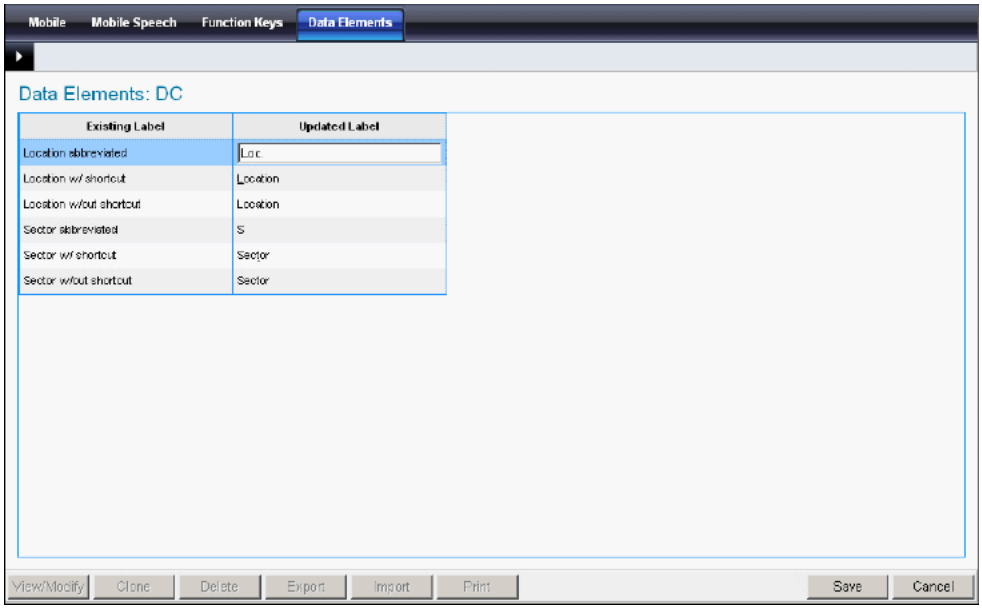


Figure 16-23 Data Elements Form

2. Click **View/Modify**.

3. Select the label you want to alias.

   You can now edit the updated label field.

4. In the Updated Label field, type the alias for the label.

   If your agency uses the term precinct rather than area, click **Area**, and then type `Precinct` in the Updated Label field.

5. Click **Save**.

CHAPTER 17

Configuring CAD Display Settings

The Display Settings configuration item contains one configuration item:

CAD Settings – Where you configure how comments and response messages display on the Comments (Cmnt) tab, and dispatch summary information, comments, and response messages display on the Dispatch (Dptch) tab in the Work Assist Area (WAA) of the Incident Management screen.

Configuring CAD WAA Settings

Use the CAD Settings screen to configure the display of comments, response messages, and dispatch summary information on the Cmnt and Dptch tabs in the WAA of the CAD Incident Management screen.

To configure CAD WAA settings:

1. From the navigation panel, select **Display Settings**.

   The CAD Settings form appears.

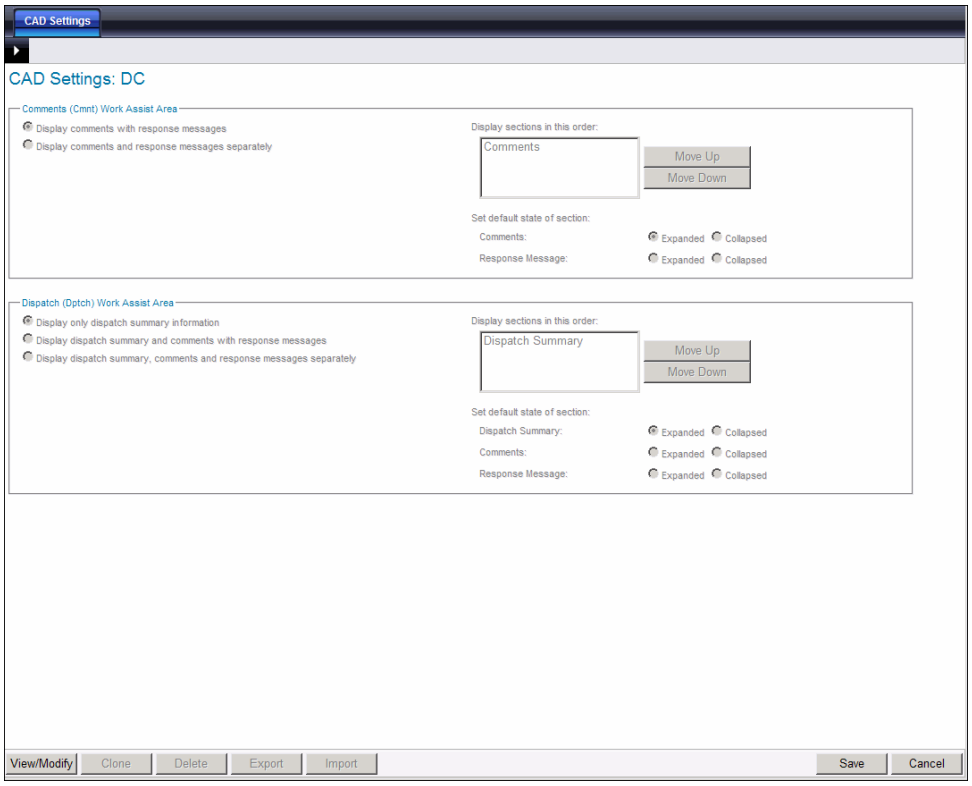


Figure 17-1 Display Settings – CAD Settings Screen

2. Click **View/Modify**.

3. In the Comments (Cmnt) Work Assist Area section, select one of the following:

   - Display comments with response messages (default):

     In this case, the other fields in this section remain disabled. In CAD, comments and response messages will be displayed together on the Cmnt tab of the Incident Management Summary screen, with comments listed first, followed by response messages. Continue with the following step.

   - Display comments and response messages separately:

The fields on the right side of the Comments (Cmnt) Work Assist Area section are enabled.

Figure 17-2 Display Comments and Response Messages Separately Selected

4. In the Display sections in this order field, use the **Move Up** or **Move Down** buttons to indicate the order in which to display the Comments and Response Messages sections.

5. In the Set default state of section field, select whether the default state of the Comments and Response Messages sections should be expanded or collapsed.

> **NOTE**
> There must be at least one comment or one response message to display for the corresponding section to be expanded. If there are no records in a section, the section is collapsed by default, even if you provision **Expanded** as the default state.

6. In the Dispatch (Dptch) Work Assist Area section, select one of the following:

   - Display only dispatch summary information (default):

     The other fields in this section remain disabled. The Dptch tab in the WAA of the CAD Incident Management screen will display only dispatch information.

   - Display dispatch summary and comments with response messages:

     In this case, the fields on the right side of the Dispatch (Dptch) Work Assist Area section are enabled. In CAD, the Dptch tab will display dispatch summary information in one section, and comments and response messages together in another section. Go to the following step to set the order in which the sections appear and to indicate whether the sections should be expanded or collapsed by default.

   - Display dispatch summary, comments and response messages separately:

     In this case, the fields on the right side of the Dispatch (Dptch) Work Assist Area section are enabled. In CAD, the Dptch tab will display dispatch summary information, comments, and response messages in three separate sections. Go to the following step to set the order in which the sections appear and to indicate whether the sections should be expanded or collapsed by default.

7. In the Display sections in this order field, use the **Move Up** or **Move Down** buttons to indicate the order in which to display the sections.

8. In the Set default state of section field, select whether the default state of the each section should be expanded or collapsed.

> **NOTE**
> There must be at least one record to display for a section to be expanded. If there are no records in a section, the section is collapsed by default, even if you provision **Expanded** as the default state.

9. Click **Save**.

CHAPTER 18

Configuring Address Books and Groups

The Address Book configuration item contains the following items:

- Address Book – Where you set additional details for the global address book and all additional address books that are available to users in your agency. This also includes ready reference contacts, such as hospital addresses and phone numbers, or the addresses and phone numbers of tow companies. For details, see “Configuring Address Books” on page 18-1.
- Group – Where you create groups of contacts used to send messages. The name of the group is unique within the domain or agency to which it belongs; other agencies can have groups with the same group names. For details, see “Configuring Groups” on page 18-12.

PremierOne automatically creates a global address book after you create your users, units, and workstations.

NOTE
Mail can be sent to all the people in a contact group, but not an address book.

Configuring Address Books

Use the Address Book configuration item to manage address books. Add an address book when you need to add ready reference information, such as phone numbers and addresses for a tow company or hospital, when you need to add another general address book that will be available to all users, or when you need to set up a private address book for someone.

You can add, modify, clone, and delete address books. For details on cloning and deleting, see “Working With Configuration Items” on page 2-9.

Adding Address Books

When you add an address book, you use four tabs of the Address Book form:

- General – Where you add general information such as the address book name, type owner, maximum number of entries, custom fields, and keywords.
- Add Existing Entries – Where you add entries for people (user IDs), units, workstations, external users, or groups that are present in an existing address book.
- Add New Entries – Where you add entries that do not currently exist in any address book or group.
- View Contacts – Where you can view the members in the address book.

Adding Address Book General Information

Address book general information includes the book name, type, owner (if it is a private type), maximum number of entries, custom fields, and keywords.

Private address books are those only one person has access to and Shared address books are those that more than one person has access to. A global address books is automatically created after users and workstations are provisioned and consists of all the personnel in the system.

To add address book general information:

1. From the navigation panel, select **Address Book**.

The Address Book form appears in the work area. A list of existing address books displays on the left side of the form.

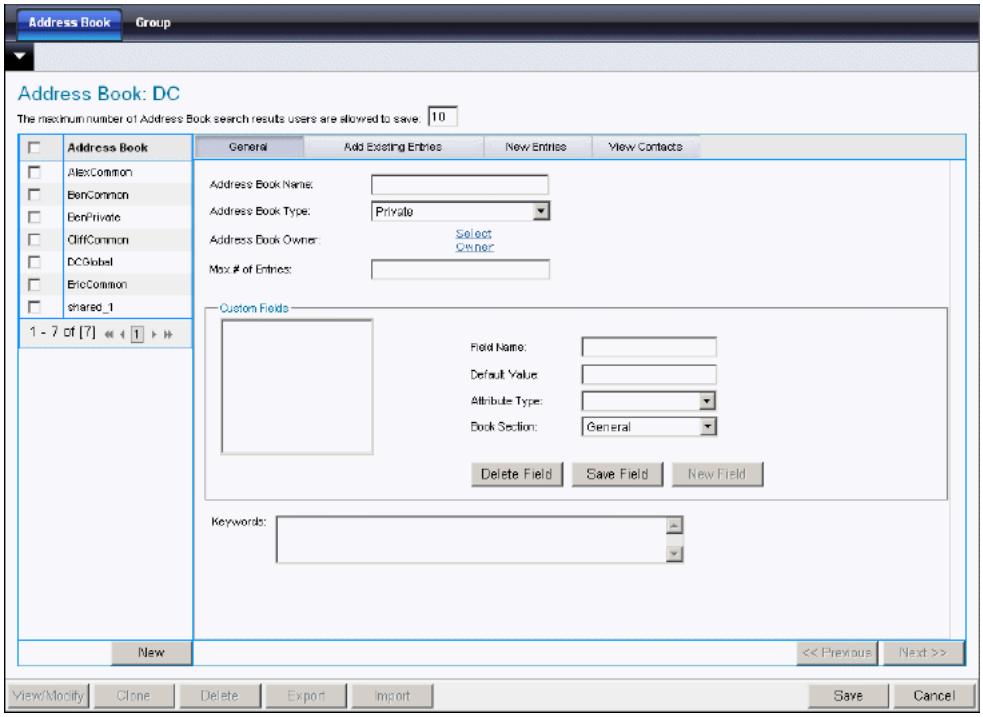


Figure 18-1 Address Book Form – General Tab

2. At the bottom of the Address Book list, click the **New** button.

3. In the Address Book Name field, type a name for the address book.

   If this is a private address book, the person for whom you are creating the book should provide you with a name.

4. In the Address Book Type field, select whether the book is a private, shared, or ready reference address book.

   - For an address book that is available to everyone, select **Shared**.
   - For an address book related to reference material, such as hospital addresses and phone numbers, or the addresses and phone numbers of tow companies, select **Ready Reference**.

- For an address book that is only available to selected users, select **Private**. A **Select Owner** link appears below the Address Book Type field.

  1) Click the link.

     The Select Owner dialog box appears.

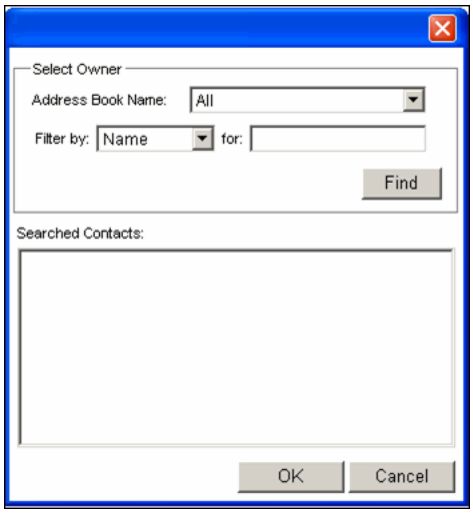


Figure 18-2 Select Owner Dialog Box

  2) From the Address Book Name list, select the address book.

  3) From the Filter by list, select a criteria on which to filter.

  4) In the for field, type the value you want to find. To retrieve all values, leave the field blank.

     Example:

     You could filter by **Name** for `Jones` where `Jones` is the owner of the private address book.

  1) Click **Find**.

     The results of your search appear in the Searched Contacts box.

  2) Select the contact from the Searched Contacts box, and then click **OK**.

5. In the Max. # of Entries field, type the maximum number of entries allowed in this address book.

   For an unlimited number of entries, enter 0.

6. In the Custom Fields section, enter the field name and default value (if any) for a new field. Select the attribute type (number, text, yes/no) and book section where the field should display and then click **Save Field**.

   The new field appears in the adjacent list of custom fields.

7. In the Keywords field, type one the keywords to use in the address book search.

   Keywords are entered in the Resources – Personnel – Contact Info configuration item.

Adding Existing Entries to Address Books

Add existing entries when the entry already exists in another address book or group. An entry can be a person (user ID), a unit, a workstation, an external user, or a group.

To add an existing entry:

1. Open the Address Book form.

   For details, see “Adding Address Book General Information” on page 18-2.

2. From the Address Book form, select the Add Existing Entries tab.

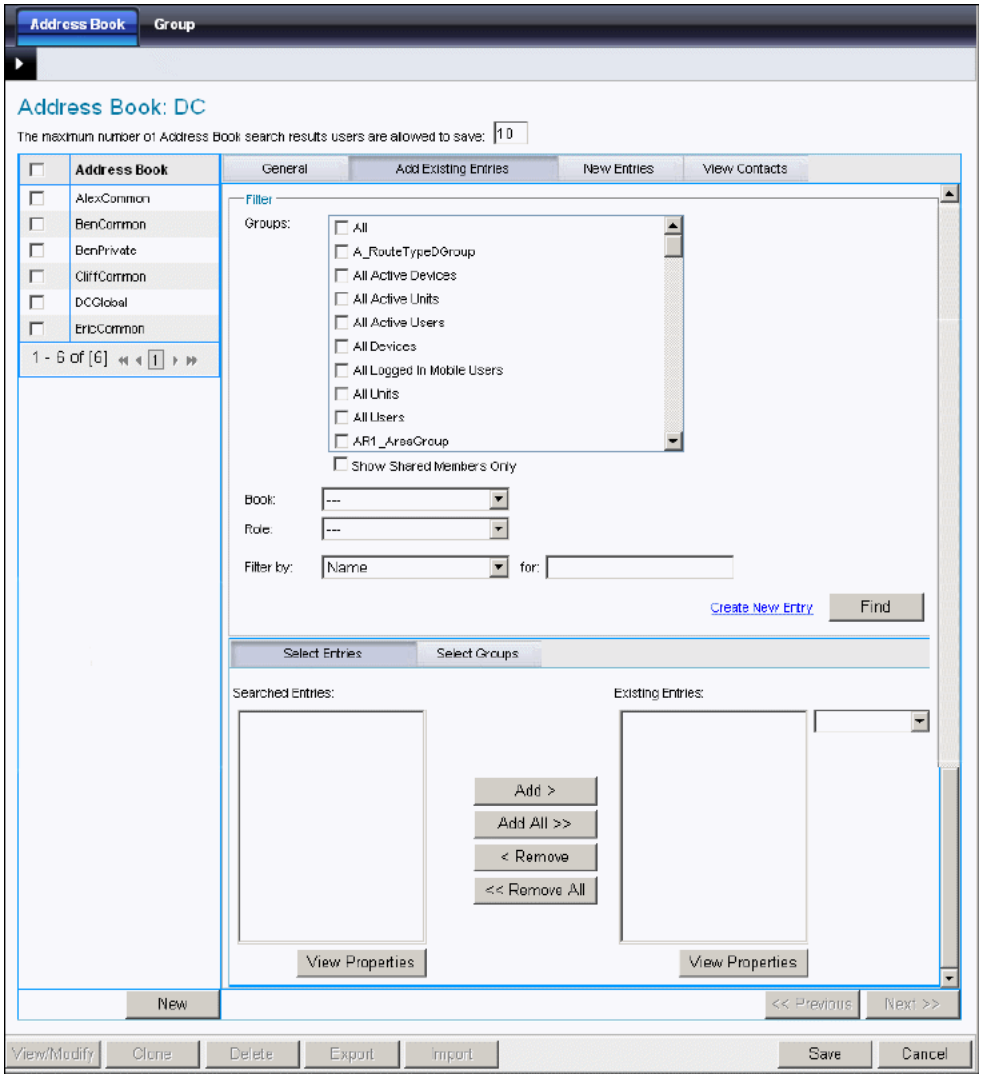


Figure 18-3 Address Book – Add Existing Entries Tab

3. In the Filter section, select the agency, address book (optional), groups (optional), and role from which to search for contacts.

   Use the Filter by field to search for Names, User IDs, Unit IDs, or Workstation IDs. Then optionally enter the value you are searching for in the for field. You can enter partial values in the for field to limit the search; for example, entering ADMIN would return all values beginning with ADMIN, such as ADMIN1, ADMIN2, and so on.

4. Click **Find**.

   The results of your search appear in the Entries section on the Select Entries subtab or in the Groups section on the Select Groups subtab.

5. Select the entries you want to add to the address book by clicking **Add** or **Add All**.

To view or edit detailed information about any of the entries, select the entry, and then click **View Properties**.

The View Properties dialog box appears.

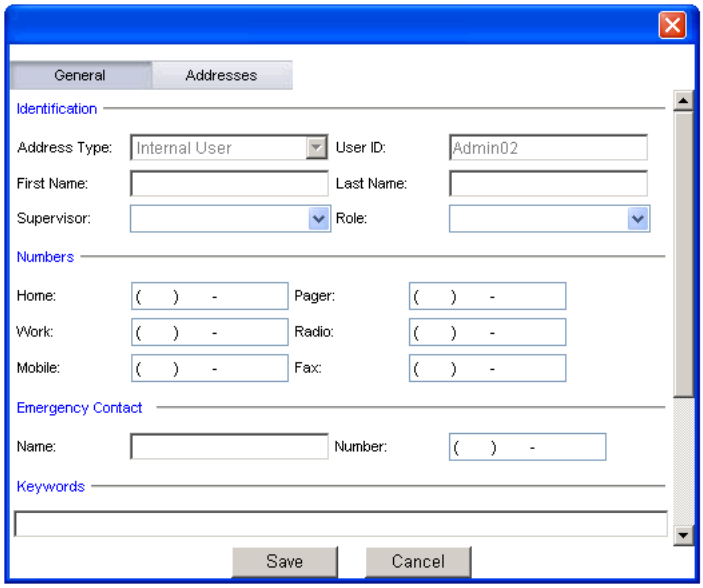


Figure 18-4 View Properties Dialog Box

6. Click **Save** to save any edits and close the dialog box, or click **Cancel** to close the dialog box.

Adding New Entries to Address Books

Add new entries when you need to create entries that do not currently exist in any group or address book.

To add an entry:

1. Open the Address Book form. For details, see “Adding Address Book General Information” on page 18-2.

2. From the Address Book form, select the New Entries tab.

   Different fields display depending on whether you are creating an address book or ready reference book.

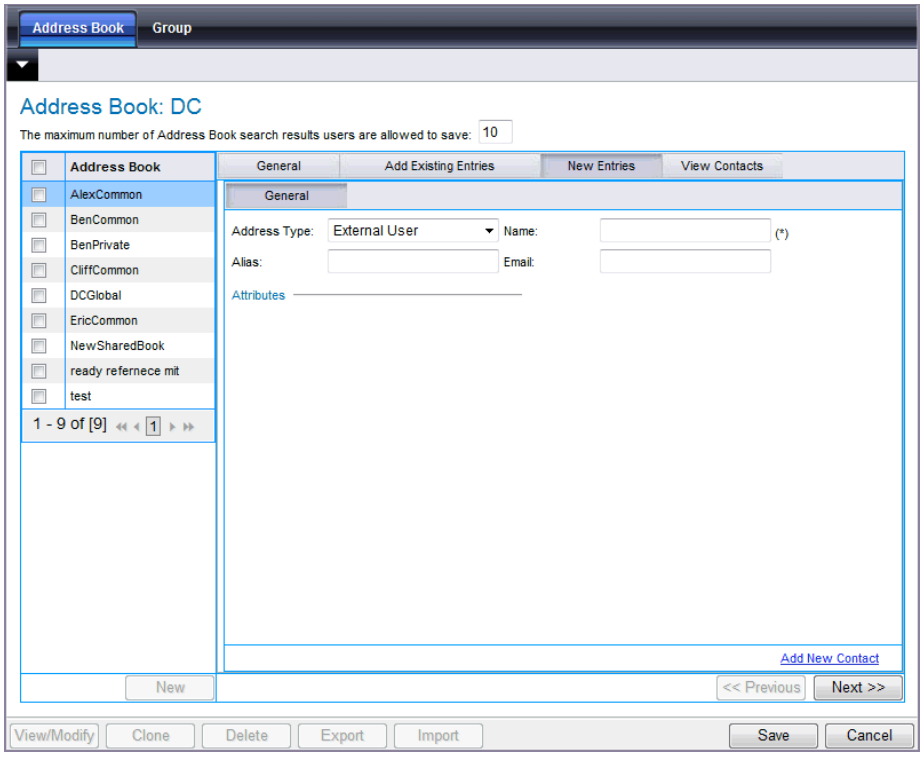


Figure 18-5 Address Book – New Entries Tab for Private and Shared Books

The following fields display for Ready Reference books.

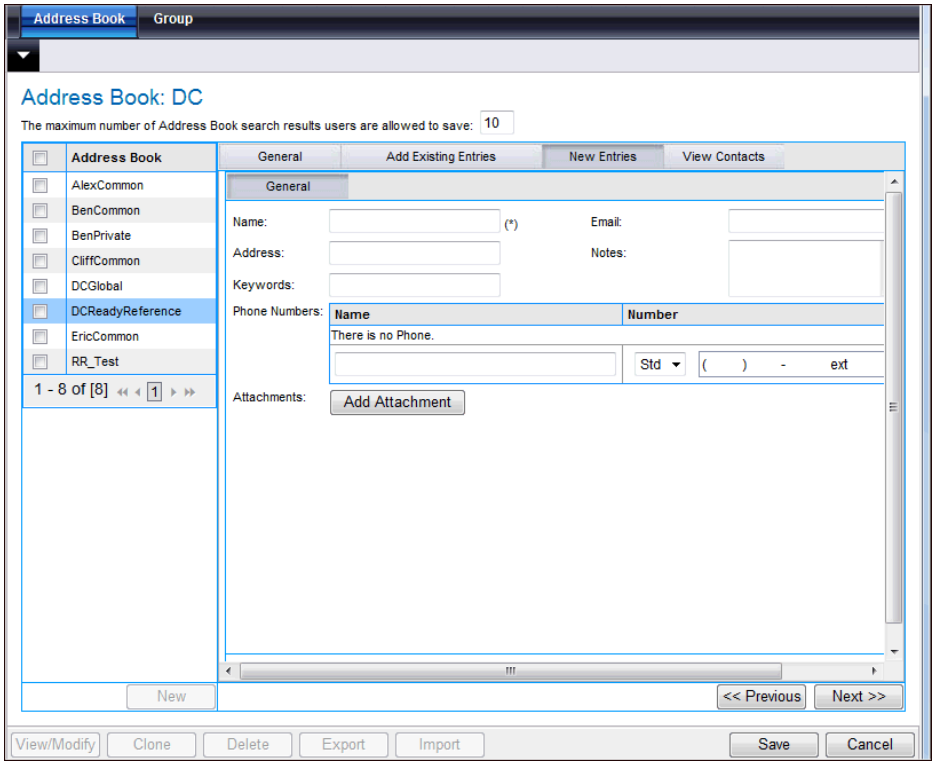


Figure 18-6 Address Book – New Entries Tab for Ready Reference Books

3. On the General subtab, enter the information and alias for this entry.

   For private and shared address books, the Alias can be a shortened version of the User ID or a shortened alias. For example, if the normal address is **MSF47**, the alias could be **MarySmith** so it is easier to remember. Or, for radios, the alias could be **MS**, to make it easier to enter into the radio using the radio keypad. Only one alias per address book entry is allowed.

   Keywords that you enter can be searched on in PremierOne CAD.

NOTE

An alias is automatically created in the Address Book based upon Radio alias value when the radio is added to in PremierOne. Any time the alias is changed in the Radio configuration, the alias is not updated in the Address Book; you must manually update the alias. The alias in the Address Book and Radio configuration do not have to match.

Messages uses the alias in the Address Book to route notification/mail messages.

For Ready Reference books, you can enter multiple phone numbers for use in provisioning Call Control. Phone numbers can be of the following types:

- STD – Standard 7-, 10- or 11-digit numbers.

By leading the entry with a + symbol, you can type any characters/phone number length regardless of the phone number template used by your system.

- SC – Star Code number. Star codes are pre-programmed in the selective router to allow PSAPs to transfer E9-1-1 calls to predetermined PSAPs while keeping the complete original ANI/ALI data retrieved with the original 9-1-1 call.
- HF – Hook flash number. Hook flash simulates quickly hanging up and then picking up again. How this works depends on the agency configuration.
- RD – Ringdown line.

4. Click **Save**.

   The entries you added appear in the Address Book list on the left in black text.

NOTE

To modify an entry, retrieve it from the View Contacts tab and then View the Properties. For details, see "Viewing Contacts in the Address Books" on page 18-11.

Viewing Contacts in the Address Books

You can display the contacts in any specific address book or ready reference book and view the properties of any individual entry.

To view contacts:

1. Open the Address Book form. For details, see "Adding Address Book General Information" on page 18-2.

2. From the Address Book form, select the View Contacts tab.

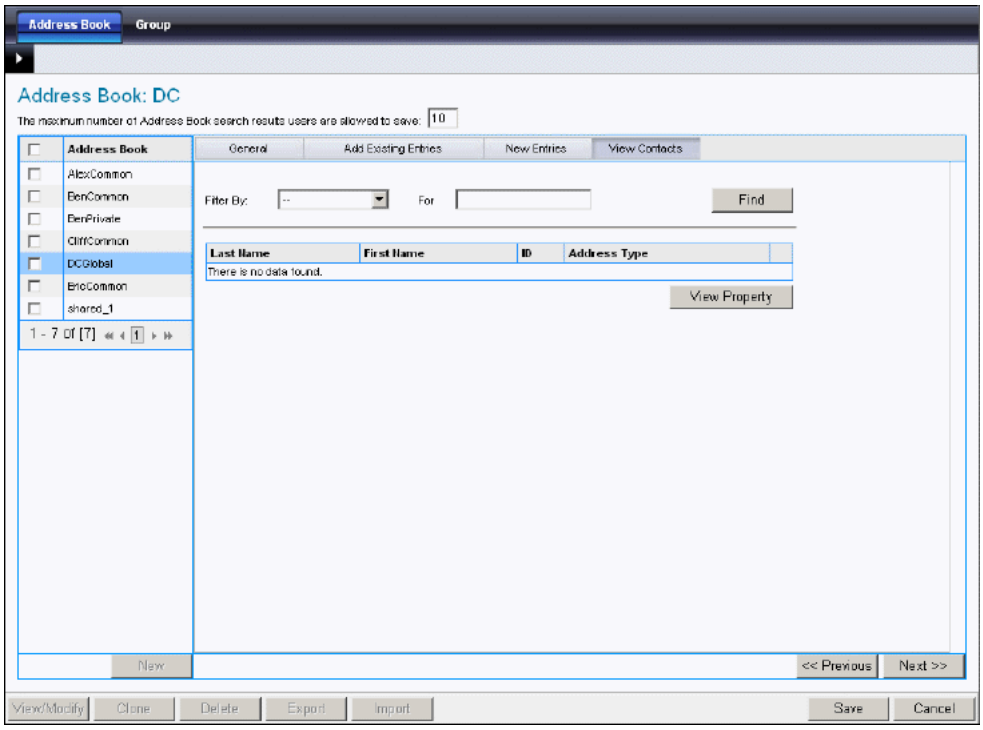


Figure 18-7 Address Book – View Contacts Tab

3. From the Filter By list, select filter for you want to use to retrieve contacts. If you do not make a selection, then all contacts are retrieved.

   Filters include Address Type, Alias, ID, Keywords, or Personnel Note (Notes are entered in the Note field for Ready Reference properties).

   In the For box, enter the text you want to search for.

   Address types include Contact, Internal User, Unit, Devices, External user, and Unroutable address. For devices, use the format, such as Device/ASTRO, Device/ Smart Client, or Device/Workstation.

4. Click **Find**.

   The results display. From the results list, you can select a contact and view and modify properties.

Configuring Groups

Use the Group configuration item to manage groups. PremierOne automatically creates several groups, such as the following: users, units, workstations, geographic boundaries such as areas, beats, or sectors, and roles.

Add groups when you need a way to send messages to a group or distribution list that does not exist. You can add, modify, clone, and delete groups. For details on cloning and deleting groups, see "Working With Configuration Items" on page 2-9.

Groups are automatically created after users and workstations are provisioned. These consist of groups such as all active devices, units, users in specific areas, users in each role, and so on. These groups cannot be modified without modifying the personnel. For example, you cannot remove a users from the group role without removing the user from the role.

Adding Groups

When you add a group, you enter information on three tabs of the Group form:

- General – Where you add description information, expiration and size limit information, and notifications information.
- Entries – Where you add entries for people (user IDs), units, workstations, external users, or other groups that are present in an existing address book.
- New Entries – Where you add entries that do not currently exist in any address book or other group.

You can also add a group by cloning an existing group that closely matches the one you want to add.

Adding Group General Information

Add a group when you or someone in your agency needs a way to send messages to a distribution list that does not yet exist.

To add group general information:

1. From the navigation panel, select **Address Book**, and then select **Group**.

The Group form appears in the work area. A list of existing groups displays on the left side of the form.

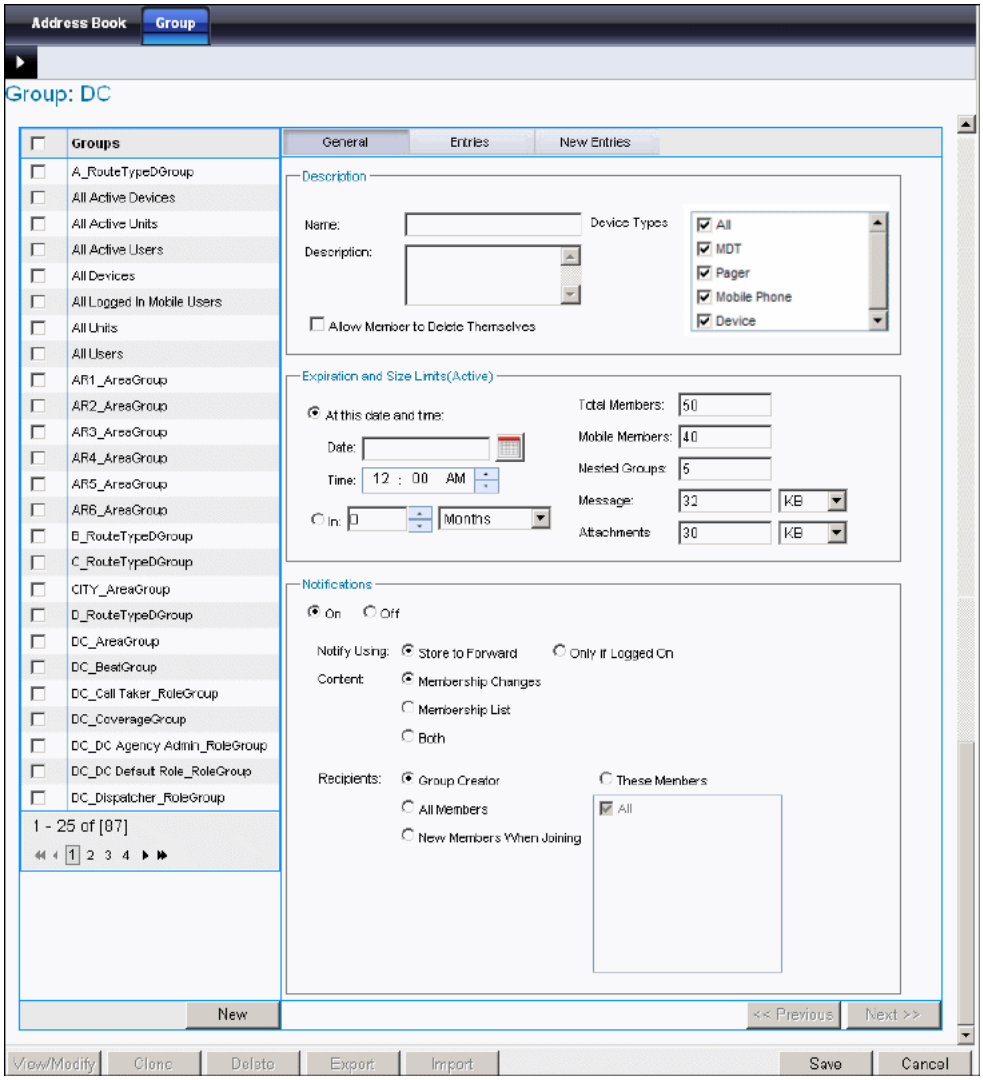


Figure 18-8 Group Form – General Tab

2. At the bottom of the Groups list, click the **New** button.
3. In the Description section, complete the following:
   a. Enter a Name and a Description for the new group.
   b. In the Device Types field, select the types of devices this group uses.
   c. Select the Allow Member to Delete Themselves check box if group members should be allowed to remove themselves from the group.
4. In the Expiration and Size Limits (Active) section, complete the following:

a. Enter values for either the Date and Time or the number of days, months, or years from the present date when this group will expire.

b. Enter information about the group including Total Members, Mobile Members, and the number of Nested Groups.

c. Enter a size value for maximum size of Messages and Attachments for this group.

5. In the Notifications section, complete the following:

a. Select if notifications are **On** or **Off**.

b. If notifications are enabled, select how and when to notify, the content of the notifications, and who the recipients of the messages should be.

6. Click **Save**.

Adding Existing Entries to a Group

Add existing entries to a group when the entry already exists in another address book or another group. Before adding existing entries to a group, complete the steps in “Adding Group General Information” on page 18-12.

To add an existing entry to a group:

1. Open the Groups form. For details, see “Adding Group General Information” on page 18-12.

2. From the Group form, select the Entries tab.

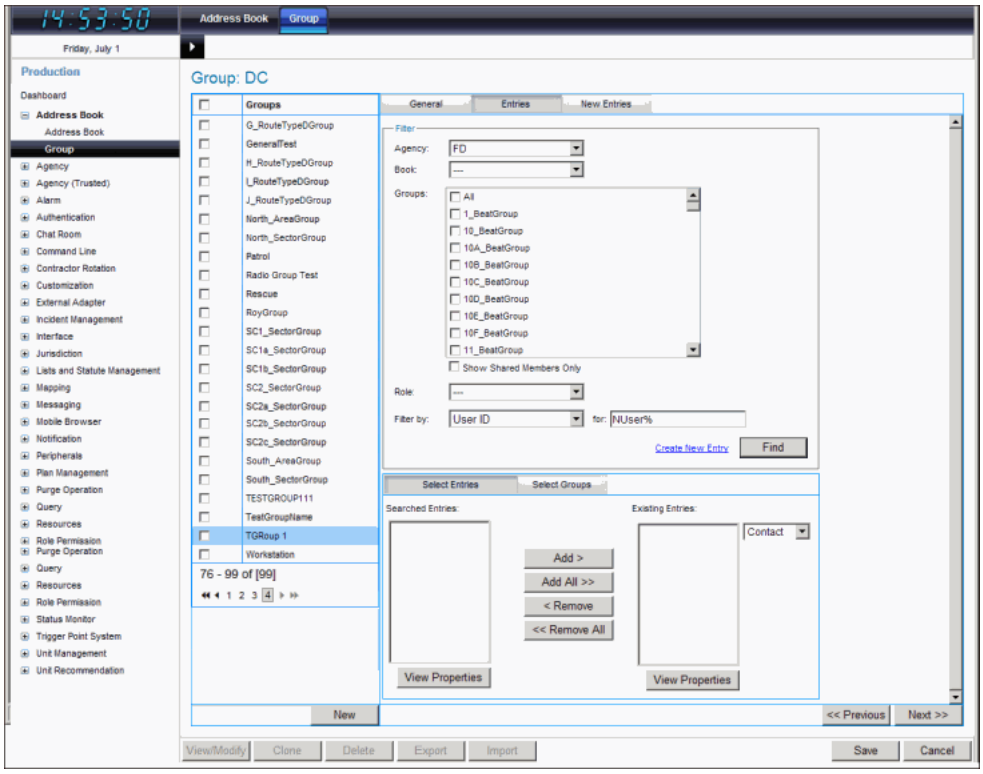


Figure 18-9 Group Form – Entries Tab

3. From the **Agency** list, select the agency.

4. From the Book list, select the address book (optional).

5. In the Filter section, select the groups, book, and role from which to select entries for the address book you are creating.

   Use the Filter by field to search for **Name**, **User ID**, **Unit ID**, or **Device ID**. Then optionally enter the value you are searching for in the for field. You can enter partial values in the for field to limit the search; for example, entering **ADMIN** would return all values beginning with **ADMIN**, such as **ADMIN1**, **ADMIN2**, and so on.

6. Click **Find**.

The results of your search appear in the Entries section on the Select Entries tab or in the Groups section on the Select Groups tab.

7. From the Select Entries or Select Groups subtab, select the entries you want to add to the group by clicking **Add** or **Add All**.

   To view or edit detailed information about any of the entries, select the entry, and then click **View Properties**.

   The View Properties dialog box appears.

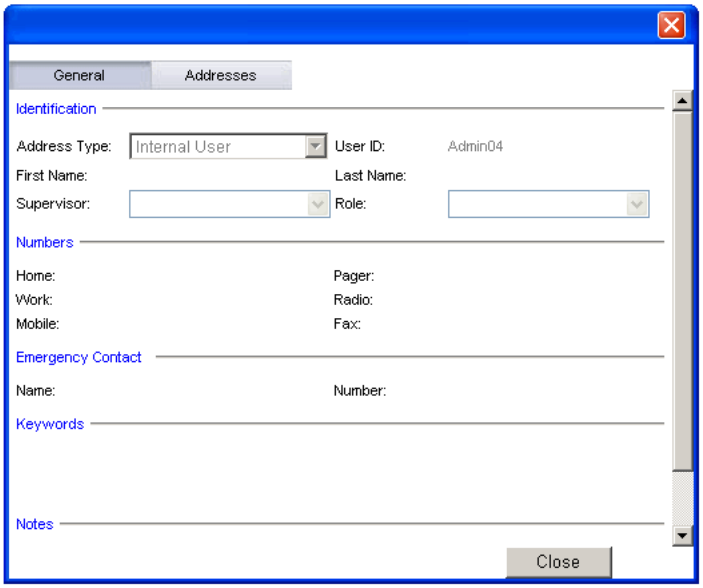


Figure 18-10 View Properties Dialog Box

8. Click **Yes** to save any edits and close the dialog box, or click **No** to close the dialog box.

Adding New Entries to a Group

Add new entries when you need to create entries that do not currently exist in any group or address book. An entry can be a person (user ID), a unit, a workstation, an external user, or a group.

To add an entry:

1. Open the Groups form. For details, see "Adding Group General Information" on page 18-12.

2. From the Group form, select the New Entries tab.

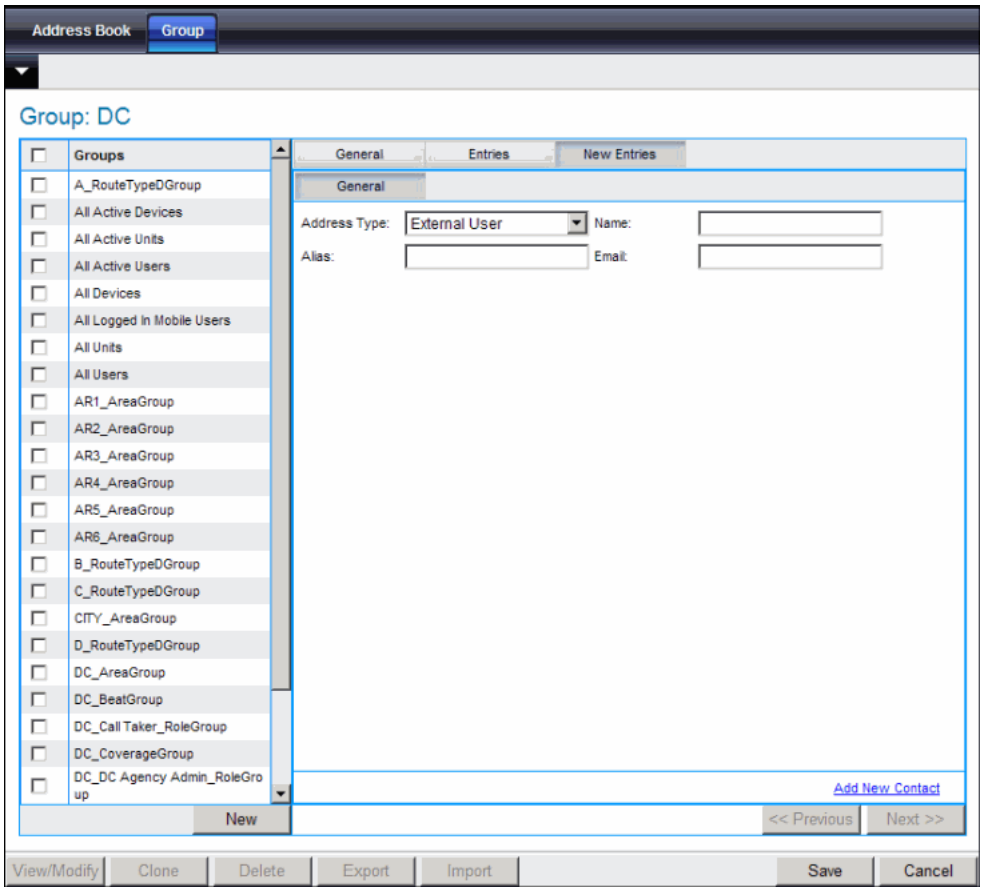


Figure 18-11 Group Form – New Entries Tab

3. In the General subtab, enter the identification, phone numbers, emergency contact, and keyword information for this entry.

   In the Address Type field, the **Unroutable Address** option is for groups that cannot receive email, such as some ready reference locations.

4. Click the Addresses subtab and enter the business, home, and email addresses for this entry.

5. Click the In Groups subtab and select the groups to which this entry belongs.

- To view a group, save your changes, select the group you want to view, and then click **View**.

> **CAUTION**
> If you choose to view a group before you save your changes, you will lose any changes you made. Make sure you save your changes before you continue with viewing a group.

- To add a contact, click the **Add New Contact** link.

The General, Entries, and New Entries tabs for new contacts appear in the work area. Start with the General tab to add your new contact.

6. Repeat the procedure for any other entries that you want to add.

   - Click **New**, and then repeat "Adding Group General Information" on page 18-12, "Adding Existing Entries to a Group" on page 18-15, and the steps in this topic. You do not need to save your changes before adding another group if you click the **New** button.

   - Save your changes, and then click the **Add Group** link.

> **CAUTION**
> If you choose to add a group by clicking the **Add Group** link before you save your changes, you will lose any changes you made. Make sure you save your changes before you continue with adding a group.

   Each unsaved entry appears in the group list on the left in blue text.

7. Click **Save**.

   The entries you added appear in the group list on the left in black text.

CHAPTER 19

Configuring Alarms

The Alarm configuration item contains the following items:

- Alarm Companies – Where you manage information regarding alarm companies. For details, see “Configuring Alarm Companies” on page 19-1.
- Alarm Records – Where you manage alarm records associated with specific locations or addresses. For details, see “Configuring Alarm Records” on page 19-3.
- Chronic Alarm Settings – Where you manage chronic alarm configuration. For details, see “Configuring Chronic Alarm Settings” on page 19-9.
- False Alarms – Where you can view and deactivate false alarm records. For details, see “Viewing False Alarms” on page 19-10.

Configuring Alarm Companies

Use the Alarm Companies configuration item to manage information regarding alarm companies. Once you create an alarm company record, you can use it to create alarm records.

You can add, modify, delete, and clone alarm company records. For details on modifying, deleting, and cloning, see “Working With Configuration Items” on page 2-9. You cannot change the Alarm Company ID. If you want to change the ID, you must delete and re-add the record.

Adding Alarm Companies

When you add an alarm company, you enter information on the General tab of the Alarm Companies form. You can also add an alarm company by cloning an existing company that closely matches the one you want to add.

To add an alarm company:

1. From the navigation panel, select **Alarm**.

The Alarm Company form appears in the work area. A list of existing alarm companies displays on the left side of the form.

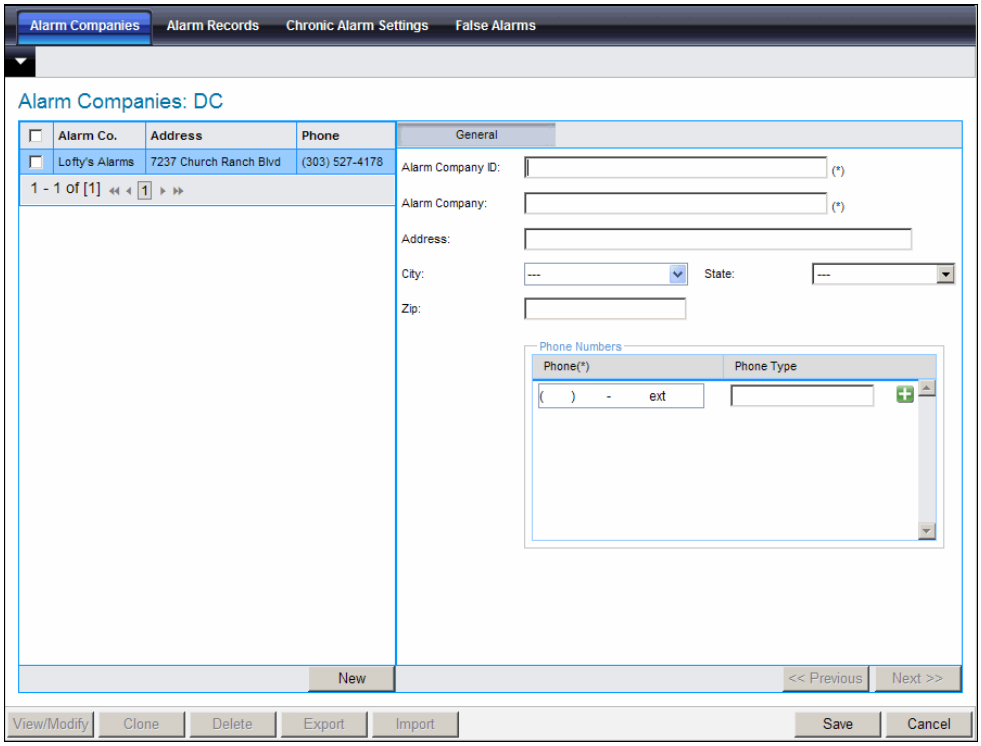


Figure 19-1 Alarm Companies Form – New

2. At the bottom of the Alarm Companies list, click the **New** button.

3. On the General tab on the right side of the work area, enter values for the alarm company ID, alarm company name, address, city, state, zip, and phone numbers.

4. In the Phone fields, type the phone number or numbers for the alarm company.

   You can use any combination of 3-digit area code, 7-digit phone number, and/or 1-4 digit extension. If you are entering an international number, start with a + symbol, enter the country code, and then the rest of the phone number information. Entering the + symbol causes the area code/phone number/extension formatting to be removed.

   Click the plus symbol (+) at the end of the row to save the phone number or numbers and add another row.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the last phone number entered, even after you click Save.

   Each unsaved alarm company appears in the list on the left in blue text.

5. Click **Save**.

The alarm companies you added display in the list on the left in black text.

Configuring Alarm Records

Use the Alarm Records configuration item to manage alarm records. Alarm records describe the alarms that are associated with specific locations or addresses.

You can add, modify, clone, and delete alarm records. For details on modifying, cloning, and deleting, see “Working With Configuration Items” on page 2-9. You cannot change the Alarm ID. If you want to change the ID, you must delete and re-add the record.

NOTE

If you are using the CryWolf false alarm interface, you do not need to manually provision the alarm database because the records provided by CryWolf are the only records in the database.

Adding Alarm Records

Add an alarm record when an alarm company contacts you or when an automatically triggered alarm comes into the dispatch center and you want to set it up for efficient dispatching. Alarm records are associated with specific locations or addresses.

When you add alarm records, you enter information on two tabs of the Alarm Records form:

- General – Where you set general information, such as alarm ID, permit number, alarm company, alarm company phone number, location information for the alarm, and contact information for the alarm.
- Incidents – Where you set incident information, such as resetting the false alarms to zero, setting the incident type, disposition, and modifying circumstance for chronic alarm settings, and setting a specific incident type, disposition, and modifying circumstance for certain days or times.

Adding Alarm Records General Information

Alarm record general information includes the alarm ID, permit number, name and phone number of the alarm company, whether this location is exempt from false alarm processing (and the reason), location for this alarm record, and contact information for this alarm record. If available, the alarm monitoring company information displays at the bottom of the page as read-only labels.

To add alarm record general information:

1. From the navigation panel, select **Alarm**, and then select **Alarm Records**.

   The Alarm Records form appears in the work area. A list of existing alarm records displays on the left side of the form.

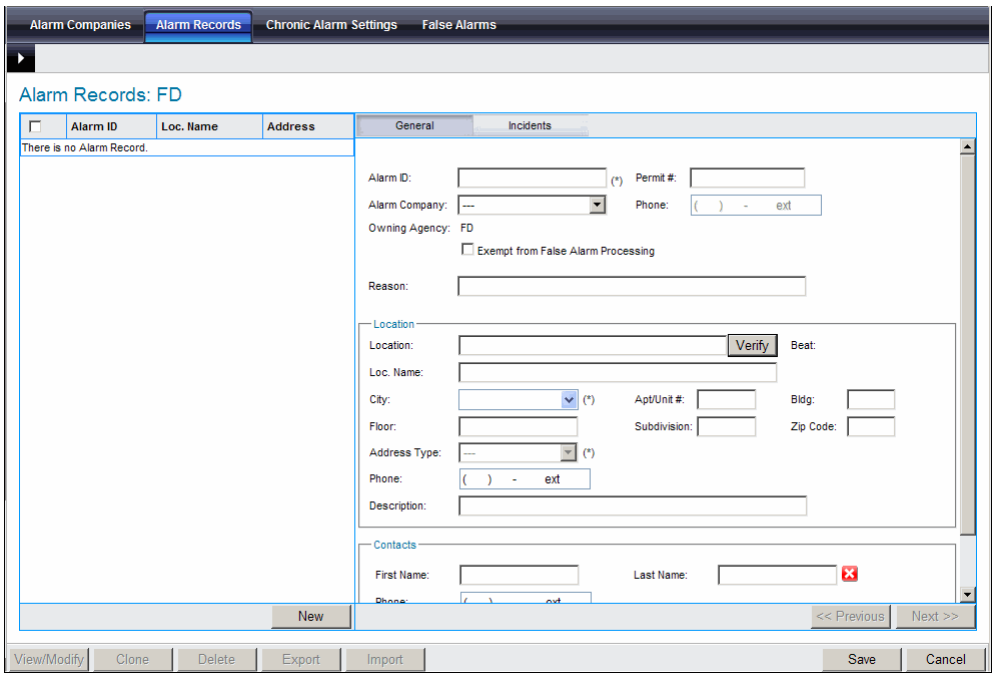


Figure 19-2 Alarm Records Form

2. Click the **New** button below the list of alarm records.

3. In the Alarm ID field, type the 6 or 10 digit numerical ID for this alarm record.

> **NOTE**
> If the selected alarm is generated by the CryWolf interface and has a status of Inactive, the following message appears in red above the Alarm ID field:
>
> ** Alarm Status: Inactive **

4. In the Permit # field, type the permit number for this alarm record.

5. From the Alarm Company list, select the alarm company that responds to this alarm. If the alarm company does not appear in the list, you need to add the alarm company. For more information, see “Adding Alarm Companies” on page 19-1.

   The phone number for the alarm company automatically appears after you select the company.

   If you want this alarm record to be exempt from false alarm processing, select the **Exempt from False Alarm Processing** check box and enter a reason for the exemption in the Reason field.

6. In the Location section, enter the location information for the alarm.

   To verify the address, click the **Verify** button. After PremierOne verifies the address, the warning icon disappears.

   If the address is a multi-beat intersection, a dialog box displays prompting you for the beat. The Areas that display are based on the active plan. If an agency has not yet provisioned an active plan, --- displays as the Area value. Select the beat and then click the **Select** button.

   Once you select the beat, the beat then displays in the Location information.

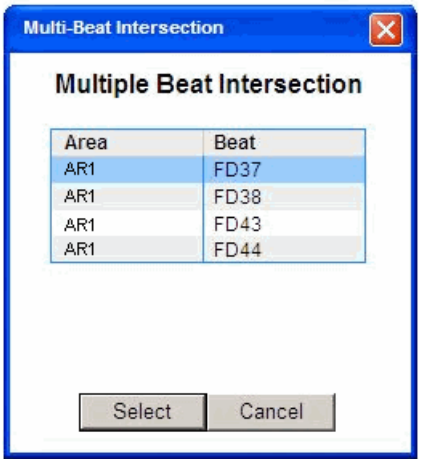


Figure 19-3 Multiple Beat Intersection Dialog Box

   For the Phone field within the Location box, you can use any combination of 3-digit area code, 7-digit phone number, and/or 1-4 digit extension. If you are entering an international number, start with a + symbol, enter the country code, and then the rest of the phone number information. Entering the + symbol causes the area code/phone number/extension formatting to be removed.

7. In the Contacts section, enter contact information for the alarm.

   For the Phone field within the Contacts group box, you can use any combination of 3-digit area code, 7-digit phone number, and/or 1-4 digit extension. If you are entering an international number, start with a + symbol, enter the country code, and then the rest of the phone number information. Entering the + symbol causes the area code/phone number/extension formatting to be removed.

To add another contact, click **Add Contact**. PremierOne displays an additional set of contact fields.

8. Click **Save**.

Adding Alarm Records Incident Information

Alarm record incident information includes:

- Number of false alarms in X number of days
- Option to reset false alarms to zero
- Chronic alarm settings, such as initial status, incident type, modifying circumstance, and response message to be sent
- Time/day specific settings, such as initial status, incident type, modifying circumstance, and response message to be sent

To add alarm record incident information:

1. Open the Alarm Records form.

   For details, see “Adding Alarm Records” on page 19-3.

2. From the Alarm Records form, select the Incidents tab.

3. Select the alarm record.

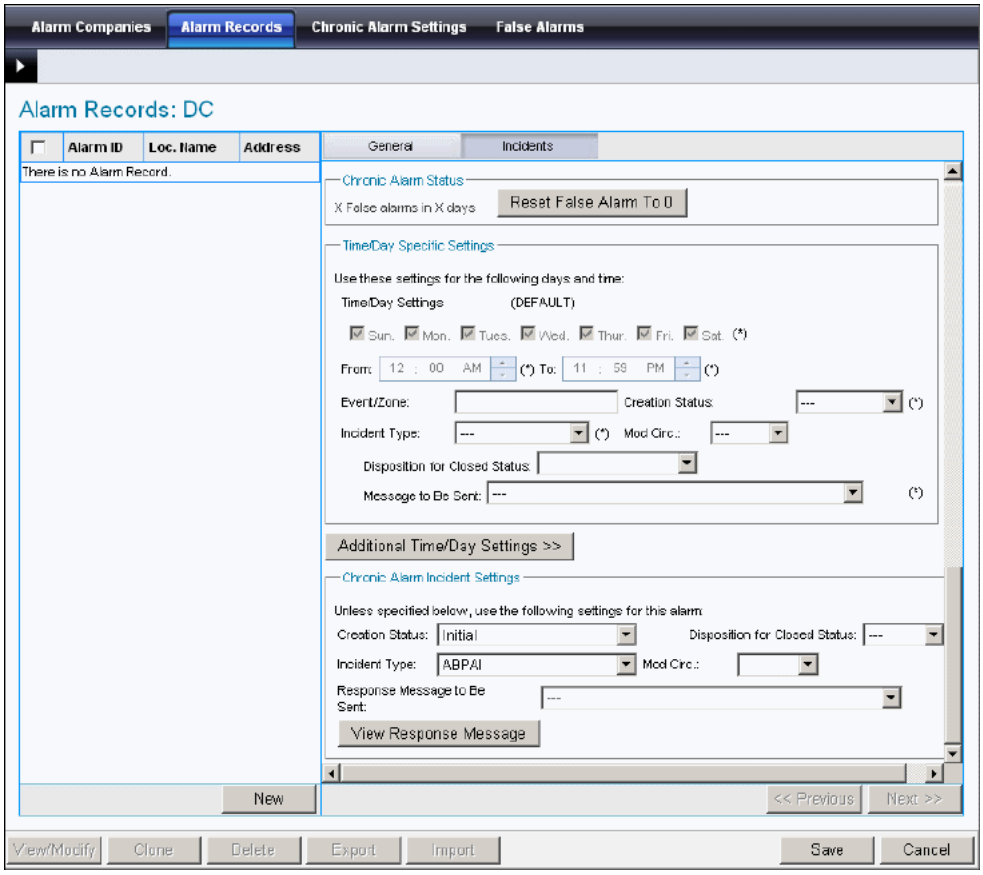


Figure 19-4 Alarm Records – Incidents Tab

4. In the Chronic Alarm Status section, view the number of false alarms that have occurred in the past X number of days; for example, 5 false alarms in 21 days.

   To reset the false alarm count, click **Reset False Alarm to 0**.

   The Time/Day Specific settings are read-only and are set to 7 days a week, 24-hours a day. To enter exceptions to these settings, select the **Additional Time/Day Settings** button, and enter the exceptions. You can select the button multiple times for more than one exception.

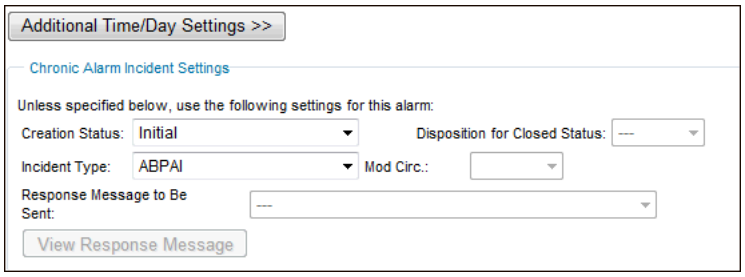


Figure 19-5 Additional Time/Day Settings

5. Enter the following values:

   - Event/Zone – Type of occurrence or area of occurrence.
   - Creation Status – The initial status for the incident (required).
   - Incident Type – The incident type for the incident (required).
   - Mod Circ – Modifying circumstance for incident.
   - Disposition for Closed Status – If the initial status is Closed, the disposition for the incident.
   - Message to be Sent – Message to attach to the alarm incident as a comment.

   Messages are created in the Response Message item of the Incident Management configuration item. For details, see "Configuring Response Messages" on page 13-45.

6. In the Chronic Alarm Incident Settings section, select values from the following lists for chronic alarms:

   - Creation Status – The initial status for the incident.
   - Disposition for Closed Status – If the initial status is Closed, the disposition for the incident.
   - Incident Type – The incident type for the incident.
   - Mod Circ – The modifying circumstance for the incident.
   - Response Message to Be Sent – The response message to attach to the incident.

   Messages are created in the Response Message item of the Incident Management configuration item. For details, see "Configuring Response Messages" on page 13-45.

   Each unsaved record appears in the Agency Records list on the left in blue text.

7. Click **Save**.

   The records you added appear in the Agency Records list in black text.

Configuring Chronic Alarm Settings

Use the Chronic Alarm Settings configuration item to manage chronic alarm settings. A chronic alarm violator is an alarm location that has been responded to and has exceeded the maximum count of allowable false alarms in a specified time frame. When the maximum alarms has been reached, the grace period changes to zero and chronic alarm violators are subjected to the configuration elements you enter upon the next alarm generation.

Dispositions for chronic alarms are set in "Configuring Dispositions" on page 13-43.

NOTE

You can only modify chronic alarm settings. You cannot add or delete chronic alarm settings.

To configure a chronic alarm setting:

1. From the navigation panel, select **Alarm**, and then select **Chronic Alarm Settings**.

   The Chronic Alarm Settings form appears.

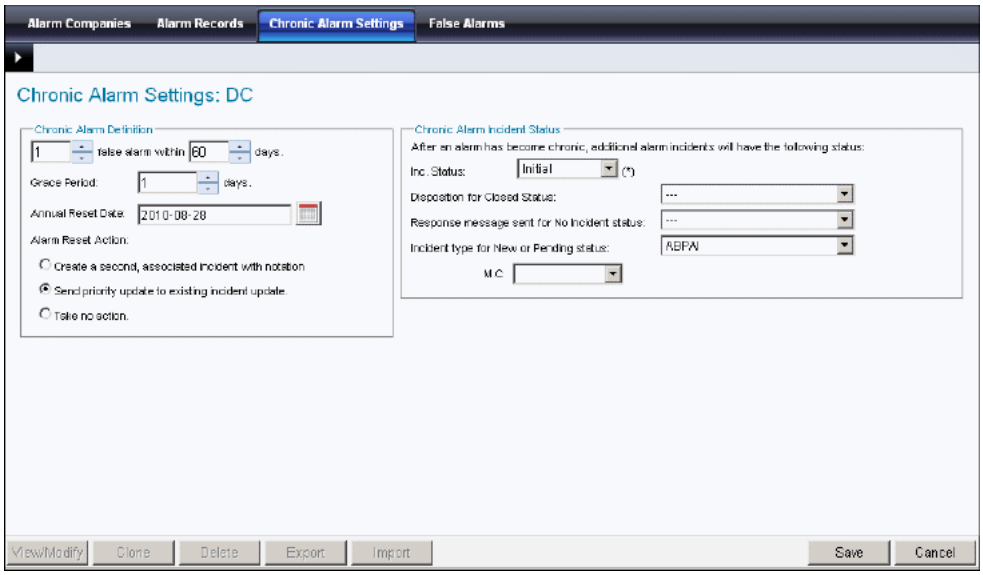


Figure 19-6 Chronic Alarm Settings Information in Work Area

2. In the Chronic Alarm Definition section, do the following:

   a. Indicate how many false alarms can occur within how many days before an alarm is considered chronic.

   b. Enter the grace period, if any, that you allow, and specify the annual reset date.

   c. In the Alarm Reset Action field, select the action to take when the alarm is reset.

- Create a second, associated incident with notation – Create a separate associated incident and add a comment regarding the alarm.
- Send priority update to existing incident update – Send a priority update to the existing incident
- Take no action – Do not take any action

3. In the Chronic Alarm Incident Status section, select the status for chronic alarm incidents.
   a. From the Inc. Status list, select a status for the incident.
   b. If you selected **Closed** in the Inc. Status field, select a disposition in the Disposition required for Closed status field.
   c. If you selected **NoIncident** in the Inc. Status field, select a response message in the Response message sent for No Incident status field.
   d. If you selected **Initial** or **Pending** in the Inc. Status field, select an incident type in the Incident type for New or Pending status field.
   e. From the M.C. list, select a modifying circumstance for the incident.
4. Click **Save**.

Viewing False Alarms

Use the False Alarms configuration item to view incidents that had a false alarm disposition. You can only view false alarm records and set records to active/inactive.

You access the False Alarms form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

Modify a false alarm when you need to change an active false alarm record to inactive.

To view a false alarm:

1. From the navigation panel, select **Alarm**, and then select **False Alarms Settings**.

   The False Alarms information form appears. By default, the false alarms that occurred on the current day display.

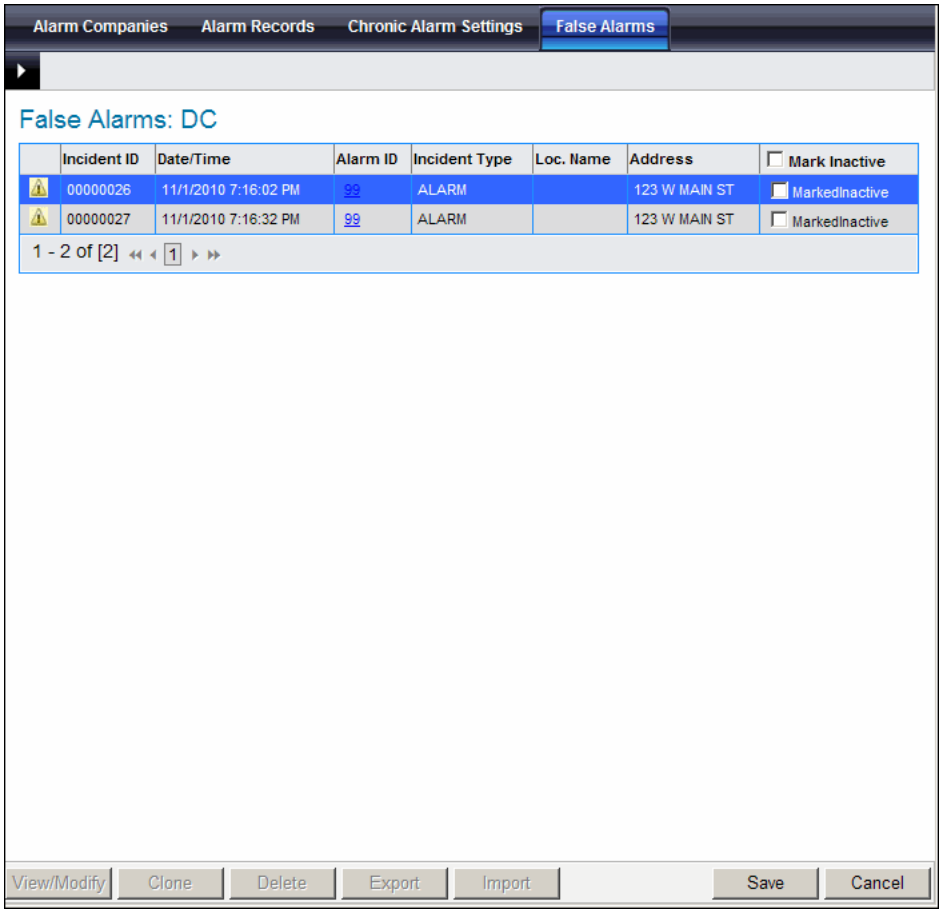


Figure 19-7 False Alarms Form

2. View the information.

3. Do any of the following:

   - To mark any false alarm record as inactive, select the **Mark Inactive** check box for that row. Then select **Save**.

- To view the Alarm associated with record, click the Alarm ID number.

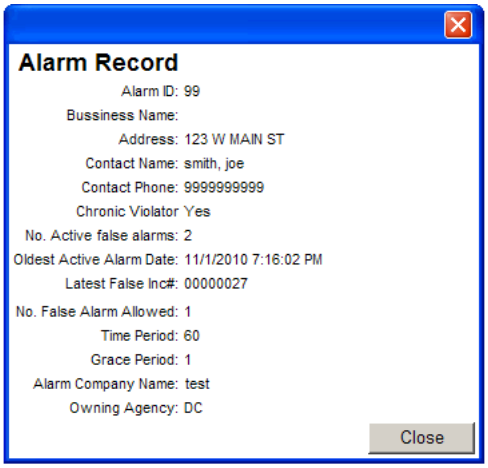


Figure 19-8 Alarm Record Dialog Box

CHAPTER 20

Configuring Chat Rooms

The Chat Room configuration item contains the following items:

- Chat Permission – Where you configure cross agency chat permission. For details, see “Configuring Chat Permissions” on page 20-1.
- Settings –Where you configure the icons used for various chat statuses and for audio and visual alerts, history settings, and delivery options. For details, see “Configuring Chat Settings” on page 20-5.
- Chat Rooms – Where you create and set the properties for chat rooms. For details, see “Configuring Chat Rooms” on page 20-9.

Two types of chat rooms are available:

- Public chat rooms – These can be permanent or temporary and are open to all users. Permanent public chat rooms persist even when members are not part of the chat. Temporary public chat rooms are automatically deleted when the last member of the chat leaves.
- Private chat rooms – These can be created by any user with the proper permissions to have private conversations with other users. Other users can only join the chat room by invitation.

Configuring Chat Permissions

Use the Chat Permissions configuration item to configure the agencies and agency types that can share chat rooms. You can have different agencies share a chat room, different agency types share a chat room, or different agencies and different agency types share a chat room.

Setting Agency-Level Chat Permissions

You can set up Chat room sharing at an agency level, which gives you precise control of the chat room sharing between agencies. For example, you could set the “Northside” law agency to be able to chat with the “Northside” fire and law agencies, the “Southside” law agency, but not the “Southside” fire agency.

If you wanted the “Northside” law agency to be able to share chat rooms with all selected agency types, such as law, EMS, or fire, use “Setting Agency Type Permissions” on page 20-4.

To set agency-level chat permissions:

1. From the navigation panel, select **Chat Room** and then select **Chat Permission**.

   The Chat Permission form appears. A list of available agencies displays on the left side of the form, along with the default agency type.

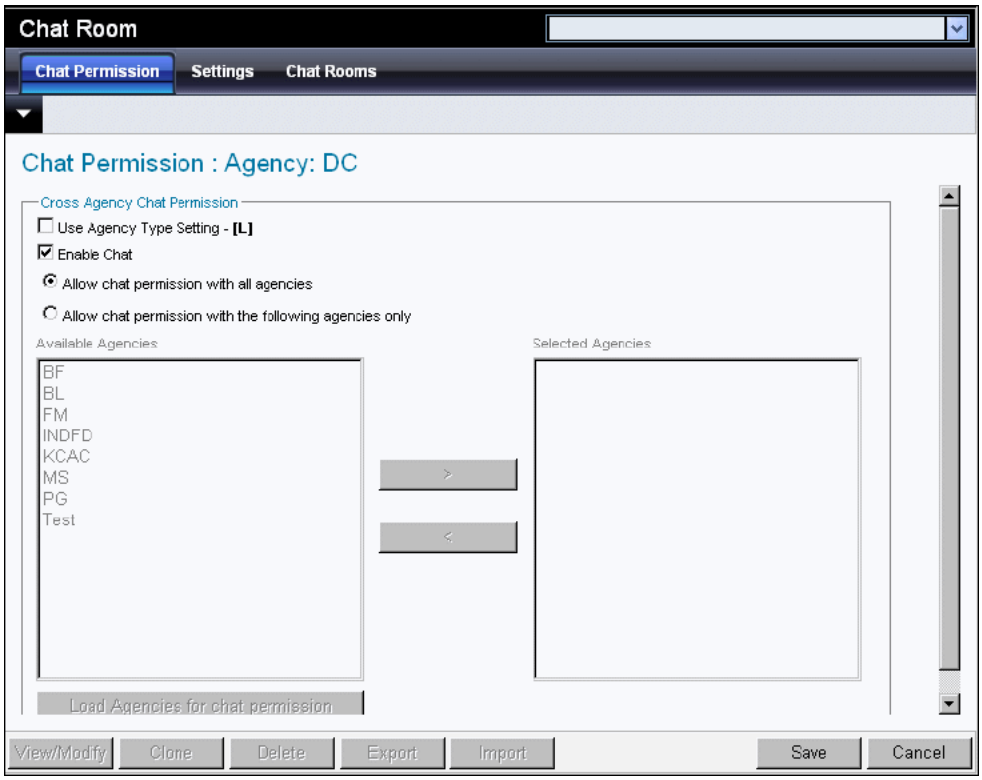


Figure 20-1 Chat Permission Form – Agency Level

2. Click the **View/Modify** button.

3. By default the **Use Agency Type** setting is selected. If you want all agencies of a type (for example L for Law) to be able to chat with each other, click **Save**.

   You are done configuring chat permissions.

4. If you want to allow chat with all agencies, clear the **Use Agency Type Setting** check box. Ensure that the **Enable Chat** check box and **Allow chat permission with all agencies** are selected, and then click **Save**.

5. If you want to choose the agencies that can chat with the selected agency, clear the **Use Agency Type Setting** check box. Select the **Enable Chat** check box and the **Allow chat permission with the following agencies only** button.

   The Available Agencies list is populated with all available agencies.

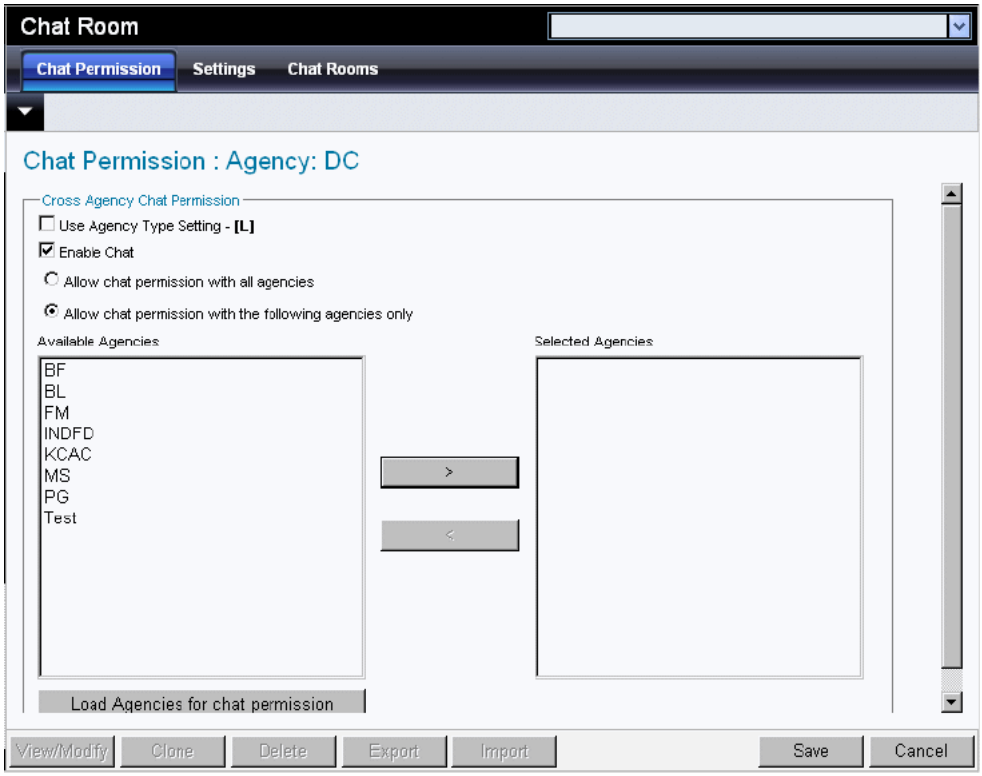


Figure 20-2 Chat Permissions Form – Available Agencies List

6. From the Available Agencies box, select one or more agencies that you want to have chat capability with this agency. Click the arrow to move your selected agencies to the Selected Agencies box.

7. When you have the Selected Agencies box correctly populated, click **Save**.

NOTE

The “Load Agencies for Chat Permission” button loads all the agencies that have been granted permission on the agency type settings and populates the “Selected Agencies” list. Clicking this button overrides any previous agency selections made at the agency level.

If one agency (agency A) gets permission to chat with agency F, then agency F automatically gets permission to chat with agency A.

Setting Agency Type Permissions

You can set chat permissions for all specific agency types to automatically include all agencies of that type. For example, when you select a “Fire” agency type, all fire agencies are allowed to chat with each other.

To set agency type permissions for chat:

1. Use the Filter to select the agency type.

   For details on how to use the filter, see “Using Filters” on page 2-7.

2. From the navigation panel, select **Chat Room** and then select **Chat Permission**.

   The Chat Permission Agency Type form appears. A list of agency types display on the left side of the form. The Enable Chat check box is selected.

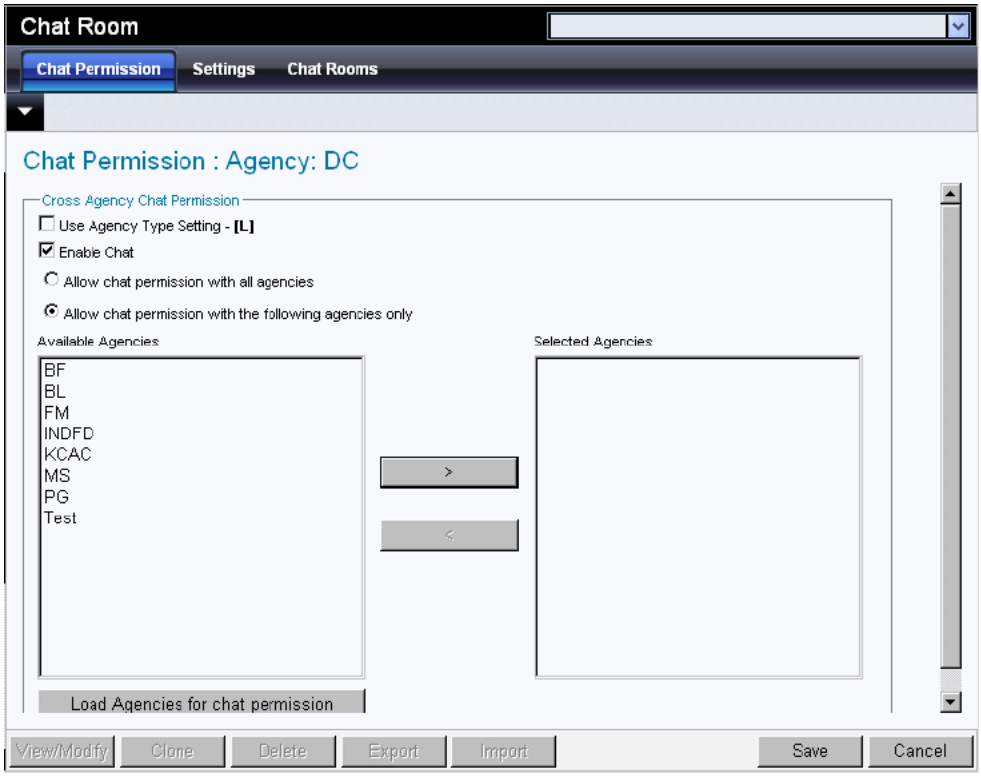


Figure 20-3 Chat Permission – Agency Type Form

3. From the Available Agency Type box, select one or more agency types that you want to have chat capability with this agency type. Click the arrow to move your selected agency types to the Selected Agency Type box.

4. When you have the Selected Agency Type box correctly populated, click **Save**.

Configuring Chat Settings

Use the Chat Settings configuration to configure general chat room settings, such as status, when updates occur, when updates are triggered, and to configure the icons that indicate the user status.

You can configure, modify, and clone chat settings. For details on cloning, see "Working With Configuration Items" on page 2-9.

Configuring Chat Settings

Chat settings apply to all chat rooms for an agency. PremierOne initially provides default settings for an agency which can then be customized. Settings are contained in two tabs: Chat Status and General. The Chat Status tab contains fields that control how the status of users is tracked and displayed. The General tab contains fields that control chat alerts, terminal history settings, and chat delivery options.

You can also add chat settings by cloning the agency settings.

Chat Settings are on two tabs:

- Chat Status – Where you track and display the status of chat room members.
- General – Where you set chat alerts, terminal history settings, and delivery options.

Configuring Chat Status Settings

The chat status settings for an agency are the settings that track and display the status of chat room members. These properties include the name of the status (such as away), how status updates occur, when status updates are triggered, and the icons to use to show user status.

To modify chat status settings:

1. From the navigation panel, select **Chat Room** and then select **Settings**.

The Chat Status tab of the Chat Settings form appears in the work area (see Figure 20-4). A list of agencies displays on the left side of the form. The possible types of chat statuses display on the left side of the window and the properties for the status display on the right side of the window.

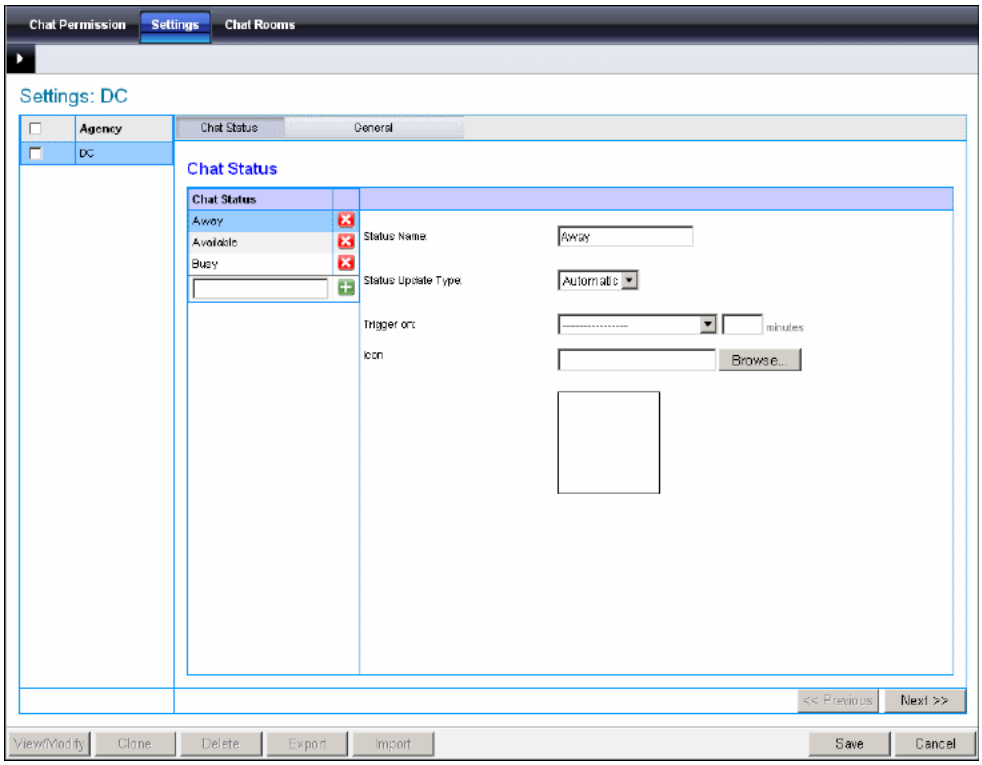


Figure 20-4 Chat Status Form – Chat Status Tab

2. Click **View/Modify**.

   You can now edit the fields on the form.

3. Do one of the following:

   - To set the properties for an existing status, select the status, and then modify the properties on the right side of the window.
   - To add a status, enter the name in the blank field at the bottom of the list of statuses and click the plus icon to the right of the field to add the status. Then enter the properties on the right side of the window.

   Properties include the following:

   Status Name – The name of the status, such as Away, Available, or Busy.

   Status update type – Whether status updates occur automatically, when the user requests them, or both.

Trigger on – When status updates are triggered and the chat status icon is updated. Options include when the Chat Window is hidden, when the user signals an emergency, when the screen is idle for a set amount of time, and when the screen saver is activated for a set amount of time. For all values except emergency, enter the time in minutes in the field to the right of the Trigger on field.

Icon – The image to use to display the chat status. Click the **Browse** button and navigate to and select the image to use. This image displays in chat rooms. You can use the following file formats for icons: GIF, JPG, JPEG, PNG, and BMP. PremierOne resizes the icon image, therefore there are no minimum or maximum image sizes.

4. Click **Save**.

Configuring General Chat Settings

General chat settings for an agency consist of alerts, terminal history settings, and delivery options.

Before modifying general chat settings, you must complete the steps in “Configuring Chat Status Settings” on page 20-5.

To modify general chat settings:

1. Open the Chat Settings form.

   For details, see “Configuring Chat Settings” on page 20-5.

2. From the Chat Settings form, select the General tab.

Fields for general chat settings display.

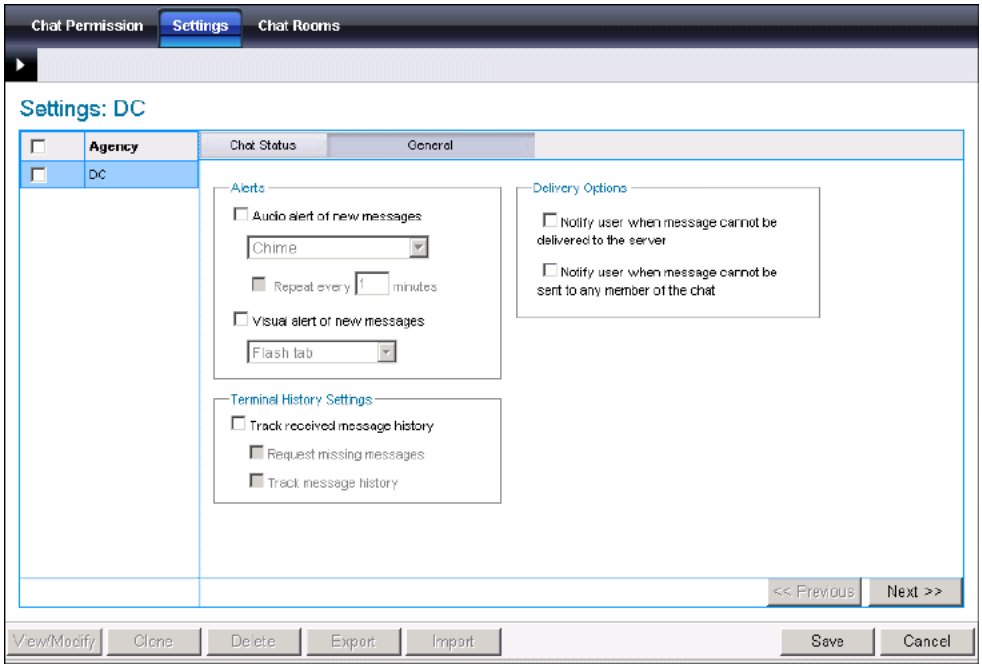


Figure 20-5 Chat Settings Form – General Tab

3. In the Alerts box, enter the visual and audio alert settings for notifications when new messages arrive in chat rooms.

4. If you want the history of received messages to be tracked, select the Track received message history check box. Then select one of the following:

   - If you want to request any messages that could be missing, select the Request Missing Messages check box.
   - If you want to track the message history, select the Track Message History check box.

> **NOTE**
> Terminal History Settings must be enabled in order for users to search Chat Room Results.

5. In the Delivery Options section, do any of the following:

   - To notify members when the chat message can't be delivered to the server, select the Notify User When Message can't be sent to the server check box.
   - To notify members when a message can't be delivered to a chat room member, select the Notify User When Message can't be sent to any member of the chat check box.

6. Click **Save**.

Configuring Chat Rooms

Use the Chat Rooms configuration form to add chat rooms. Chat room properties consist of general properties and a list of members.

You can add, modify, clone, and delete chat rooms. For details on cloning and deleting, see "Working With Configuration Items" on page 2-9.

Adding Chat Rooms

Settings for chat rooms are in three tabs:

- General – Contains settings for the name, owner, description, type of chat room (public or private), deletion rules, member limits and updates, and message history.
- Member – Displays a list of chat room members and their properties.
- Add Member – Used to add chat room members.

You can also add a chat room by cloning an existing chat room that closely matches the one you want to add.

Adding General Chat Room Settings

General chat room settings include the name, owner, description, type of chat room (public or private), deletion rules, and maximum number of members.

To configure general chat room settings:

1. From the navigation panel, select **Chat Room** and then select **Chat Rooms**.

The Chat Rooms form appears with the General tab in focus. A list of existing chat rooms displays on the left side of the form.

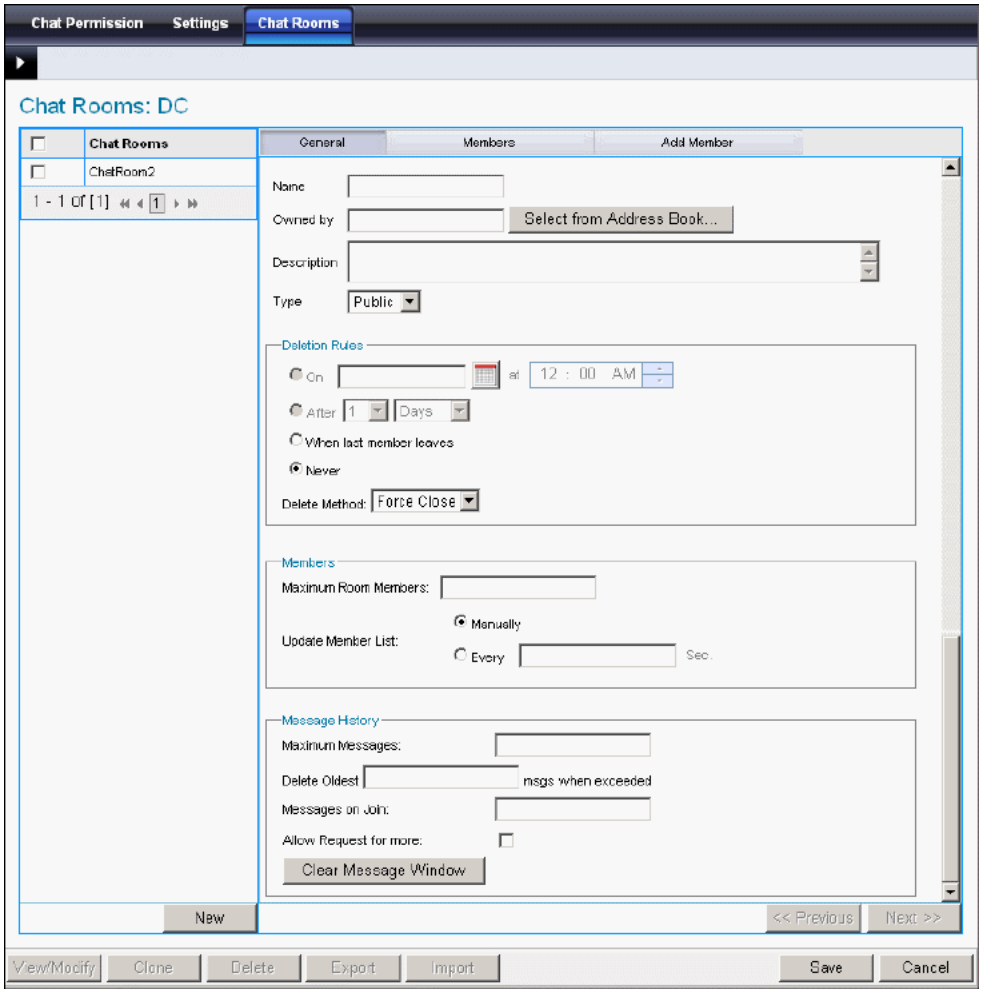


Figure 20-6 Chat Rooms Form – General Tab

2. At the bottom of the Chat Room list, click the **New** button.

   You can now edit the fields on the form.

3. Enter the relevant information for the chat room.

   Chat rooms can be public or private. Public chat rooms are open to all users whereas private chat rooms are only open to users who are specifically invited to join the chat room.

4. Click **Save**.

Adding Chat Room Member Properties

The Members tab for a chat room displays a list of members who are currently in the chat room. In this tab, you can view responses from members, invite members, re-invite members, configure member properties, block members, remove members, delete members, and Re-send invitations to chat members.

To configure chat room member properties:

1. Open the Chat Rooms form.

   For details, see "Adding Chat Rooms" on page 20-9.

2. From the Chat Room form, select the Members tab.

   A list of existing members displays.

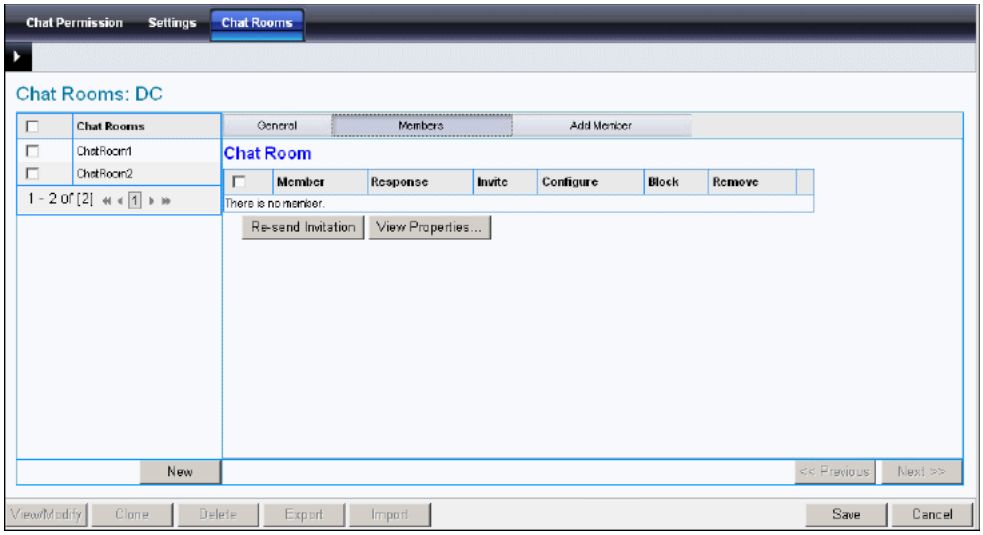


Figure 20-7 Chat Rooms Form – Members Tab

3. Do any of the following:

   - To invite a member to the chat room, select the **Invite** check box for the member.
   - To re-invite a member to the chat room, select the members and click **Re-send Invitation**.
   - To configure the properties for a member, select the **Configure** check box for the member.
   - To block a member, select the **Block** check box for the member.
   - To remove a member, select the **Remove** check box for the member.

- To delete a member, select the member and click the delete icon at the end of the row for the member.
- To view the properties of the member, including whether they are online, select the member and click **View Properties**.

4. Click **Save**.

Adding Members to Chat Rooms

Use the Add Members tab to add members to a chat room.

To add members to the chat room:

1. Open the Chat Rooms form.

   For details, see "Adding Chat Rooms" on page 20-9.

2. From the Chat Room form, select the Add Members tab.

   Fields for adding members display.

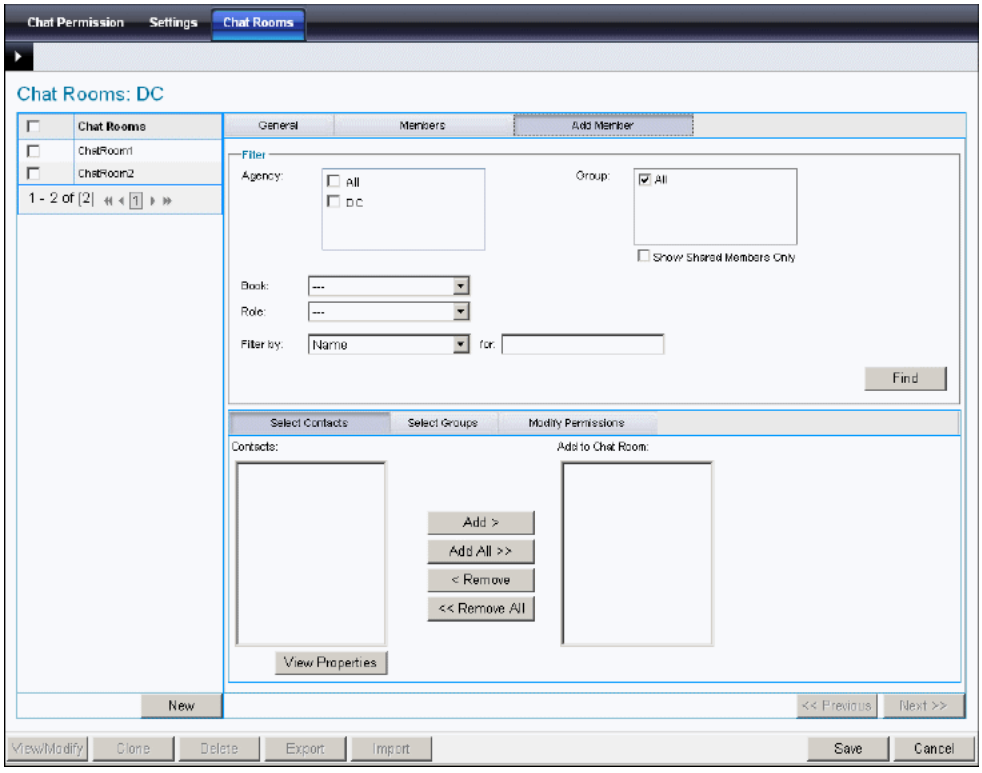


Figure 20-8 Chat Rooms Form – Add Members Tab

3. In the Agency box, select the agencies for which you want to view members.

   You must select the Agency to Activate the other fields.

4. Do any of the following, as required:
   - In the **Group** box, select the groups from which you want to add members.
   - From the Book list, select the address book you want to search for members.
   - From the Role list, select the role for the contacts.
   - From the Filter by field, select the criteria you want to use as a filter and then enter the text in the box to the right. For example, you could select the Filter Name and then enter the name Smith to search for all contacts with the last name of Smith.
5. Do one of the following:
   - To search for contacts with the specified criteria, select the **Select Contacts** tab.

     Contacts display in the Contacts list.
   - To search for groups with the specified criteria, select the **Select Groups** tab.

     Groups display in the Groups list.
6. From the Contacts or Groups list, select the contacts or groups to add and click the right arrow to add them to the Add to Chat Room list.
7. Repeat the procedure for any other chat rooms that you want to add.

   Each unsaved chat room appears in the list on the left in blue text.
8. Click **Save**.

   The chat rooms you added display in the list on the left in black text.

CHAPTER 21

Configuring the Command Line

The Command Line configuration item contains the following items:

- Commands – Where you can view, add, and modify commands. For details, see “Configuring Commands” on page 21-1.
- Identifiers – Where you can view the name of an identifier and the commands in which it is used, and configure aliases for identifiers. For details, see “Configuring Identifiers” on page 21-7.
- Separators – Where you can manage command line separators. For details, see “Configuring Separators” on page 21-8.
- Behaviors – Where you modify the default behavior for whether dynamic help and command line errors are shown on the command line. For details, see “Configuring Command Line Behaviors” on page 21-10.

Configuring Commands

Use the Commands configuration item to add and modify commands. Add a command when you want to alias one of the default Motorola commands. You can then modify the aliased command. You cannot create a totally new command; all commands must be aliased from existing Motorola commands.

You can clone commands and then alias them for easier use. For example, assume you want a single command that always presents the next appropriate or closest ambulance. You could clone the `ID` Command give it a name of `AMB`. In the defaults for the command, select **View/Modify** for the `RL` identifier (response list: count-capability), and then enter whatever the capability for an ambulance is, such as `1-ALS`.

In cases for a multi-casualty incident, you could clone the `ID` command and set it to recommend the next 10 ambulances; this way you would not have to change the incident type.

The default order of the command parameters can also be changed to match the specific operations of your agency, For example, in the case of `IU`, you might want a command where you can enter `IU.Inc#/UnitID.comments` instead of the current default order. You could change the existing order or clone the command with a new name such as `COM`. You could then enter `COM.Inc#/UnitID`.

You can also benefit from cloning the address book (AB) command. You can clone the command, and then alias the command with the default address book, and maybe even default keywords. Adding keywords that match the Personnel skills in Provisioning can aid in quick retrieval with an aliased AB command like SS.

You can add, modify, and clone commands. For details on cloning, see "Working With Configuration Items" on page 2-9.

NOTE

Users will have access to the command set of the agency they signed onto, regardless of whether they change the working agency.

To add a command:

1. From the navigation panel, select **Command Line**, and then select **Commands**.

A list of all commands appears.

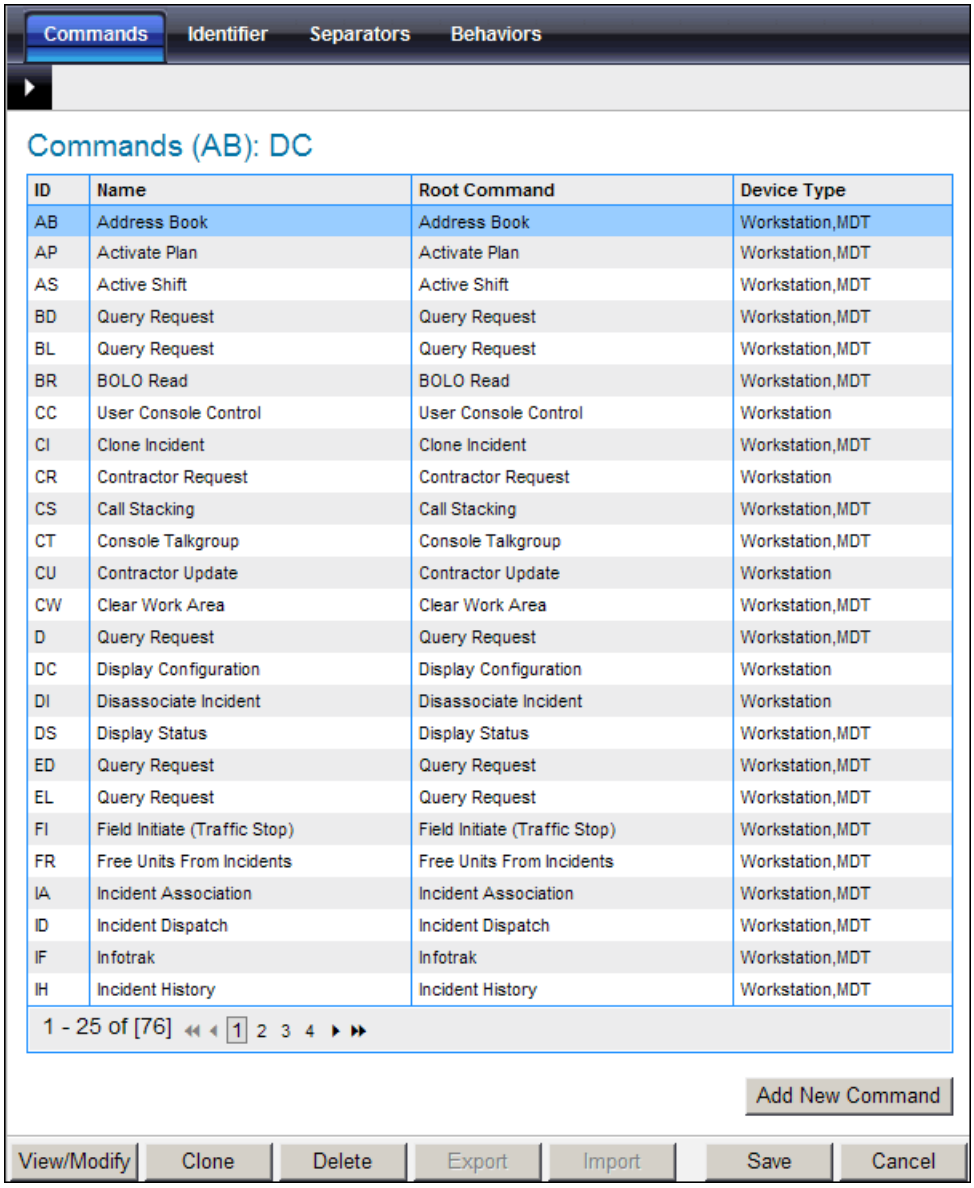


Figure 21-1 Command Form Showing List of All Commands

2. Click **Add New Command**.

A blank Commands form appears.

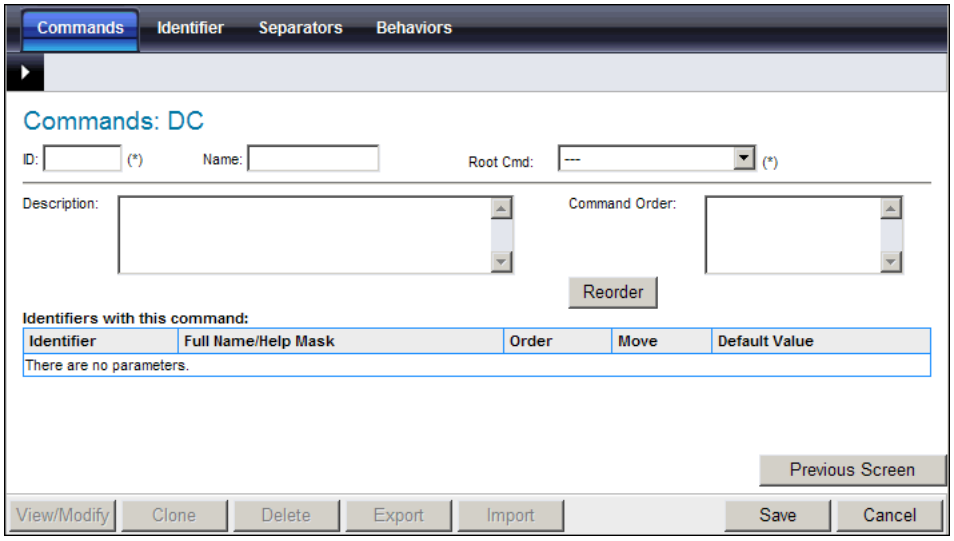


Figure 21-2 New Command Form

3. From the Root Cmd list, select the command you want to use as a template for your new command, and then click **Add New Command**.

The Description, Command Order, and Identifiers for the selected root command appear in the corresponding fields.

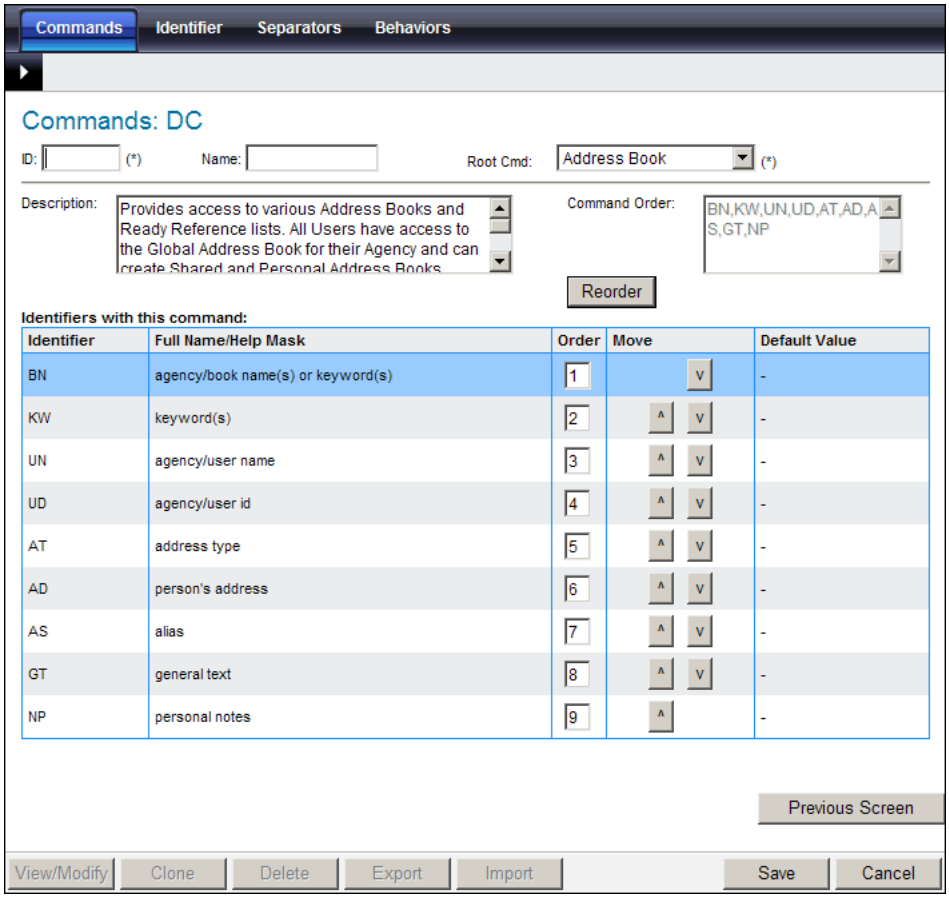


Figure 21-3 New Command Form - Root Cmd Selected

4. In the ID field, type a unique ID for the new command.
5. In the Name field, type an alias name of the new command.
6. In the Description field, make any necessary changes to the command description.
7. To change the order of the identifiers, select an identifier, and then click the up or down button to move the identifier up or down in the table.

   To exclude an identifier from the new command, type a zero (0) in the Order field for that identifier.
8. Click the **Reorder** button.

   The identifiers redisplay in the new order.
9. To modify the information about an identifier, click **View/Modify**.

The editable list of identifiers appears.

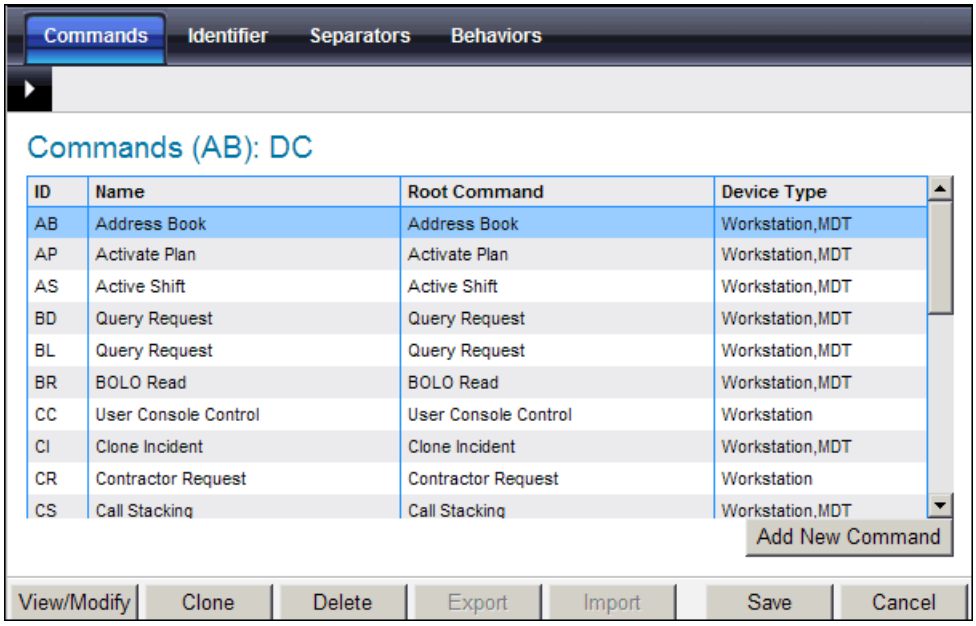


Figure 21-4 Editable List of Identifiers

10. Select the identifier you want to modify.
11. Do any of the following:
    - To use an alias for the identifier, select the alias from the Alias list.

      For instructions on creating aliases, see “Configuring Identifiers” on page 21-7.
    - To change the full name for the identifier, enter the new name in the **Full Name** check box. The Full Name is what displays on the command line.

      You can have a different full name for the identifier for different commands.
    - To specify a default alias, enter the alias in the Default Alias field.
12. Click **Save**.

Configuring Identifiers

Use the Identifier configuration item when you want to see the name of an identifier and the commands in which it is used. You can also configure aliases for identifiers.

These are the default identifiers provided by Motorola. you cannot add or change the default list of identifiers, nor can you delete any of the identifiers.

To modify the order or default value of an identifier that is associated with a specific command, see “Configuring Commands” on page 21-1.

To view command identifiers:

1. Access the form for commands. For instructions, see “Configuring Commands” on page 21-1.

2. Click the **Identifier** tab.

   The Identifier form appears. You can use the alphabetical links at the top of the form to display a list of all identifiers, or the identifiers that begin with a specific letter.

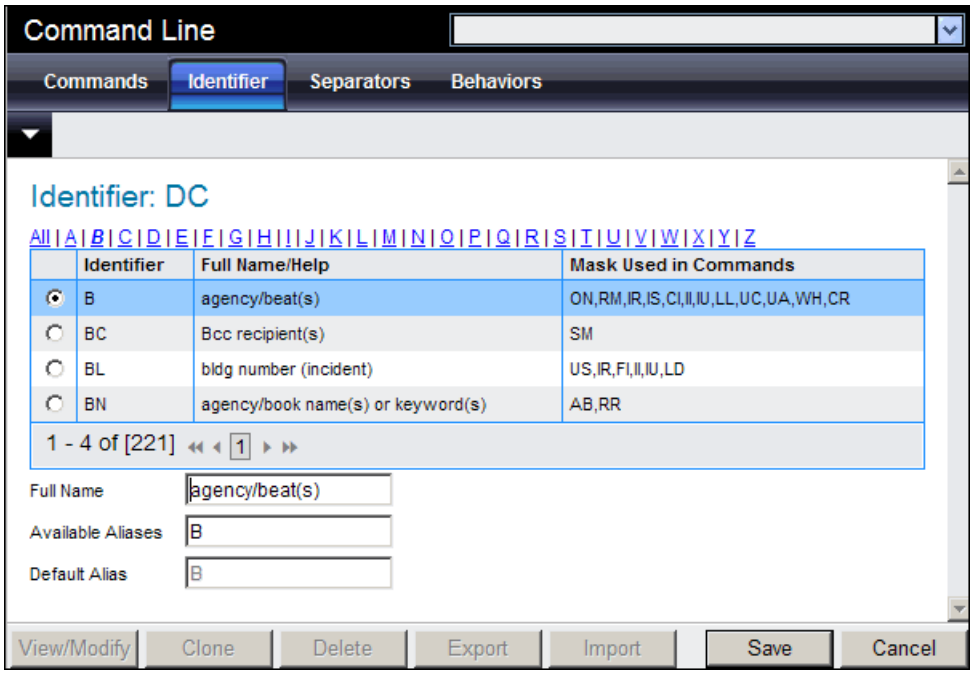


Figure 21-5 Identifier Form

3. Select the identifier you want to view or modify.

   PremierOne populates the fields at the bottom of the form with the identifier’s name and alias information.

4. In the Full Name field, enter the default name that you want to display for the identifier in the dynamic help on the command line.

   For example, for the identifier AG, you might want to display Agency.

   This is the default value for the name. You can enter other values for the name for the identifier for each command. For details, see “Configuring Commands” on page 21-1.

5. In the Available Aliases field, enter the aliases that you want to be made available for the command identifier.

   Different aliases could be used for an identifier in different commands. For example, for address, you agency might use LOC for the CI command and ADR for the II command. Separate the aliases with commas.

   The default alias for each command using this identifier will be the first alias listed in this field.

   You assign these aliases to command identifiers in the Command Line configuration item. This is also where you select the default alias. For details, see “Configuring Commands” on page 21-1.

6. Click **Save**.

Configuring Separators

Use the Separators configuration item to manage command line separators. Separators include the character used to separate commands on the command line, multiple values for the same identifier, name values, command sets, or agency IDs.

Modify separators when you need to use a different character to separate commands on the command line, multiple values for the same identifier, name values, command sets, or agency IDs.

To configure separators:

1. Access the form for commands. For instructions, see “Configuring Commands” on page 21-1.

2. Click the **Separators** tab.

The Separators form appears.

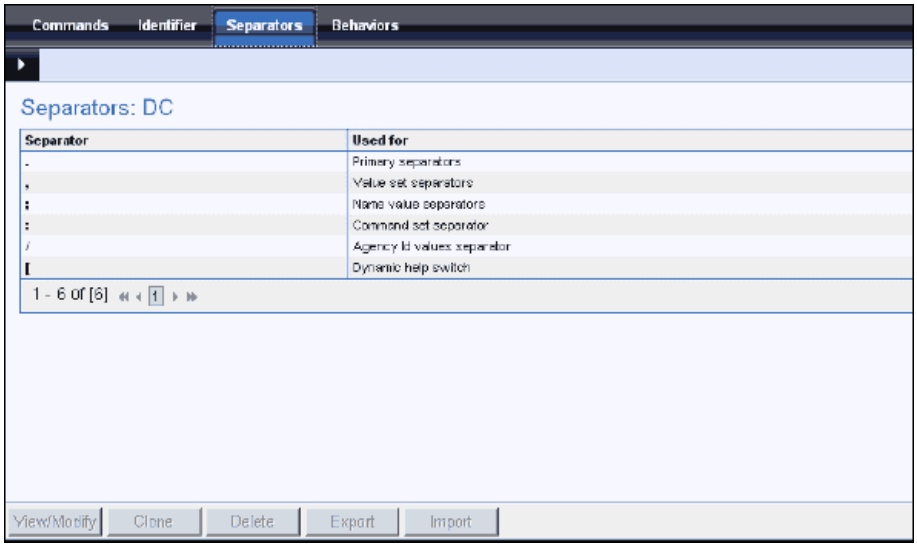


Figure 21-6 Separators Form

3. Select the separator you need to change.

4. In the **Separator** column, select the symbol you want to use.

   - Primary separators – The character used as the separator on the command that indicates the end of the entry of a command or identifier/value pair (default is .). Example: `II.123 w main.theft`

     NOTE
     If your agency uses the CAD-to-CAD Call for Service interface, Motorola recommends that you do not use the tilde (~) as the primary separator as this character is used to reference a foreign agency incident number.

   - Value set separators – The character used to separate multiple values in a listing on the command line (default is ,). Example: `ON.unit1, unit2, unit 3`

   - Name value separators – The character used to separate an identifier from the value entered for use by the identifier (default is ;). Example: `II.L;123 w main st.T;accident`

   - Command set separator – The character used to allow multiple issuances of different values in the same command (like issuing the command twice/more from one command line entry (default is ^).

   - Agency ID values separator– The character used to separate agency ID from other information in values entered on the command line (default is /). Example: `IS.DC/AR1.`

- Dynamic help switch – The character used to turn on/off dynamic help on the command line (default is []).

5. Click **Save**.

Configuring Command Line Behaviors

Use the Behaviors configuration item to control whether dynamic help and command line errors are shown on the command line.

Modify behaviors when you want to change whether dynamic help displays by default and whether command line errors are shown on the command line.

To modify a behavior:

1. Access the form for commands. For instructions, see "Configuring Commands" on page 21-1.

2. Click the Behaviors tab.

   The Behaviors form appears.

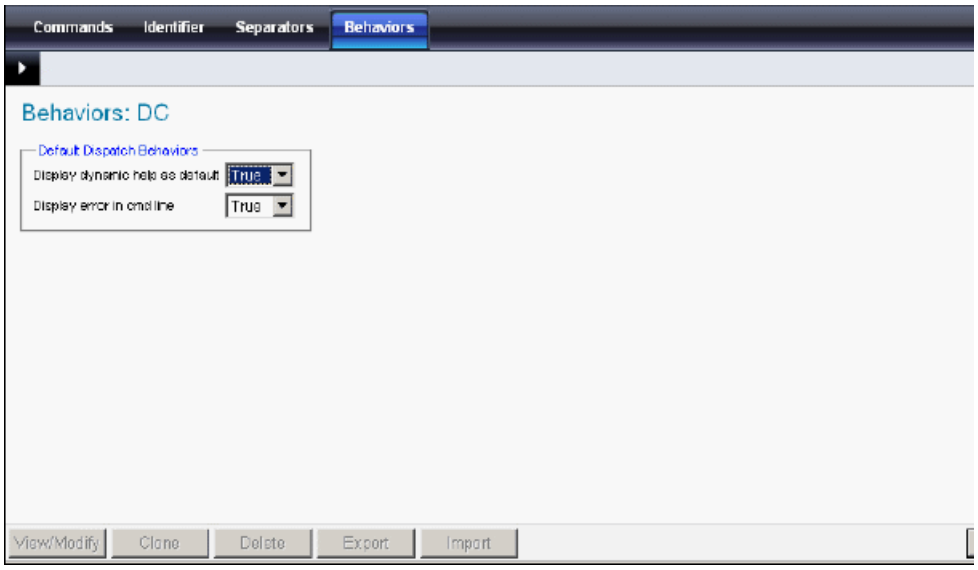


Figure 21-7 Behaviors Form

3. To show command line hints, select **True** from the Display dynamic help as default list.

Each user can override this setting in CAD by selecting **Command Line** from the **Utilities** menu, and then selecting **Dynamic Help**.

Example: When the user enters the II (initiate incident) command, by typing `II` followed by a period, the following appears on the command line indicating that the next identifier in order is `L` (location):

`II.L;<location>`

4. To show errors on the command line, select **True** from the Display error in cmd line list.

   Each user can override this setting in CAD by selecting **Command Line** from the Utilities menu, and then selecting **Syntax Error Notification**.

5. Click **Save**.

CHAPTER 22

Configuring Interfaces

The Interface configuration item contains the following items:

- Alerting – Where you configure toning, paging, and tear-and-run interfaces. For details, see “Configuring the Alerting Interface” on page 22-1.
- External System – Where you configure external interfaces, such as CADfusion™ and LiveMUM™. For details, see “Configuring the External System Interface” on page 22-21.
- Infotrak – Where you configure default data for Infotrak. For details, see “Configuring Infotrak” on page 22-37.
- Q/A – Where you configure the default values for use with Pro QA and ProQA Paramount. For details, see “Configuring the QA Interface” on page 22-39.
- Radio – Where you configure the radios interface. For details, see “Configuring the Radios Interface” on page 22-45.
- Records – Where you configure PremierOne Records to create a CAD incident number or report number to be used for Record cases. For details, see “Configuring the Records Interface” on page 22-56.
- Reporting – Where you configure the name, description, and URL of reporting data warehouses. For details, see “Configuring Names and Descriptions of Reporting Data Warehouses” on page 22-57.

Configuring the Alerting Interface

Alerting is defined as toning, paging, and tear and run. It can be performed automatically based on incident dispatch or manually using the TN command.

NOTE

Be sure you have completed “Adding Systems” on page 11-67 before you configure the Alerting interface.

Use the Alerting configuration item to set up the parameters for your agency for paging, toning, and tear and run, and for printing agency alerts. The Alerting form has seven tabs for the following:

- Settings – Where you enable alerting, set how you will use In-Station and Out-of-Station unit status for auto alerting, and set printing parameters for alerting.
- Alerting Scheme – Where you configure the combination of attributes that are allowed for auto alerting. The alerting scheme defines how the record names are built.
- Toning system – Where you enable toning systems at the agency level.
- In Station Record – Where you configure in-station records at the agency level for any toning system assigned to the agency. This applies to auto alert and to TN manual alerts.
- Out of Station Record – Where you configure out-of-station records at the agency level for any toning system assigned to the agency.
- Override Record – Where you configure unit-based alerting records that override the default behavior of the Alerting Scheme. This applies to auto alert and to TN manual alerts.
- Response Parameters – Where you configure common response parameters for all toning statuses

NOTE

Auto Alerting uses the “In-Station” unit status; therefore, it is critical for unit status definitions to also be properly configured when Auto Alerting is used. If a unit is not “In Station,” auto alerts will not be generated. Think “Not In Station, Not Alerted.” For more information, see “Configuring Unit Status Codes” on page 10-11.

There is also a section called “Alerting Example” on page 22-18 that shows you how PremierOne uses the alerting settings, override record, in-station record, out-of-station record, and Always print alert upon dispatch all together. There is also a section called “Customizing the Alerting Interface” on page 22-20 where you can get information about customization the alerting features.

The following definitions may be of use:

Alerting: The process of sending all types of alerts.

Toning: The process of sending a specific type of alert through toning equipment (fire station alerting).

Alert Type: In CAD, one of the main categories of the Unit Alerting List: Toning, Paging, Tear and Run, Two-Tone Paging, FAX, and so on.

Alerting Type: In toning, a field that is encapsulated within an alert message that is sent to toning equipment. A toning alerting type controls the tone sequence that will be sent so an agency can have toning equipment that sends a different alert signal (tone) for fire than for EMS. When multiple units type are used from the same area covered by the toning device, then the All Call Alerting Type is used, and the equipment sends yet another distinct tone sequence that alerts the station that an ALL CALL was given.

Configuring Alerting Settings

Configure alerting settings to enable alerting, determine how you will use In-Station and Out-of-Station unit status for auto alerting, and to set printing parameters for alerting.

To configure alerting settings:

1. From the navigation panel, select **Interface**, and then select **Alerting**.

   The Settings form appears.

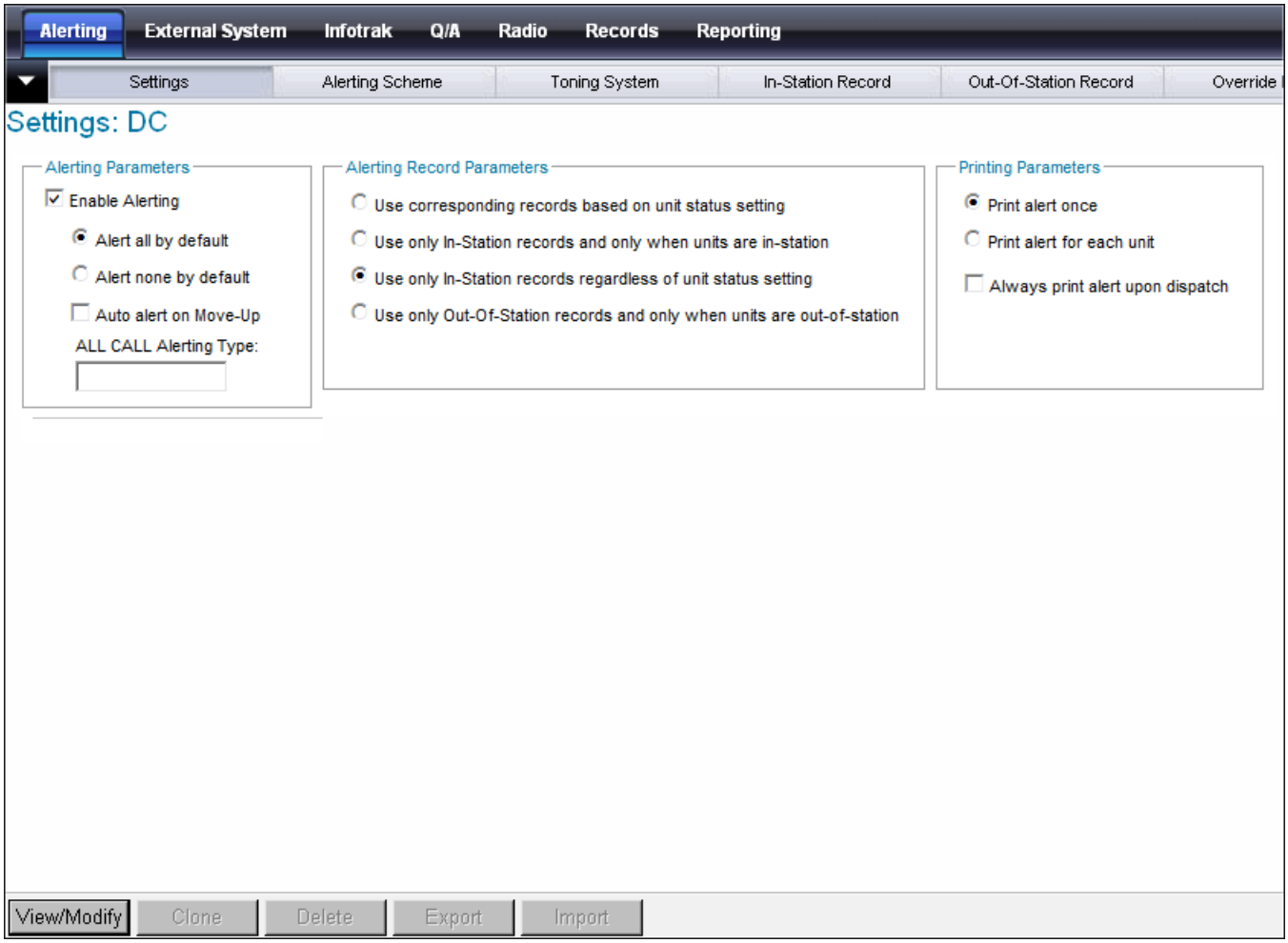


Figure 22-1 Alerting Form – Settings Tab

2. If necessary, select the Settings tab.

3. In the Alerting Parameters section, do the following:

   a. Select the Enable Alerting check box to enable alerting.

   NOTE
   If you do not enable alerting, no alerting will occur, even when the TN override identifier is used.

   b. Set how Auto Alert on Dispatch should be used:

   This setting controls whether alerts in the Unit Alerting List are selected. By enabling Auto alert on Dispatch by default, PremierOne builds alert messages on incident dispatch and sends them to relevant pagers, printers, and toning equipment.

   If auto alerting and/or TN commands are being used, Auto alert on Dispatch by default must be enabled.

   - To generate an Alerting List with all the possible items in the Unit Alerting List selected, select the **Auto alert all on Dispatch by default** check box.

     The default behavior for Auto alert all on Dispatch by default is to select all alerts in the Unit Alerting List. However, other provisioning settings and a unit's status can cause some or all of the alerts in the Unit Alerting List to be cleared.

     Using the move up (MU) command with TN;y has no affect and the currently selected list of alerts are sent as provisioned.

     Using the move up (MU) command with TN;n forces all alerts to be cleared from the Unit Alerting List and no alerts are sent.

   - To generate a Unit Alerting List with no items selected, select the **Do not auto alert by default** check box.

     This setting controls whether alerts in the Unit Alerting List are cleared. The default behavior for Do not auto alert by default is to clear all the alerts in the Unit Alerting List.

     Using the move up (MU) command with TN;y forces all alerts to be selected.

     Using the move up (MU) command with TN;n has not meaning because all of the alerts are already cleared.

     Do not auto alert by default takes precedence over the Always print alert upon dispatch field located in the Printing Parameters section.

c. To build alert messages upon Move-Up actions and send them to relevant pagers, printers, and toning equipment, select the Auto alert on Move-Up check box.

d. In the ALL CALL Alerting Type field, type the toning alerting type number used for alerting everyone.

When multiple records are used within the same toning coverage area (station), it is possible that multiple CAD alert types will be found. Because only one CAD alert type can be used within one alert message to a single toning coverage area (station), the user must tell PremierOne which alert type to use. The All Call special toning alerting type can be used in this situation. The All Call alerting type is an agency-wide toning alerting type used when more than one CAD alert type has been found for a particular toning device.

Example:

Assumptions:
Alerting Scheme = Station ID/Duty Type
All Call Alerting Type = 4
Agency = FD
ENG01 = Engine 01
AMB01 = Ambulance 01
FD/ENG01: DutyType = ENG
FD/AMB01: DutyType = EMS
ST01 = Station 01
FD/ST01/ENG: Alert Type = 1, Unit Alerting List = Toning, FD, **1**.
FD/ST01/EMS: Alert Type = 2, Unit Alerting List = Toning, FD, **1**.

If the user enters:
`TN.U;FD/ENG01, FD/AMB01` (to tone two units)

The Unit Alerting List shows:
FD/ENG01
Toning
Device 1, Alert Type 1
FD/AMB01
Toning
Device 1, Alert Type 2

This shows that PremierOne should send CAD alert type 1 and CAD alert type 2 to toning device 1 with a single alert message. However, this is not possible. Therefore, PremierOne looks for the All Call toning alerting type. Because the All Call alerting type is defined as 4, PremierOne builds an alert message for toning device 1 and sets the alerting type to 4 in this message.

4. In the Alerting Record Parameters section, do the following to determine how to use In-Station and Out-of-Station unit status for alerting:

a. To support the following scenarios, select Use corresponding record based on unit location.

Use In-Station records when a unit is in-station, and Out-of-Station records when a unit is out-of-station.

b. To support the following scenarios, select Use only In-Station records and only when units are in-station.

   Use In-Station records when a unit is in-station. No alerting is done when units are out-of-station. Unit status is the most important factor. If a unit is out-of-station, no alerting is attempted, even if pagers are assigned to personnel, vehicles, or units.

c. To support the following scenarios, select Use only In-Station records regardless of unit location.

   Use In-Station records regardless of the unit's status. The units status is ignored.

   Alerting is done independent of a unit's status. Therefore, alerting always uses the assigned alerts (pagers) and the In-Station record(s) to build the Unit Alerting List. The selection of these alerts is controlled only by the default settings of Auto alert on Dispatch by default and Do not auto alert by default.

d. To support the following scenarios, select Use Out-of-Station records and only when units are out-of-station.

   Use Out-of-Station records when a unit is Out-of-Station. Unit status is the most important factor. If a unit is in-station, no alerting is done, even if pagers are assigned to personnel, vehicles, or units.

5. To control how many printed alerts (Tear 'N Run reports) are sent to each printer, select one of the following in the Printing Parameters section:

   - To send one copy of the incident information to each unit associated with the incident, select **Print alert once**.

     Any/all associated printers of a dispatched unit will receive one printout independent of the number of units sent from the same stations.

   - To send one copy of the incident information for each unit to each configured printer if the unit is in the station, select **Print alert for each unit**.

     Each unit will receive a printout on every unit-associated printer.

   - To always print an alert upon dispatch, independent of the unit's status, select the **Always print alert upon dispatch** check box. This setting applies only when one the following options is selected:

     - Use only In-Station records and only when units are in-station
     - Use only Out-Of-Station records and only when units are out-of-station

6. Click **Save**.

Configuring an Agency Alerting Scheme

Configure an agency alerting scheme to allow any combination of a list of attributes to be used for auto alerting.

An alerting record has a named key that is uniquely associated with that record. When a unit is dispatched, the alerting scheme allows PremierOne to build the key for the unit that was dispatched in order to find the appropriate alerting record.

The alerting scheme defines how the record names are built.

Example:

If you select Toning System and Station ID as your alerting scheme, and your agency is `FD`, your selected toning system is `Z25`, and you selected station is `S01`, then your alert record name becomes agency name + the toning system + the station ID, or **FD-Z25-SO1**.

It is important to remember that the alerting scheme does not control the content of the records.

If an alerting record cannot be found, or if the record is found but is blank, the Unit Alerting List will only include pagers, if any.

To configure an agency alerting scheme:

1. Access the form for Alerting. For instructions, see "Configuring Alerting Settings" on page 22-3.

2. Select the Alerting Scheme tab.

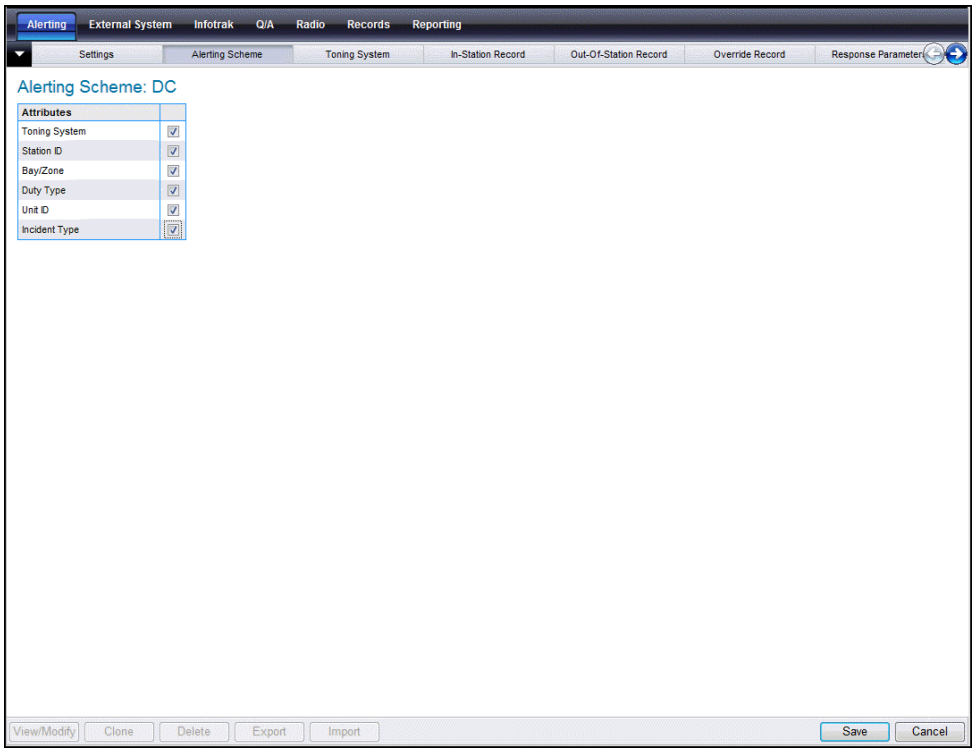


Figure 22-2 Alerting Form – Alerting Scheme Tab

3. In the Attributes box, select the check box next to each attribute you want to use for auto alerting. You may select as many as you want.

4. Click **Save**.

Configuring and Enabling Existing Toning Systems at the Agency Level

Configure toning systems at the agency level to enable them for your agency's use. You may want to configure more than one toning system so you can activate your main system for normal use, and then activate your backup system if needed.

To configure and enable existing toning systems at the agency level:

1. Access the form for Alerting. For instructions, see "Configuring Alerting Settings" on page 22-3.

2. Select the Toning System tab.

A list of currently configured and enabled toning systems, if any, display in the Toning System list on the left side of the window.

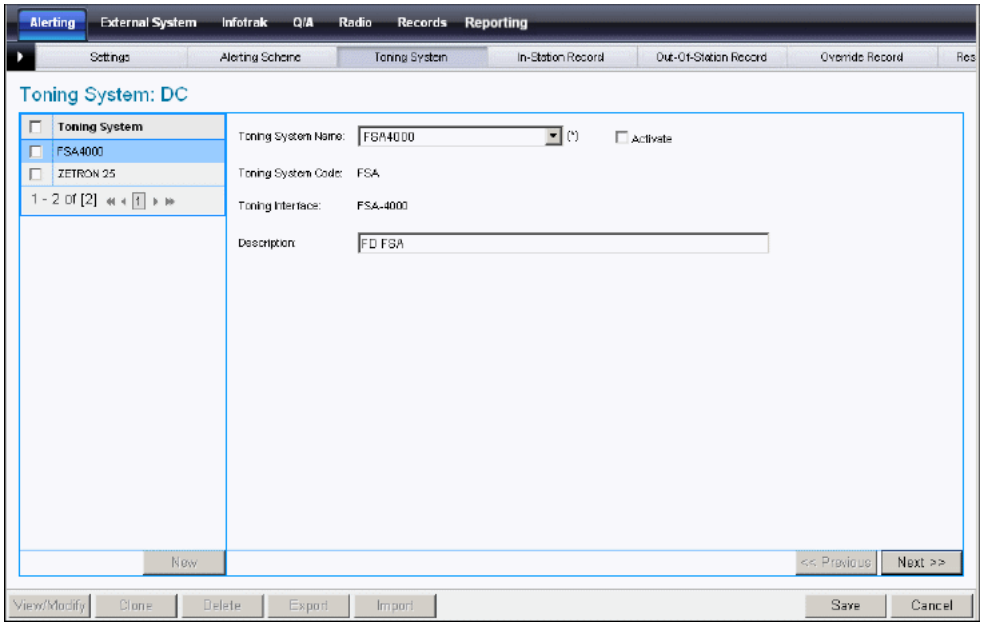


Figure 22-3 Alerting Form – Toning System Tab

3. From the Toning System Name list, select a name from the list of system names.

   When you select the system name, the Toning System Code and the Toning Interface fields automatically populate.

   An agency can have more than one toning system. This allows the agency to have one toning system activated and a stand-by system ready for backup.

4. In the Description field, type a description for this system for your agency.

5. To activate this system, select the Activate check box.

6. Click **Save**.

Configuring Alerts for In-Station

Configure in-station records at the agency level for any toning system assigned to the agency. This applies to auto alert and to TN manual alerts.

Using the In-Station form, you can do the following:

- Determine what alerts are sent when units are in-station
- Provision the alerting records used for auto alerting
- Clone alerting records to create more records like the one selected and to copy records from one database to another

To configure alerts for in-station:

1. Access the form for Alerting. For instructions, see "Configuring Alerting Settings" on page 22-3.

2. Select the In-Station Record tab.

   A list of currently configured records, if any, display in the Records Name list on the left side of the window.

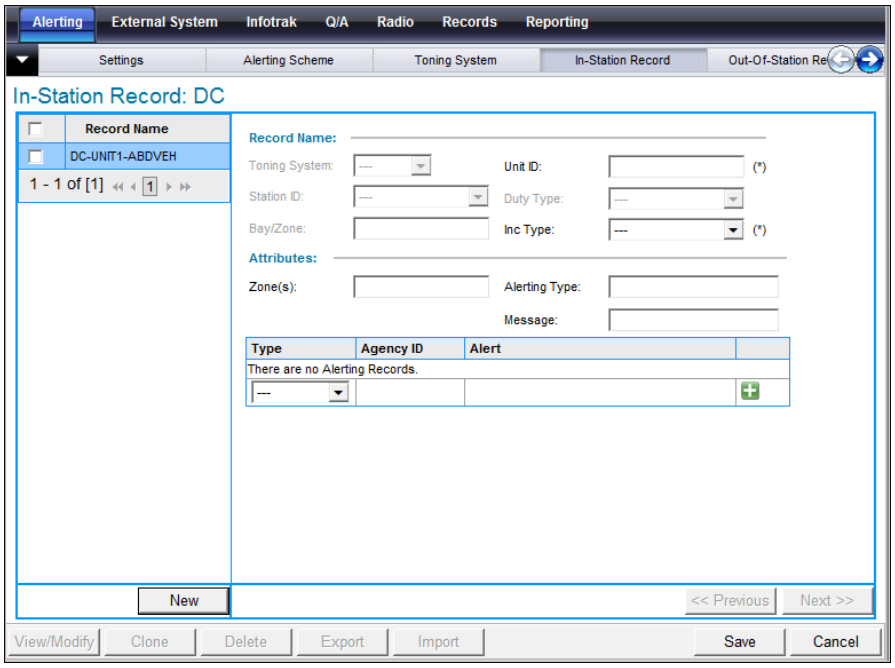


Figure 22-4 Alerting Form – In-Station Record Tab

3. From the Toning System list, select the code for the system your agency is using for its primary system.

4. From the Station ID list, select the station.

Station ID is enabled and required only if it is included in your agency's Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

5. In the Bay/Zone field, type the bay or zone number for toning alerts.
6. In the Unit ID field, type the ID for the unit.

   Unit ID is enabled and required only if it is included in your agency's Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

7. From the Duty Type list, select the duty type.

   Duty Type is enabled and required only if it is included in your agency's Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

8. From the Inc Type list, select the incident type.
9. In the Zones field, enter the name of one or more zones in the fire station. Separate multiple zones with commas.
10. In the Alerting Type field, enter the toning alerting type.
11. In the Message field, type the message for these criteria.

    You can use a maximum of 15 characters.

12. In the Alerting List table, do the following:

    a. From the Type list, select the type of alert, such as external email, fax, pager, pager group, printer, toning, or two-tone radio alert.

    b. From the Agency ID list, select the agency. Agency ID is only used for alerts specific to agencies or defined within an agency.

    c. From the Alert field, select or enter the alert to use. The Alert field is either a list or ope text field, depending on the type of alert being added.

    d. Click the plus symbol to add another row.

    CAUTION
    If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

    e. Repeat for additional Types for this record.

13. Click **Save**.

Configuring Alerts for Out-of-Station

Configure out-of-station records at the agency level for any toning system assigned to the agency. Using the Out-of-Station form, you can do the following:

- Determine what alerts are sent when units are out-of-station
- Provision the alerting records used for auto alerting
- Clone alerting records to create more records like the one selected and to copy records from one database to another

You can clone, export, and import out-of-station records. For details on cloning, exporting, and importing, see "Working With Configuration Items" on page 2-9.

To configure alerts for out-of-station:

1. Access the form for Alerting. For instructions, see "Configuring Alerting Settings" on page 22-3.

2. Select the Out-of-Station Record tab.

   A list of currently configured records, if any, display in the Records Name list on the left side of the window.

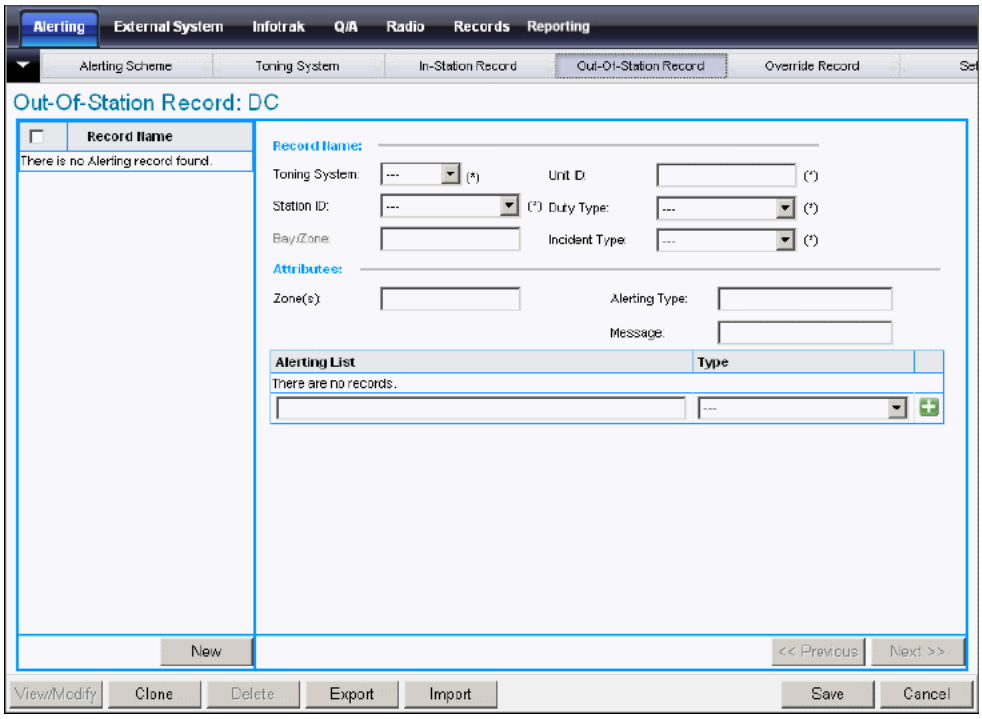


Figure 22-5 Alerting Form – Out-of-Station Record Tab

3. From the Toning System list, select the code for the system your agency is using for its primary system.

4. From the Station ID list, select the station.

Station ID is enabled and required only if it is included in your agency's Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

5. In the Bay/Zone field, type the bay or zone number for toning alerts.
6. In the Unit ID field, type the ID for the unit.

   Unit ID is enabled and required only if it is included in your agency's Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

7. From the Duty Type list, select the duty type.

   Duty Type is enabled and required only if it is included in your agency's Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

8. From the Inc Type list, select the incident type.
9. In the Zones field, enter the name of one or more zones in the fire station. Separate multiple zones with commas.
10. In the Alerting Type field, enter the toning alerting type.
11. In the Message field, type the message for these criteria.

    You can use a maximum of 15 characters.

12. In the Alerting List table, do the following:

    a. In the Alerting List field, select the type of alert, such as external email, fax, pager, pager group, printer, toning, or two-tone radio alert.

       Depending on the option you select, the Agency ID field becomes enabled. Select the agency ID.

    b. From the Alert list, select or enter the type of alert.

    c. Click the plus symbol to add another row.

    CAUTION
    If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

    d. Repeat for additional Types for this record.

13. Click **Save**.

Configuring Unit-Based Alerting Records That Override the Default Scheme

Configure unit-based alerting records that override the default behavior in the Alerting Scheme. When used, this function provides a unit-based alerting record to define how and if the unit should be alerted when dispatched. You can also create blank override records (with only the Unit ID) to allow unit exceptions that require no alerting. This unit record is optional for each and every unit provisioned for an agency. This applies to auto alert and to TN manual alerts.

Override records can be created for *any* unit, including temporary units.

These records are sometimes referred to as override records because they are records for units that are used to override the provisioned Agency Alerting Scheme (see "Configuring an Agency Alerting Scheme" on page 22-7).

Example:

A fire agency may use temporary units that are not in the system; however, the agency wants those units to receive alerts. Therefore, the fire agency would use override records for those units.

You can clone, export, and import override records. For details on cloning, exporting, and importing, see "Working With Configuration Items" on page 2-9.

To configure unit-based alerting records that override the default scheme:

1. Access the form for Alerting. For instructions, see "Configuring Alerting Settings" on page 22-3.

2. Select the Override Record tab.

A list of currently configured override records, if any, display in the Records Name list on the left side of the window.

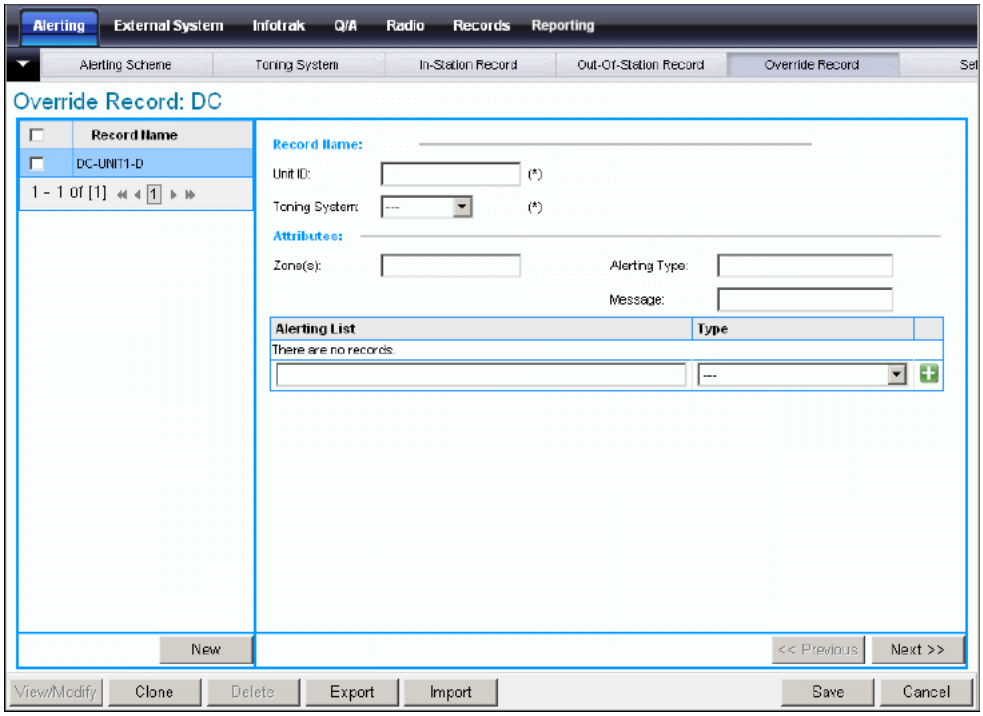


Figure 22-6 Alerting Form – Override Record Tab

3. In the Record Name section, do the following:

   a. In the Unit ID field, type the unit ID of the units whose alerting record you want to override the default alerting scheme. Separate multiple IDs with a comma.

   b. From the Toning System list, select the toning system you are using.

4. In the Attributes section, do the following:

   a. In the Zone field, type the name of the zone in the fire station to which this override applies.

   b. In the Alerting Type field, type the numeric value for the toning alerting type to which this override applies.

   c. In the Message field, type the message for the criteria.

      You can use a maximum of 15 characters.

5. In the Alerting List table, do the following

   a. In the Type field, select a type, such as external email, fax, pager, pager group, printer, toning, or two-tone radio alert.

      The codes in the drop-down list come from “Configuring Devices” on page 11-43.

b. In the Alerting List, type the name that corresponds to the type you selected.

Example:

If you selected Printer in the Type field, type the name of the printer in the Alerting List field. If you selected Pager, in the Type field, type the name of the Pager in the Alerting List field.

c. Click the plus symbol at the end of the row.

CAUTION
If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

d. Repeat the step to add additional types for this record.

6. Click **Save**.

Configuring Common Response Parameters For All Toning Statuses

Configure common response parameters for all toning statuses on an agency level.

These parameters are initially configured in the `Alerting\Alertingprovisioningconfiguration_config.xml` file in the Configuration module of the System Management Tool Portal. For more information, see the *PremierOne System Administrator Guide*. They are used to show the common toning statuses of Public Address (PA) system ON and OFF, Alert Request Sent, and Alert Failure or Success.

To configure common response parameters for all toning statuses:

1. Access the form for Alerting. For instructions, see “Configuring Alerting Settings” on page 22-3.

2. Select the Response Parameters tab.

A list of currently configured response parameters display in the Response Parameters form.

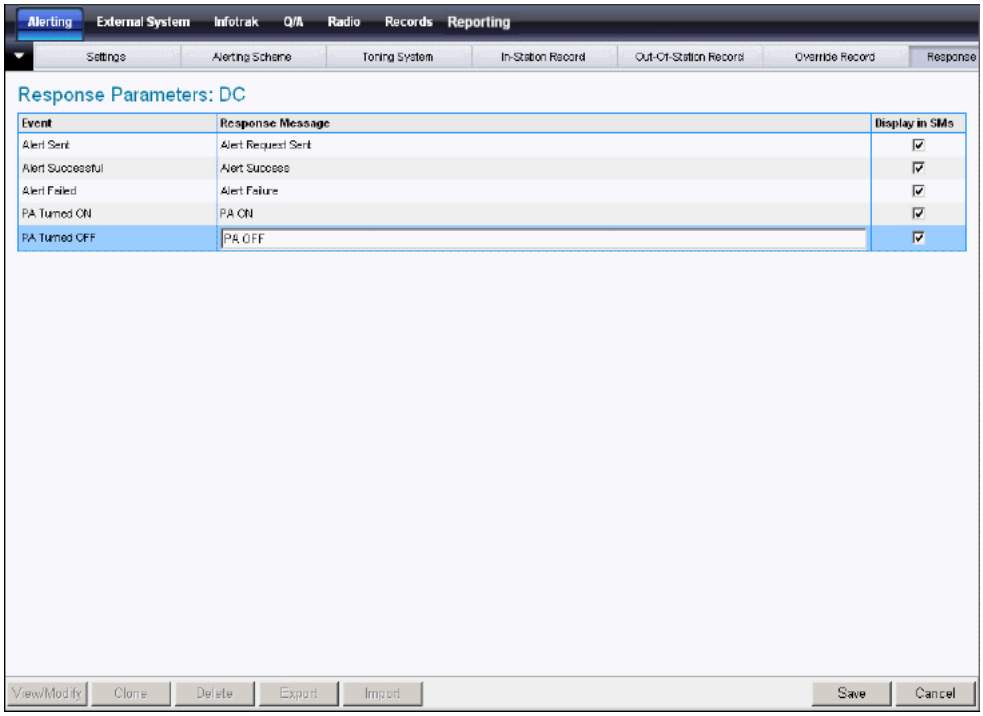


Figure 22-7 Response Parameters Form

3. To edit the response message, click in the Response Message field.

   The field becomes editable. Type your new response message.

   The response message is what appears in alerts and, if selected, in status monitors.

   The original Event/Response Message text comes from the `Alerting\AlertingProvisioningConfiguration.config.xml` file in the Configuration module of the System Management Tool Portal.

4. To cause the listed response message to display in the Toning Status monitor, select the Display in Status Monitors check box.

   Where the toning status message is sent, for example, to which work stations' Toning Status monitors, is determined by the user's sign-on coverage area(s) and station(s).

5. Click **Save**.

Alerting Example

This example shows how PremierOne uses the provisioning of override records, in-station, out-of-station, and Always print alert upon dispatch all together. In addition, the use of the TN identifier is shown.

The steps below are all the things that PremierOne checks and does to build a Unit Alerting List.

1. Check the provisioning of auto alerting.
   - If enabled, continue.
   - If not enabled, stop.
2. Check for unit-assigned alerts (for example, pagers). For more information, see "Configuring Devices" on page 11-43.
   - If assignments exist, add these to the Unit Alerting List.
3. Check for a unit override record. For more information, see "Configuring Unit-Based Alerting Records That Override the Default Scheme" on page 22-14.
   - If one exists, access it and add any alerts to the Unit Alerting List.
4. Check alert provisioning for how to use In-Station status and Always print alert upon dispatch. For more information, see "Configuring Alerts for In-Station" on page 22-10, and "Configuring Alerting Settings" on page 22-3.
   - If provisioned for Use only In-Station records and only when units are in-station:
     - Get the alerts from the in-station record and put the alerts into the Unit Alerting List.
     - If unit is in-station:

       If Auto alert all on Dispatch by default is selected, select all unit alerts.

       If Do not auto alert by default is selected, clear all unit alerts.
     - If unit is out-of-station:

       Clear all unit alerts.

       If Always print alert upon dispatch is selected, select printers on the Unit Alerting List.

       If Do not auto alert by default is selected, clear all unit alerts.
     - If TN;y is used on the command line, select all unit alerts.
     - If TN;n is used on the command line, clear all unit alerts.

Motorola Solutions Confidential

- If provisioned for Use only Out-of-Station records and only when units are out-of-station:
  - Get the alerts from the out-of-station record and put the alerts into the Unit Alerting List.
  - If unit is in-station:

    Clear all unit alerts.

    If Always print alert upon dispatch is selected, select printers on the Unit Alerting List.

    If Do not auto alert by default is selected, clear all unit alerts.
  - If unit is out-of-station:

    If Auto alert all on Dispatch by default is selected, select all unit alerts.

    If Do not auto alert by default is selected, clear all unit alerts.
  - If TN;y is used on the command line, select all unit alerts.
  - If TN;n is used on the command line, clear all unit alerts.
- If provisioned for Use only In-Station records regardless of unit location:
  - Get the alerts from the in-station record and put in the Unit Alerting List.
  - If Auto alert all on Dispatch by default is selected, select all unit alerts.
  - If Do not auto alert by default is selected, clear all unit alerts.
  - If TN;y is used on the command line, select all unit alerts.
  - If TN;n is used on the command line, clear all unit alerts.
- If provisioned for Use corresponding records based on unit location:
  - If unit is in-station, get alerts from the in-station record and put in the Unit Alerting List.
  - If unit is out-of-station, get alerts from the out-of-station record and put in the Unit Alerting List.
  - If Auto alert all on Dispatch by default is selected, select all unit alerts.
  - If Do not auto alert by default is selected, clear all unit alerts.
  - If TN;y is used on the command line, select all unit alerts.
  - If TN;n is used on the command line, clear all unit alerts.

Customizing the Alerting Interface

Your agency may want to customize the Alerting interface to more closely meet the agency's specific needs, such as customizing outputs from tear and run messages.

To customize the Alerting interface:

1. From the System Management Tool Portal, select **Configuration**.
2. Click the Edit tab.
3. To customize Tear and Run output:
   a. In the box on the left, scroll down until you find `PagingToningTnRDataFormat`.
   b. Click the following option: **PagingToningTnRInterface\PagingToningTnRDataFormat_config.xm**.

      The `pagingtoningtnrinterface\pagingtoningtnrdataformat_config.xml` file opens in the box on the right.

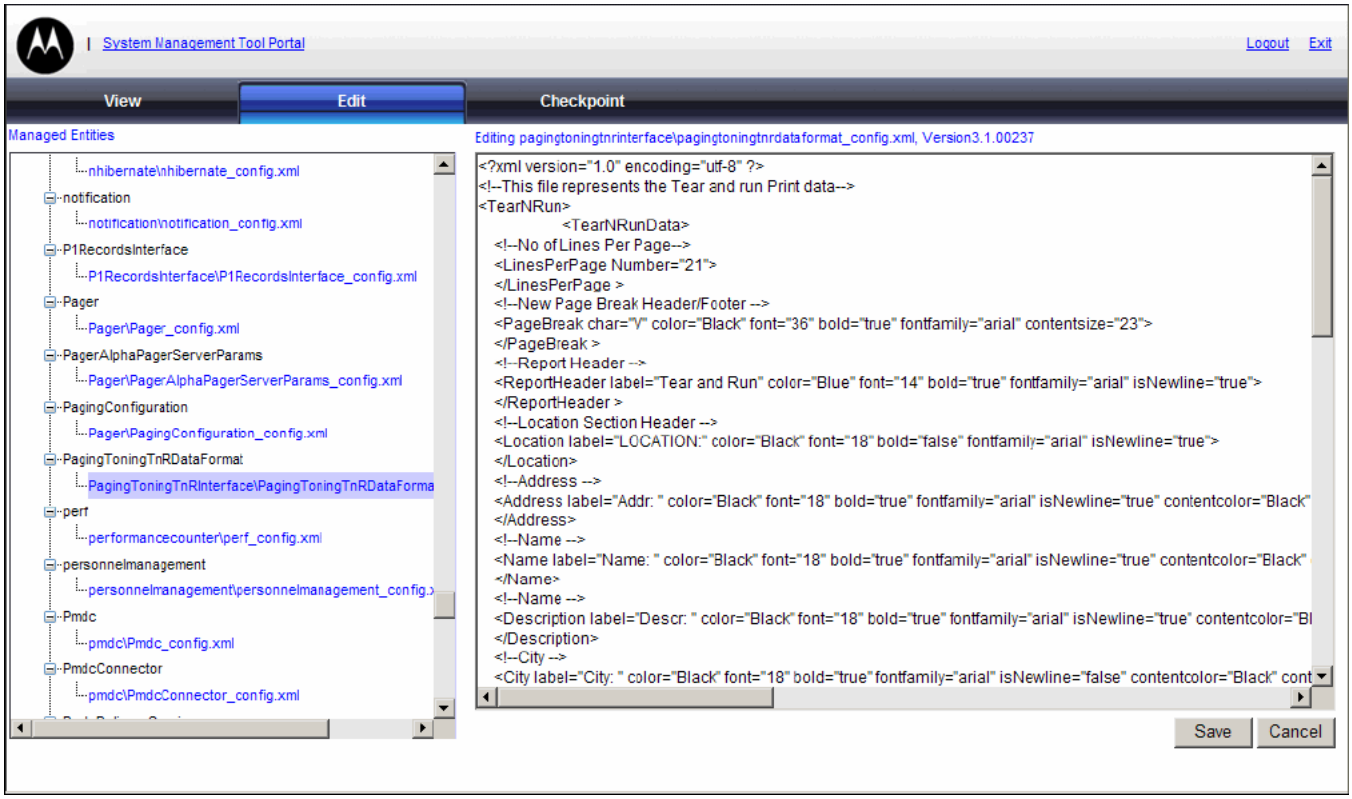


Figure 22-8 PagingToningTnRInterface\PagingToningTnRDataFormat_config.xml File

4. To customize Paging configuration:

   a. In the box on the left, scroll down until you find `PagingConfiguration`.

   b. Click the following option: **Pager\PagingConfiguration_config.xml**.

      The `pager\pagingconfiguration_config.xml` file opens in the box on the right.

5. To customize alpha pager server parameters:

   a. In the box on the left, scroll down until you find `PagerAlphaPagerServerParams`.

   b. Click the following option: **Pager\PagerAlphaPagerServerParams_config.xml**.

      The `pager\pagingconfiguration_config.xml` file opens in the box on the right.

6. To customize the IDs, heartbeats, timeouts, whether acknowledgment is required, maximum message length, and so on for pagers:

   a. In the box on the left, scroll down until you find `Pager`.

   b. Click the following option: **Pager\Pager_config.xml**.

      The `pager\pagingconfiguration_config.xml` file opens in the box on the right.

7. Using XML, change the appropriate lines to meet the needs of your agency.

8. Click **Save**.

9. Unless the XML file specifically states otherwise at the top of the file, you will need to restart your server for the changes to take effect.

Configuring the External System Interface

Use the External System configuration item to configure external interfaces.

Two commonly used external interfaces are CADfusion™ from FATPOT Technologies and LiveMUM™ from Deccan International.

CADfusion links different CAD systems together and gives agencies real time views of their neighboring agency's calls, regardless of the CAD system used. All connected agencies have immediate call coordination, instant messaging, and secure call transfer capabilities.

LiveMUM (Live Move-Up-Module) connects with CAD systems to identify holes in fire incident coverage or changes in a unit's status. LiveMUM then recommends the optimal move-ups for apparatus. LiveMUM is configured to account for both a communication center's specific policies and business rules and the live status of unit changes from CAD, combined with a move-up algorithm to guarantee balanced coverage needs.

The External System configuration item contains the following items:

- External System – Where you describe and configure the system that will be sharing data through the Cad-to-Cad interface
- Local Agency Settings – Where you enable external systems.
- Foreign Agency Settings – Where you enable agency setting for foreign CAD systems. This is used when the External System Interface is used as a CAD-to-CAD Call for Service Interface.

Configuring System Identification for External Interfaces

Use the System Identification form to name, describe, and configure the system that will be sharing data through the Cad-to-Cad interface.

To configure system identification for external interfaces:

1. From the navigation panel, select **Interface**, and then select **External System**.

   The System Identification tab of the External System window appears.

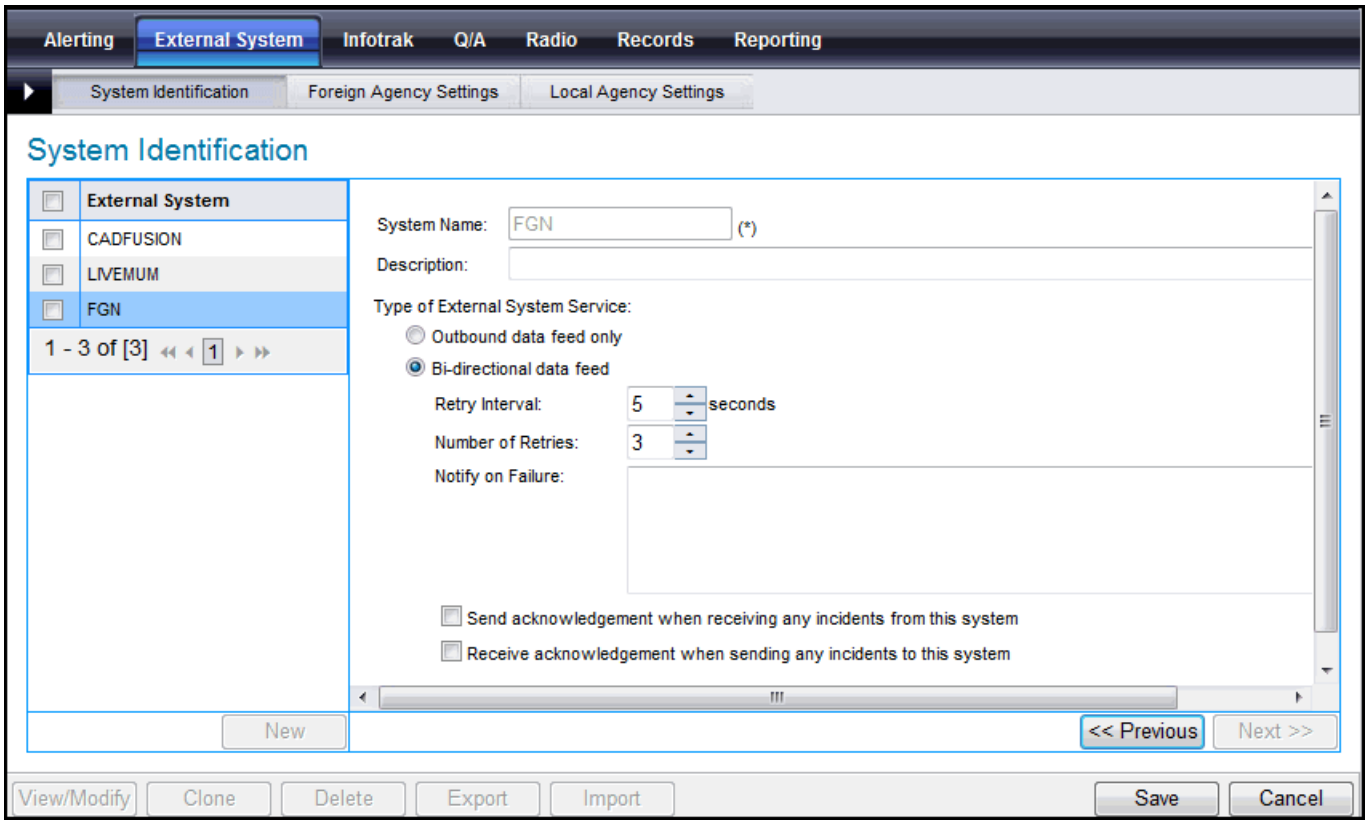


Figure 22-9 External System – System Identification Tab

2. In the System Name field, type the name of the system.

   The System Name is used as the System ID for NIEM (National Information Exchange Model) conformance.

3. In the Description field, type a description for the system.

   The description is used as the Organization Name for NIEM conformance.

4. In the Type of External System Service section, do the following:

   a. Select one of the following to identify the type of external system with which to communicate. The default is Outbound data feed only.

      - Outbound data feed only (used for CADfusion and LiveMUM)
      - Bi-directional data feed (used for CAD-to-CAD Call for Service)

   b. The following fields are enabled only if you selected Bi-directional data feed for the Type of External System Service:

      - In the Retry Interval field, use the up and down arrows to select the number of seconds for the retry interval.
      - In the Number of Retries field, use the up and down arrows to select the number of times to retry.
      - Select how you want to send and receive acknowledgements for incidents in the first two check boxes.
      - Select how you want to send and receive acknowledgements for unit status updates in the last two check boxes.

5. Click **Save**.

Configuring Local Agency Settings

Use the Local Agency Settings form to enable the external system.

To configure local agency settings:

1. Access the form for External Systems. For more information, see “Configuring System Identification for External Interfaces” on page 22-23.
2. Select the Local Agency Settings tab.
3. From the External System list on the left, select the system you want to enable.

If you selected Outbound data feed only for the Type of External System Service on the System Identification tab, a check box to enable the Outbound data feed appears.

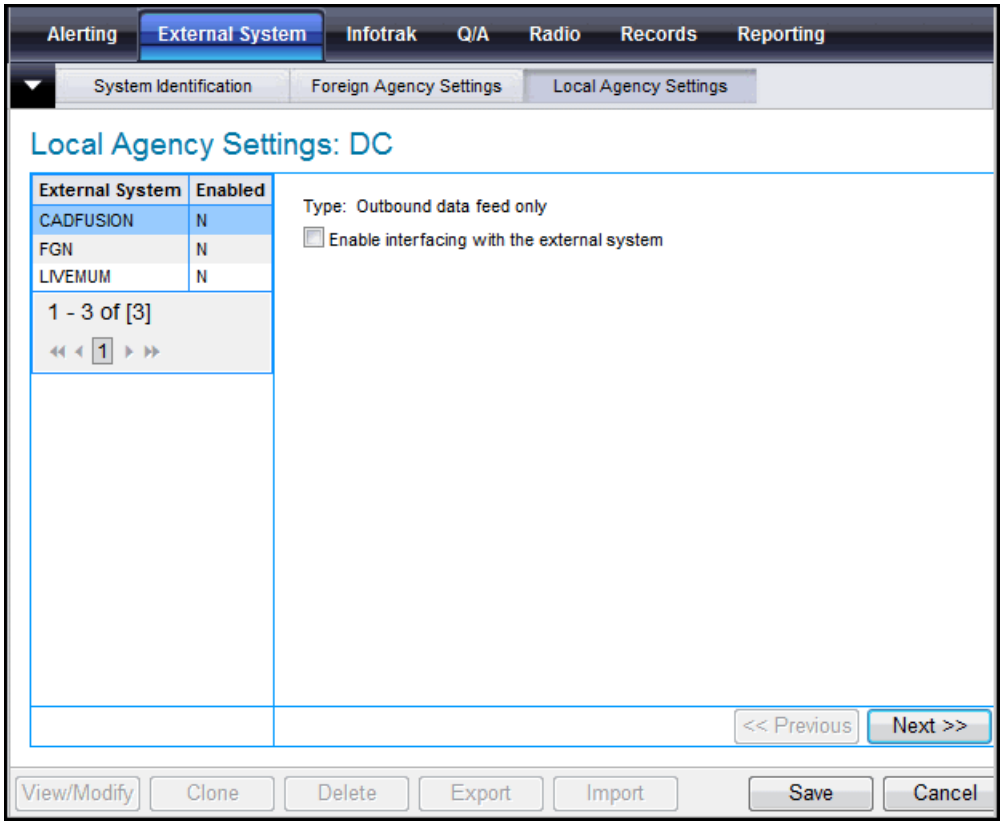


Figure 22-10 External System – Agency Settings Tab, Outbound Data Feed Only

4. Select the **Enable interfacing with External System** check box.

If you selected Bi-directional data feed for the Type of External System Service on the System Identification tab, fields for the Bi-directional data feed appear.

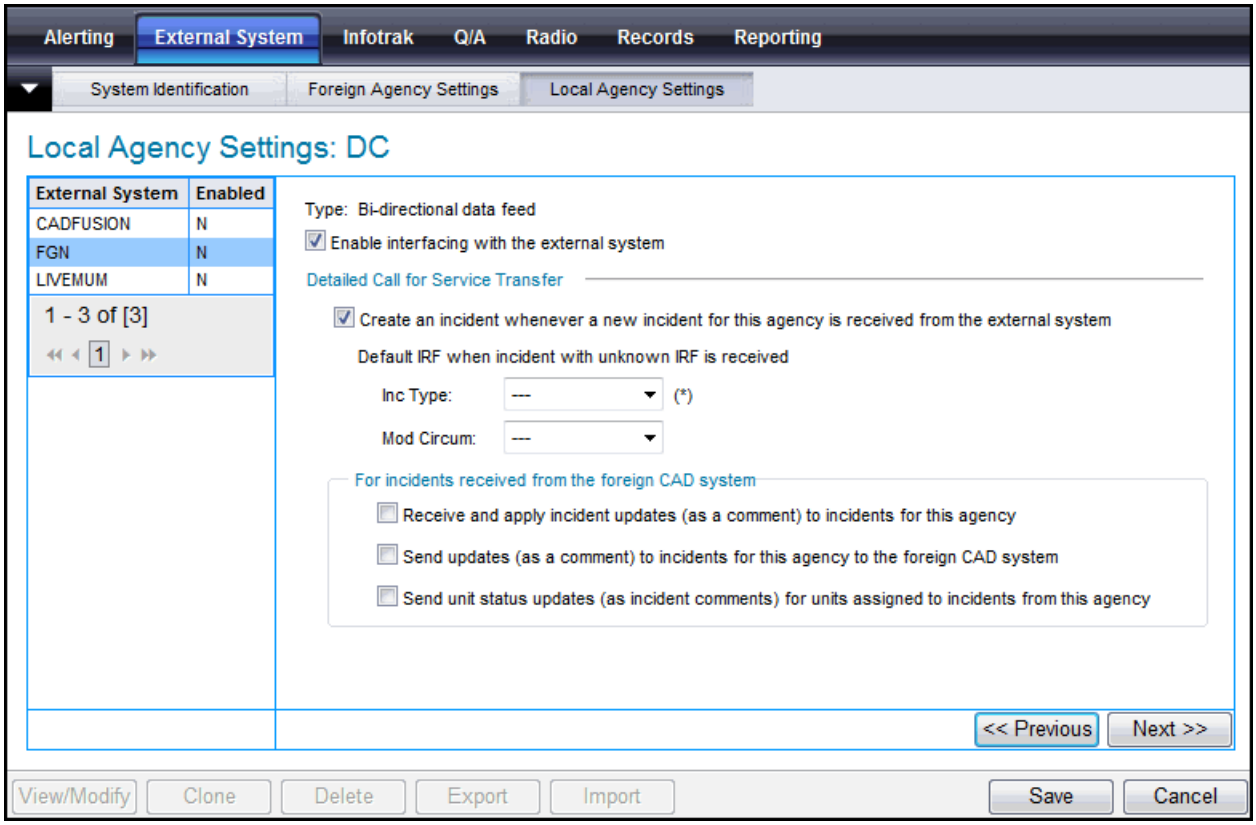


Figure 22-11 External System – Agency Settings Tab, Bi-Directional Data Feed

5. Select the **Enable interfacing with external system** check box.

6. If you want to Create an incident whenever a new incident for this agency is received from the external system, select that check box.

   a. From the Inc Type list, select the incident type for the new incident. You must select an incident type.

   b. From the Mod Circum list, select the modifying circumstance for the new incident. You can leave this field blank (---).

7. If you want to Send all unit status updates for this agency to the external system, select that check box.

8. Click **Save**.

Using the External System Interface as a Call for Service Interface

The External System Interface can also be used as a CAD-to-CAD Call for Service (CFS) interface.

The PremierOne CAD-to-CAD Call for Service (CFS) interface, allows for a bi-directional transfer of incident data between one or more CAD systems that are communicating with PremierOne via this interface. This includes the bi-directional transfer of incidents that are initiated and/or updated on either system.

Unit status code changes for units assigned to transferred incidents can be transferred from PremierOne to another CAD system as an incident comment.

Call for Service Features

The Call for Service interface includes the following features:

- Initial request for service
- Address update for the request for service
- Incident type update for the request for service
- Unit status code changes for units assigned to transferred incidents
- Updates to initial caller
- Additional comments and notes for the CAD incident

Call for Service Definitions

The following definitions may be of use:

- **Foreign Agency** – An agency being managed within a Foreign CAD system.
- **Local Agency** – An agency being managed within the PremierOne CAD system that is communicating with one or more Foreign CAD systems via the Call for Service interface.
- **Foreign CAD System** – The external CAD system that is connected to PremierOne via the Call for Service interface. These CAD systems can be comprised of CAD systems from various vendors, or comprised of other PremierOne systems.

- **Local CAD System** – The PremierOne CAD system that is communicating with external CAD systems via the Call for Service interface.

Provisioning the Call for Service Interface

In Provisioning, you do the following tasks:

- Provision your Foreign CAD systems
- Provision your Local Agencies
- Provision your Foreign Agencies
- Provision a default Incident Source Code to be used when creating an incident received from a Foreign CAD system
- Provision default incident statuses for Foreign Agencies

Overview of Provisioning the Local Agency

PremierOne can be provisioned to create new incidents that are received *from* a Foreign CAD system *for* a Local Agency, and then transferred to PremierOne.

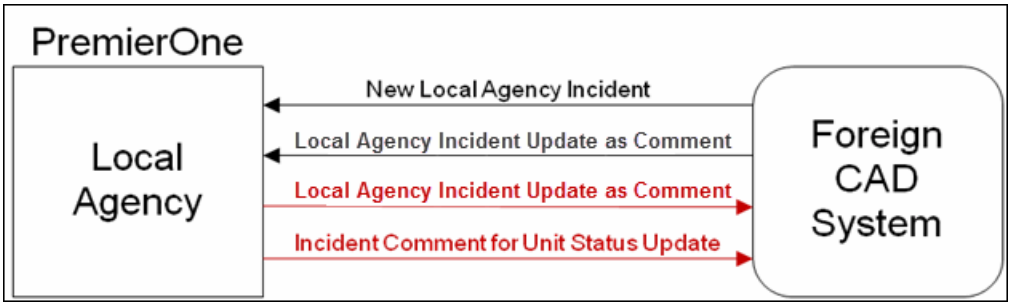


Figure 22-12 Local Call for Service Requests

For each of the incidents received from a Foreign CAD system and created on PremierOne for a Local Agency, the Local Agency can be *further* provisioned to support Call for Service Requests in the following ways:

- Receive incident updates as comments

  PremierOne does not update incident data directly when updates are received from a Foreign CAD system. Rather, all incident updates received from the Foreign CAD system are applied as comments.

- Send incident updates as comments

- Send unit status updates as comments against the incident to which the unit is assigned

  Unit status code changes are not transferred to the Foreign CAD system as actual unit status update transactions. Instead, unit status code changes are sent to a Foreign CAD system as comments against the incident currently assigned to the respective unit.

Overview of Provisioning the Foreign Agency

PremierOne can also be provisioned to transfer new Foreign Agency incidents created on the Local CAD system to a Foreign CAD system.

Figure 22-13 Foreign Call for Service Requests

For each Foreign Agency incident that is transferred to a Foreign CAD system, the Foreign Agency can be *further* provisioned to support Call for Service Requests in the following ways:

- Send incident updates as comments
- Receive incident updates as comments

  PremierOne does not update any incident data directly when updates are received from a Foreign CAD system. Rather, all incident updates received from the Foreign CAD system are applied as comments.

- Receive updates to the unit's status as comments against the incident to which the units is assigned

All updates received from the Foreign CAD system and applied to the Foreign Agency incident can also be applied to all associated incidents.

Provisioning Foreign CAD Systems

Provision the Foreign CAD systems that will be sending and receiving incident data through Call for Service Requests. Also provision notification recipients for unacknowledged Call for Service Requests sent to Foreign CAD systems.

To provision Foreign CAD systems:

1. From the Navigation pane, select **Interface**, and then select **External System**.
2. Select **System Identification**.

   The System Identification form appears.

   A list of existing External Systems, if any, displays on the left side of the screen.
3. Click **New** at the bottom of the External System list.

   The fields in the System Identification form become editable.

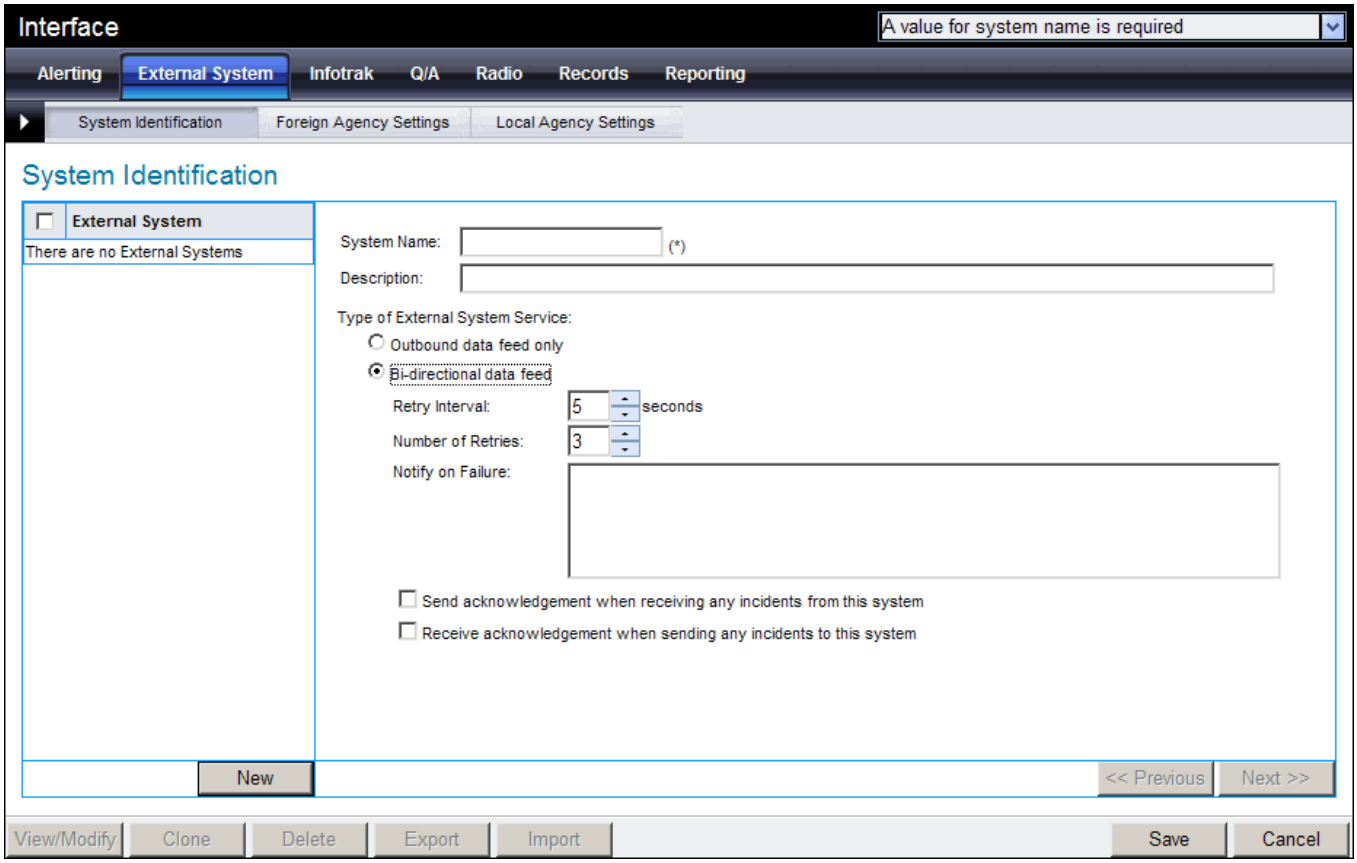


Figure 22-14 External System – System Identification Form

4. In the System Name field, type the name of the Foreign CAD system.

   This field is used to identify which system each Foreign Agency is associated with and which Foreign CAD systems receive data from a Local Agency.
5. In the Description field, type a description for the Foreign CAD system.

6. In the Type of External System Service section, do the following:

   a. Select the **Bi-directional data feed** option.

      The fields below become editable.

   b. In the Retry Interval field, select the number of seconds to wait before resending a Call for Service for a transaction that was not acknowledged by the Foreign CAD system.

      This number cannot be less than 5 seconds.

   c. In the Number of Retries field, select the number of times to resend incident or unit data for a transaction that was not acknowledged by the Foreign CAD system.

   d. In the Notify on Failure text box, type the email addresses for one or more recipients that will receive an email message when a request sent to the Foreign CAD system exceeds its number of retries. Separate multiple email addresses with commas.

      The email addresses can be any valid email address that is supported by PremierOne's messaging service.

   e. Select the **Send Acknowledgement when receiving any incidents from the system** check box to send an acknowledgement for each transaction received from the Foreign CAD system.

   f. Select the **Receive acknowledgement when sending any incidents to this system** check box to receive an acknowledgement for each incident transaction sent to the Foreign CAD system.

7. Click **Save**.

Provisioning Local Agencies

Provision Local Agencies that will be *sending* Call for Service Requests and updates *to* a Foreign CAD system. Also provision Local Agencies to *receive* requests *from* a Foreign CAD system.

To provision Local Agencies:

1. From the Navigation pane, select **Interface**, and then select **External System**.

2. Select the Local Agency Settings tab.

The Local Agency Settings form appears.

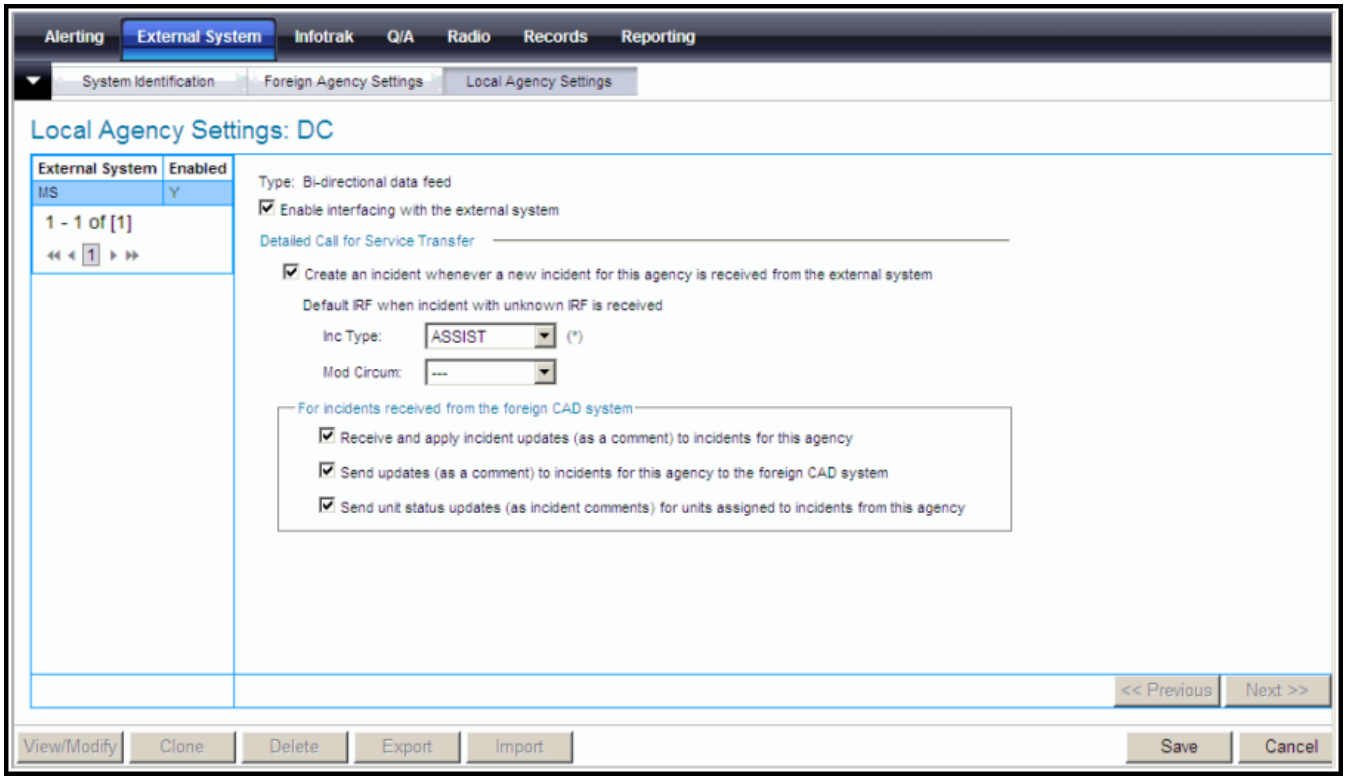


Figure 22-15 External System – Local Agency Settings Form

3. Select a Foreign CAD system from the list on the left.

   The Type field displays which type of external system service was selected on the System Identification form.

4. Click **View/Modify**.

5. Select the **Enable interfacing with the external system** check box to enable the Local Agency to communicate with the specified Foreign CAD system.

6. Select the **Create an incident whenever a new incident for this agency is received from the external system** check box to enable incident creation when incidents are received from the specified Foreign CAD system.

   The additional fields become editable.

7. In the Default IRF when incident with unknown IRF is received section, do the following:

    a. From the Incident Type list, select the default incident type to use when an incident is received from the Foreign CAD system with an Incident Response Factor (IRF) that is not provisioned for the corresponding Agency/Agency Type.

    b. From the Mod Circum list, select the default modifying circumstance to use when an incident is received from the Foreign CAD system with an IRF that is not provisioned for the corresponding Agency/Agency Type.

8. In the For incidents received from the Foreign CAD system section, do the following:

    a. Select the **Receive and apply incident updates (as a comment) to incident for this agency** check box to indicate that you want to receive incident updates from the Foreign CAD system.

    b. Select the **Send updates (as a comment) to incidents for this agency to the Foreign CAD system** check box to indicate that incident updates to the Local Agency should be sent to the Foreign CAD system.

    c. Select the **Send unit status updates (as incident comments) for units assigned to incidents from this agency** check box to indicate that unit status updates for units assigned to the Local Agency incident should be sent to the Foreign CAD system.

9. Click **Save**.

Provisioning Foreign Agencies

Each Foreign Agency must be provisioned on the Local CAD system in order for incident data to be transferred via the Call for Service interface.

Configuring the Specific Foreign Agency

You must add the agency to the system and configure the agency as a Foreign Agency.

To configure the specific Foreign Agency:

1. From the Navigation pane, select **Agency**, and then select **Agency**.

The Agency form appears.

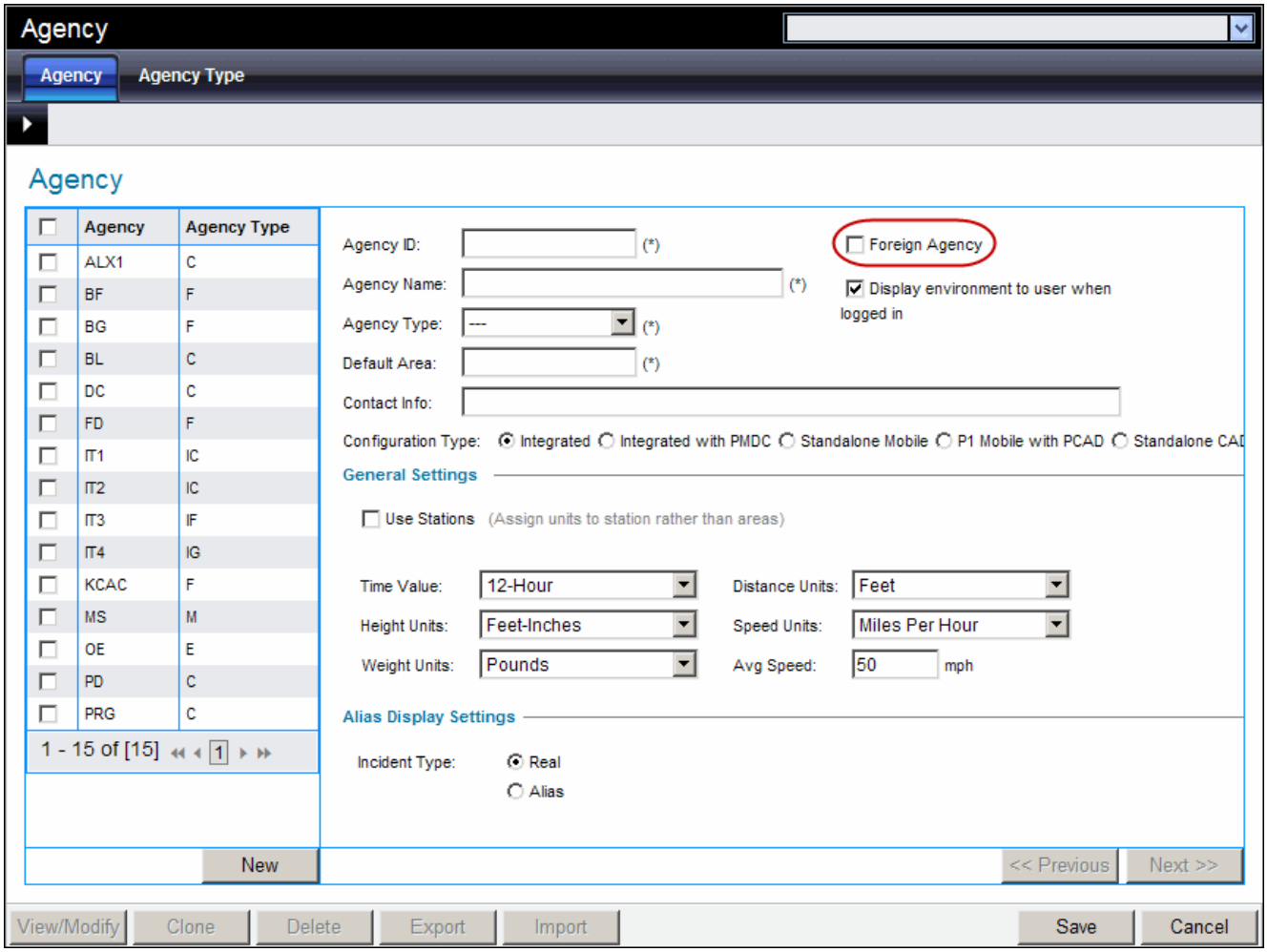


Figure 22-16 Agency – Agency Form

2. Enter the agency information, including the following required fields:
   a. Agency ID
   b. Agency Name
   c. Agency Type
   d. Default Area
3. Select the **Foreign Agency** check box.
4. Click **Save**.

Configuring Foreign Agency Information

Provision Foreign Agencies to be used to *send* a Call For Service Request *to* a Foreign CAD system, and to *receive* a Call For Service Request *from* a Foreign CAD system.

To configure Foreign Agency information:

1. From the Navigation pane, select **Interface**, and then select **External System**.
2. Select the Foreign Agency Settings tab.

   The filter area opens.
3. From the Agency list in the filter area, select the Foreign Agency you want to configure. If the Foreign Agency is not listed, you must set it up. See "Configuring the Specific Foreign Agency" on page 22-33.

   The Foreign Agency Settings form appears.

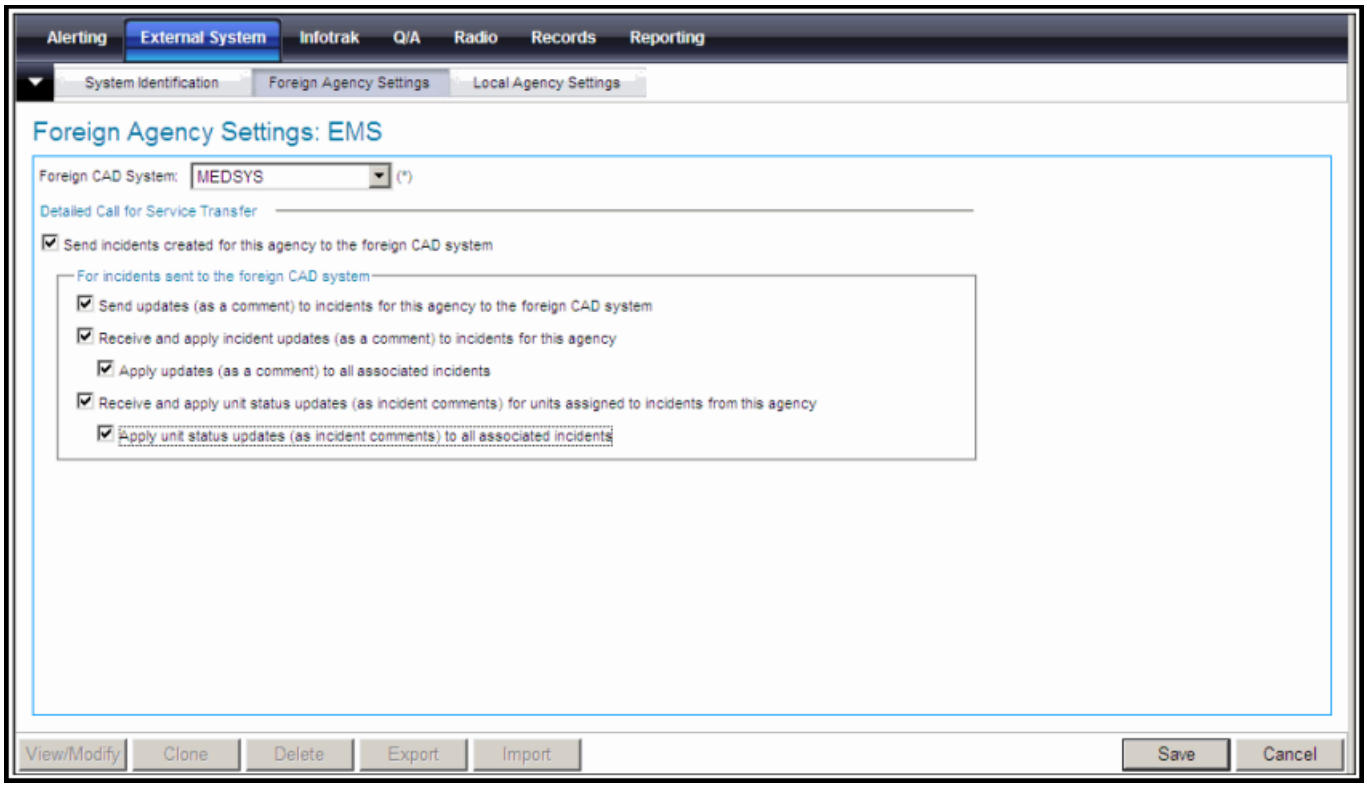


Figure 22-17 External System – Foreign Agency Settings Form

4. Click **View/Modify**.
5. From the Foreign CAD system list, select the Foreign CAD system for which you are setting agency information.

6. *Optional*: Select the **Send incidents created for this agency to the Foreign CAD system** check box.

   The remaining fields become editable.

7. *Optional*: Select the **Send updates (as a comment) to incidents for this agency to the Foreign CAD system** check box to cause updates *performed on the Local CAD system* to incidents created on the Local CAD system for this agency to be *sent to* the Foreign CAD system.

8. *Optional*: Select the **Receive and apply incident updates (as a comment) to incidents for this agency** check box to cause incident updates *performed on the Foreign CAD system* to incidents created on the Local CAD system for this agency to be *received from* the Foreign CAD system and applied to the incident.

   Select **Apply updates (as a comment) to all associated incidents** to cause the incident updates received from the Foreign CAD system to be applied to all incidents associated with the updated incident.

9. *Optional*: Select the **Receive and apply unit status updates (as incident comments) for units assigned to incidents from this agency** check box to receive updates to the unit's status as comments against the incident to which the unit is assigned.

   Select **Apply updates (as a comment) to all associated incidents** to cause the incident updates received from the Foreign CAD system to be applied to all incidents associated with the updated incident.

10. Click **Save**.

11. *Optional*: Repeat these steps to configure additional Foreign Agencies. You must set up the addition Foreign Agencies in "Provisioning Foreign CAD Systems" on page 22-29 first.

Provisioning the Default Incident Source Code

Provision a default incident source code to be used when creating an incident received from a Foreign CAD system.

To provision the default incident source code:

1. From the Navigation pane, select **Incident Management**, and then select **Incident Source Code**.

   The Incident Source Code form appears with the Code list tab in focus.

2. Select the Set Defaults tab.

3. Click **Save**.

Provisioning Default Incident Status

Provision the default incident status for the Foreign Agency to use when creating an incident from a Foreign CAD system.

To provision the default incident status:

1. From the Navigation pane, select **Incident Management**, and then select **Service Settings**.

   The Service Settings form appears.

   NOTE
   For the Initial Status field, the choices are **Open** or **Closed**. Pending is not an option because the local agency will not be managing the incident.

   - If you create the Foreign Agency incident as a Closed incident on the Local CAD system, no further action is required for this incident. When you create the Closed incident, you can use the provisioned disposition for the incident.
   - If you create the Foreign Agency incident as an Open incident, users on the Local CAD system are required to manually close the incident.

2. Click **Save**.

Configuring Infotrak

Use the Infotrak configuration item to configure the default incident date for Infotrak.

To configure Infotrak for PremierOne:

1. From the navigation panel, select **Interface**, and then select **Infotrak**.

   The Infotrak filter area appears.

2. Select the appropriate agency.

3. Click **OK**.

The Infotrak form appears.

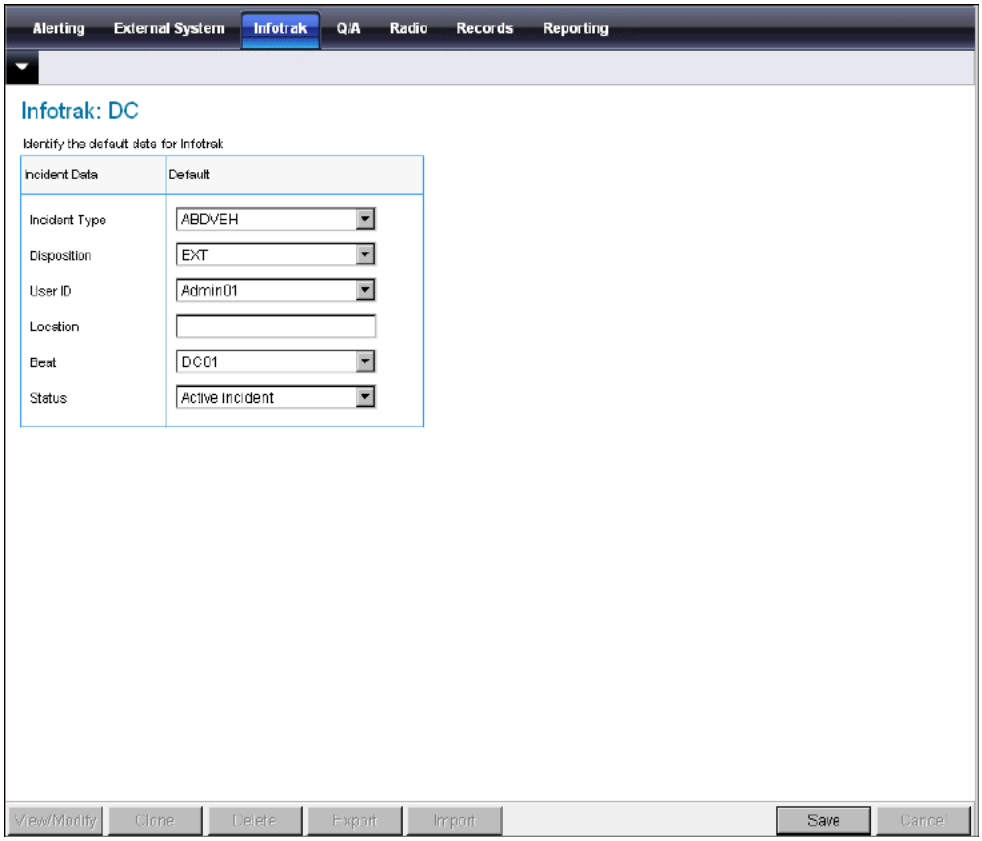


Figure 22-18 Infotrak Form

4. Select the default incident data for Infotrak.
5. Click **Save**.

Configuring the QA Interface

ProQA™, a third-party software application by Priority Dispatch Corporation, is used to gather information during the initiation of medical and fire incidents. ProQA is used by emergency dispatchers who have been trained and certified in the use of the Medical Priority Dispatch System (MPDS). ProQA can be used for medical and fire incidents on the same system.

ProQA Paramount™ is an updated version of ProQA that includes police in addition to fire and medical.

NOTE

You can configure either the ProQA interface or the ProQA Paramount interface, but not both.

ProQA and ProQA Paramount information consists of general settings that effect ProQA to CAD client interactions, configuring fields to import to CAD, and setting the location of the `comm.dat` file, which passes the information between the CAD client and ProQA.

The QA interface is configured on two subtabs, ProQA and ProQA Paramount, in the Interface—QA configuration item:

- ProQA – Where you configure ProQA for fire and medical.
- ProQA Paramount – Where you configure ProQA Paramount for fire, medical, and police.

Configuring ProQA

Use the ProQA subtab to configure ProQA for fire and medical.

To configure ProQA information:

1. From the navigation panel, select **Interface**, and then select **Q/A**.

The ProQA tab of the Interface form appears. The Clone, Delete, Export, and Import buttons are disabled.

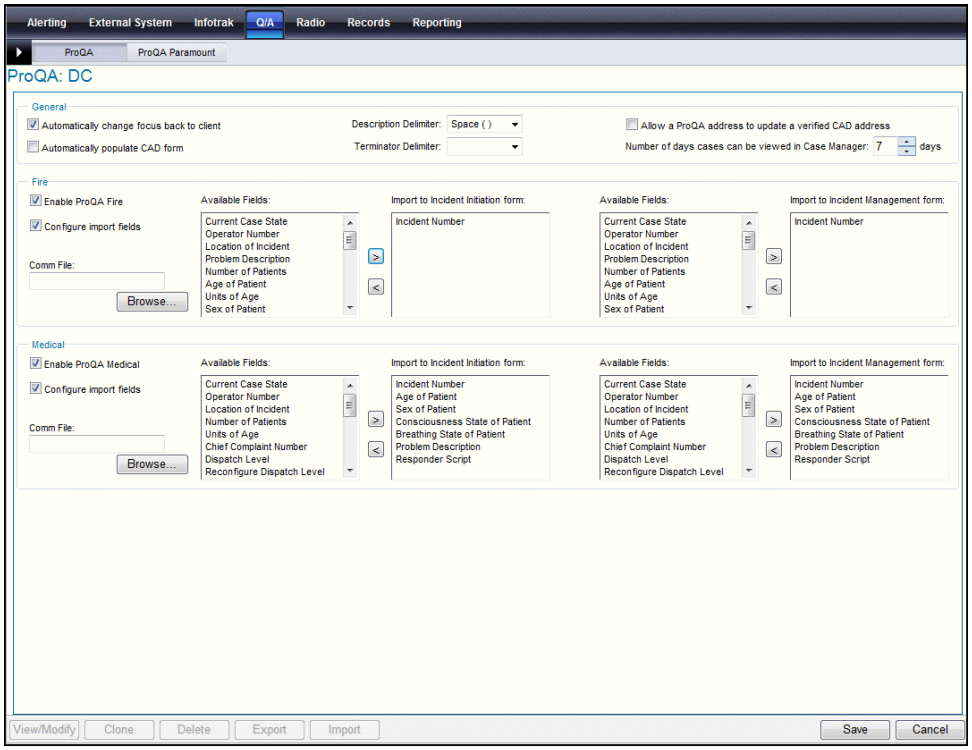


Figure 22-19 ProQA Form

2. At the bottom of the form, click the **View/Modify** button.
3. In the General section, do any of the following:

   - To automatically change focus back to the CAD client after the CAD user enters and submits case information, select the **Automatically change focus back to client** check box.

     If you do not select this option, the CAD user must manually place the focus from ProQA to CAD.

   - To automatically populate the CAD Initiate Incident form with the ProQA case data, select the **Automatically populate CAD form** check box.

     If you do not select this option, the CAD user must populate the Initiate Incident form with ProQA data using shortcut keys (Ctrl+Alt+P) or the menu option.

   - From the Description Delimiter list, select the character to separate the fields that are imported from ProQA into CAD (a space is used by default).

   - From the Terminator Delimiter list, select the character to indicate the end of the list of imported values.

- To allow addresses entered in ProQA to update those in CAD, select the **Allow a ProQA address to update a verified CAD address** check box.
- In the Number of days cases can be viewed in Case Manager field, enter or select the number of days you want cases maintained for viewing in the ProQA Case Manager.

4. In the Fire and Medical sections, do any of the following:
   - To enable the use of ProQA, select the **Enable Pro QA Medical** or **Enable Pro QA Fire** check box.
   - To select additional fields to import from ProQA to CAD, select the **Configure Import fields** check box.

     By default seven fields are included (Incident Number, Age of Patient, Sex of Patient, Breathing State of Patient, Problem Description, Current Case State, and Responder Script). You only need to select this check box if you want to select additional fields for import.

     After selecting the check box, select the fields that you want to add from the Available Fields box and use the right arrow to add them to the Import to Incident Initiation form box. Then select the fields that you want to add from the second Available Fields box and use the right arrow to add them to the Import to Incident Management form box.
   - Click the **Browse** button to the right of the Comm File field, and navigate to and select the `comm.dat` file to use with ProQA.

     This file passes the information between the CAD client and ProQA. The file is created as part of the ProQA installation.
5. Click **Save**.

   The configuration information is saved.

Configuring ProQA Paramount

Use the ProQA Paramount subtab to configure ProQA Paramount for fire, medical, and police.

To configure ProQA Paramount information:

1. From the navigation panel, select **Interface**, and then select **Q/A**.

   The QA Interface form appears, with the ProQA tab in focus (see Figure 22-19 on page 22-40).
2. Select the **ProQA Paramount** subtab.

The ProQA Paramount form appears.

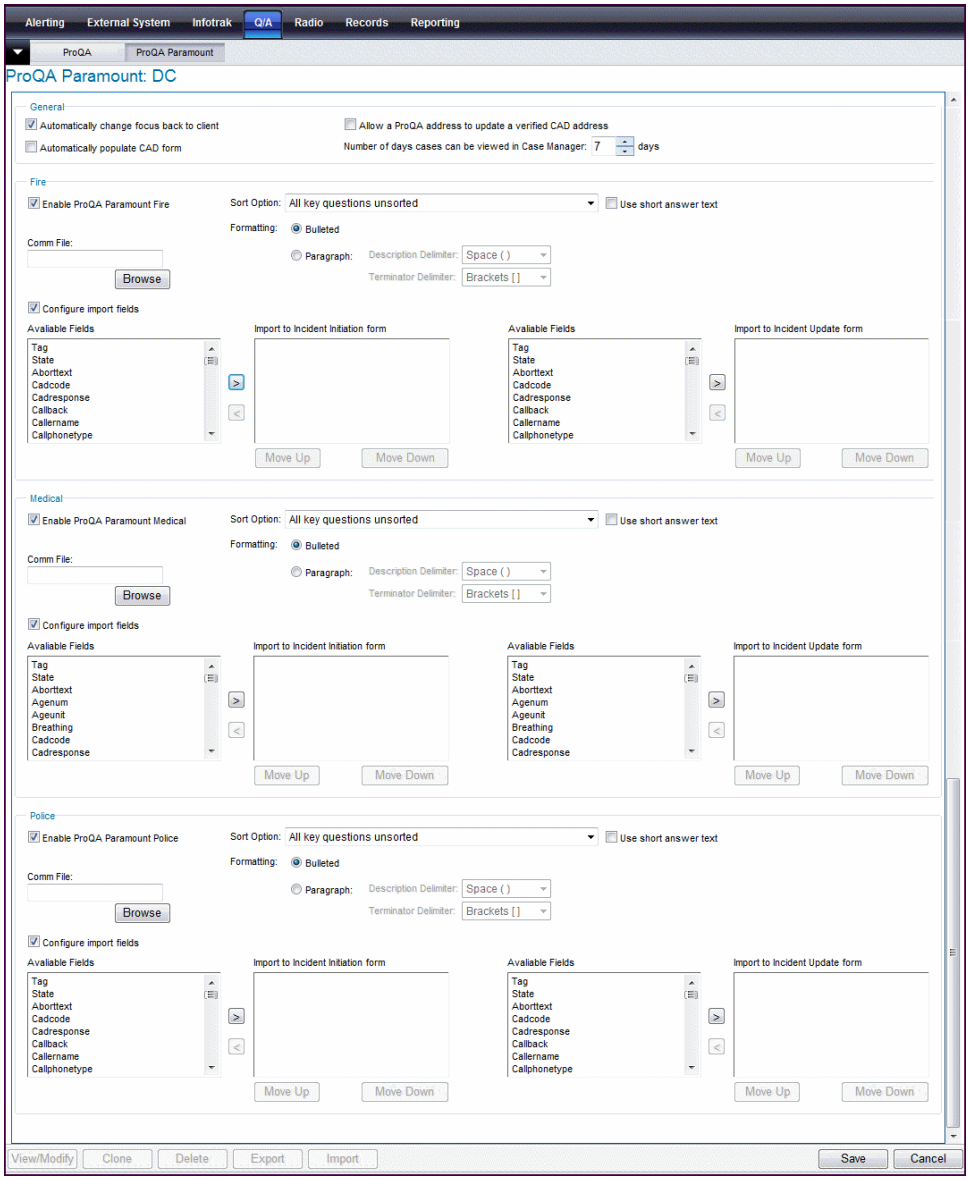


Figure 22-20 ProQA Paramount Form

3. At the bottom of the form, click the **View/Modify** button.

4. In the General section, do any of the following:

   - To automatically change focus back to the CAD client after the CAD user enters and submits case information, select the **Automatically change focus back to client** check box.

     If you do not select this option, the CAD user must manually place the focus from ProQA Paramount to CAD.

   - To automatically populate the CAD Initiate Incident form with the ProQA case data, select the **Automatically populate CAD form** check box.

If you do not select this option, the CAD user must populate the Initiate Incident form with ProQA Paramount data using shortcut keys (Ctrl+Alt+P) or the menu option.

- To allow addresses entered in ProQA Paramount to update those in CAD, select the **Allow a ProQA address to update a verified CAD address** check box.
- In the Number of days cases can be viewed in Case Manager field, enter or select the number of days you want cases maintained for viewing in the ProQA Case Manager.

5. In the Fire, Medical, and Police sections, do any of the following:

   - To enable the use of ProQA Paramount, select the appropriate check boxes: **Enable Pro QA Paramount Fire, Enable Pro QA Paramount Medical**, or **Enable Pro QA Paramount Police**.
   - From the Description Delimiter list, select the character to separate the fields that are imported from ProQA Paramount into CAD (a space is used by default).
   - From the Terminator Delimiter list, select the character to indicate the end of the list of imported values.
   - From the Sort Option list, select one of the following:
     - **All key questions unsorted**
     - **All key questions with safety questions floated**
     - **Pertinent answers with safety questions floated**
     - **Pertinent & important answers with safety questions floated**

     To display short text answers with any selected sort option, select the **Use short answer text** check box.

- In the Formatting field, select the format in which to display ProQA Paramount information: **Paragraph** or **Bulleted**.

- To select additional fields to import from ProQA Paramount to CAD, select the **Configure Import fields** check box.

  After selecting the check box, select the fields that you want to add from the Available Fields box and use the right arrow to add them to the Import to Incident Initiation form box. Then select the fields that you want to add from the second Available Fields box and use the right arrow to add them to the Import to Incident Management form box.

  NOTE
  For fields that require a predefined code, Paramount and CAD will need to be provisioned with the same codes.

- To the right of the Comm File field, click the **Browse** button and navigate to and select the `comm.dat` file to use with ProQA Paramount.

  This file passes the information between the CAD client and ProQA Paramount. The file is created as part of the ProQA Paramount installation.

6. Click **Save**.

   The configuration information is saved.

ProQA Paramount Keyboard Shortcuts and Function Keys

The following shortcuts and function keys are available to CAD users when ProQA Paramount is enabled.

Table 22-1 ProQA Paramount Keyboard Shortcuts and Function Keys

Function	Shortcut	Note
Fire ProQA Paramount application	**CTRL+ALT+F**	If Fire ProQA Paramount is provisioned, the shortcut is functional when an II or IU form is displayed in the active work area
Medical ProQA Paramount application	**CTRL+ALT+M**	If Medical ProQA Paramount is provisioned, the shortcut is functional when an II or IU form is displayed in the active work area
Police ProQA Paramount application	**CTRL+ALT+L**	If Police ProQA Paramount is provisioned, the shortcut is functional when an II or IU form is displayed in the active work area
Case Manager ProQA Paramount application	**CTRL+ALT+C**	If Fire or Medical or Police ProQA Paramount is provisioned, the shortcut is functional when an II or IU form is displayed in the active work area
Import ProQA Paramount data to CAD	**CTRL+ALT+P**	

Configuring the Radios Interface

CAD can be interfaced to a radio system that manages the communications among the agency radios. Radio configuration is system-wide and works across agencies.

The Radios window contains the following tabs:

- System Configuration – Contains radio system information.
- Radio System Settings – Contains system settings for channel groups and two-tone radio alerting.
- Talkgroups Configuration – Contains settings for talkgroups, radio frequency that is used by radio operators to communicate on a trunk radio system.
- Channel Groups Configuration – Contains settings for Channel Groups, groups of radio channels or talkgroups that a radio console operator can use to transmit an APB or other notifications. Channel Groups only function with radio systems that allow the CAD client to co-exist on the same workstations as the radio control application provided by Motorola.

In addition to the Provisioning available on the tabs, you can provision the button position, disposition code, unit status, and location from the Configuration module of the System Management Tool Portal. For more information, see the *PremierOne System Administrator Guide*.

Configuring System Configuration Settings

Radio system information consists of the system ID, radio name, whether the radio system is currently available, beeps, duration, and delays for priority transmissions, and beeps and duration for channel requests.

To configure a radio system:

1. From the navigation panel, select **Interfaces**, and then select **Radio**.

The System Configuration tab of the Radio form appears.

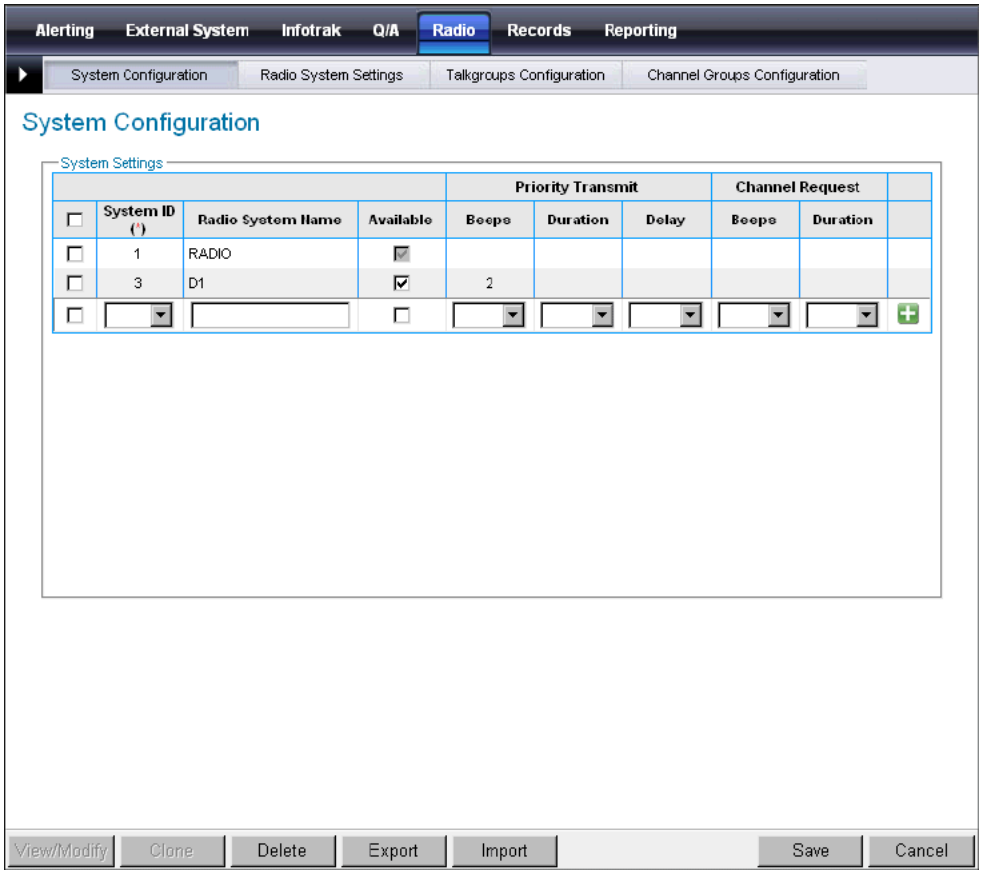


Figure 22-21 Radios Form – System Configuration Tab

2. At the bottom of the form, click the **View/Modify** button.
3. From the System ID list, select the radio system ID.

   This ID is used to uniquely identify the radio system. You can use up to ten radio systems. Only one of the systems can be active at any time.
4. In the Radio System Name field, enter a descriptive name for the radio system.
5. If the radio system is available, select the **Available** button.
6. Do the following for the Priority Transmit request:

   - From the Beeps list, select the number of beeps to sound for a priority transmit request.

     The beeps signify a preempt audio sound in the radio operator's headset when the operator is transmitting on a channel.
   - From the Duration list, select the duration of the beep. Increments are 10 milliseconds.

Values define the number of 10 msec intervals each beep will last. For example, a value of 2 is a 20 msec duration for each beep; 20 msec will also pass between each beep.

- From the Delay list, select the number of seconds to lapse after the broadcast preempt message is issued and the APB transmit is issued.

7. Do the following for the Channel Request:

   - From the Beeps list, select the number of beeps to sound for a channel request.
   - From the Duration list, select the duration of the beep.

     Values define the number of 10 msec intervals each beep will last. For example, a value of 2 is a 20 msec duration for each beep; 20 msec will also pass between each beep.

NOTE
Motorola recommends that the Beeps and Duration values are significantly different between the Priority Transmit and Channel Request to allow the radio operator to distinguish between the two functions.

8. Click the plus symbol to the right of the Duration field to save the radio system settings and add another row.

CAUTION
If you do not click the plus symbol, PremierOne does not save the agency information, even after you click Save.

9. Repeat the procedure to add any additional radio systems.
10. Click **Save**.

Configuring Radio System Settings

Radio system settings include the following:

- General – Where you configure system settings for channel groups.
- Two-tone alerting – Where you configure settings for two-tone alerting.

Configuring General Radio Settings

Use the General Settings section of the Radio Systems Settings form to configure system settings for channel groups.

NOTE
Channel Groups are only supported by the MC7500.

Channel groups are groups of radio channels or talkgroups, often called Multi Select or Msel groups, that a radio console operator can use to transmit an APB or other notifications. Channel groups only function with radio systems that allow the CAD client to co-exist on the same workstations as the radio control application provided by Motorola.

System settings for channel groups include whether channel group dispatch is enabled, whether the system is available and the radio control, function code, and level. For details on adding channels to the Channel Groups, see “Configuring Channel Groups” on page 22-54.

To configure general settings:

1. Access the form for Radios. For instructions, see “Configuring System Configuration Settings” on page 22-45.

   The System Configuration tab of the Radio form appears.

2. Click the Radio System Settings tab.

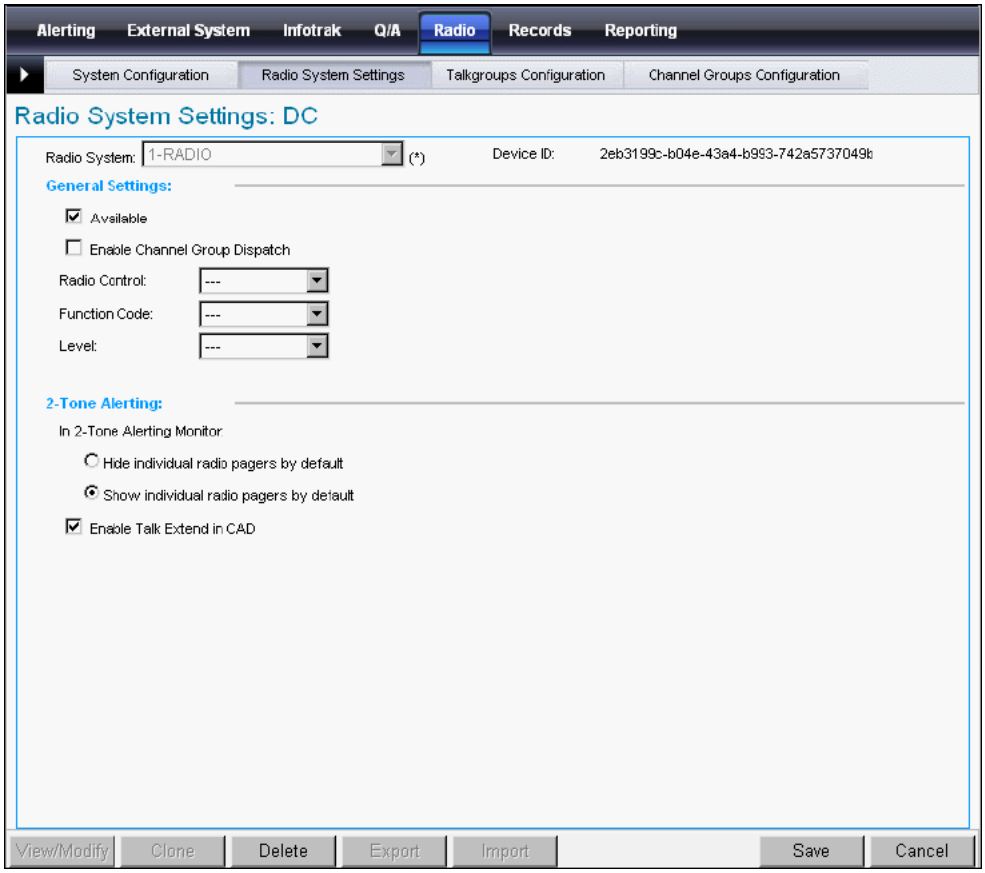


Figure 22-22 Radios Form – Radio System Settings Tab

3. At the bottom of the form, click the **View/Modify** button.

4. From the Select System to Configure Radios list, select the radio system for which you want to enable channel groups.

5. If the Channel Groups feature is ready and available, select the **Available** check box.

6. To use the Channel Groups feature with incident dispatch, select the **Enable Channel Groups Dispatch** check box.

7. From the Radio Control list, select a value to indicate which radio control system is being used.

   - If a radio control system is not being used, select **0**.
   - If the CentraCom Gold Elite radio control system is being used, select **1.**
   - If the MCC7500 is being used, select **2**.

8. From the Function Code list, select one of the following actions for the channels in the channel group in the Radio system display.
   - P – Populate the channels to the Channels in Groups list. Use this selection when you might want to add additional channels manually.
   - L – Populate the channels to the Channels in Groups list and then load the channels.
   - O – Populate the channels to the Channels in Groups list, load the channels, and then open the channels. This transmits audio to the headset on the receiving end.
9. From the Level list, select the name for the Channel Group to use.
   - B – Use the name of the beat containing the incident.
   - S – Use the name of the sector responsible for the incident.
   - A – Use the name of the area containing the incident.
10. Click **Save** or continue to configure two-tone alerting.

Configuring Two-Tone Alerting

Use the Two-Tone Alerting section of the Radio System Settings form to configure two-tone alerting. Two-tone radio alerting (sometimes referred to as two-tone paging) is a method of sending tones out to a group of pagers. These tones alert the person carrying the pager.

NOTE
This feature only available with the CENTRACOM Gold Elite Console. For setup and usage, contact Motorola for assistance.

Optionally, the tones can be followed by a voice message from a dispatcher. This option is called Talk Extend. When Talk Extend is used, the tones are followed by an open microphone and voice is transmitted from the dispatcher's radio console to all the pagers/radios in the group. Then, all the queued two-tone alerts are sent in parallel (at the same time) so the transmission channel is open for all of them at the same time.When Talk Extend is disabled, the two-tone radio alerts are sent sequentially (one after another). Therefore, when Talk Extend is disabled, one group will start and finish before the next group starts. This continues until the pager queue is empty.

Two-tone radio alerts can be sent just like any other toning event. They are supported from the II, ID, UX, and TN commands.

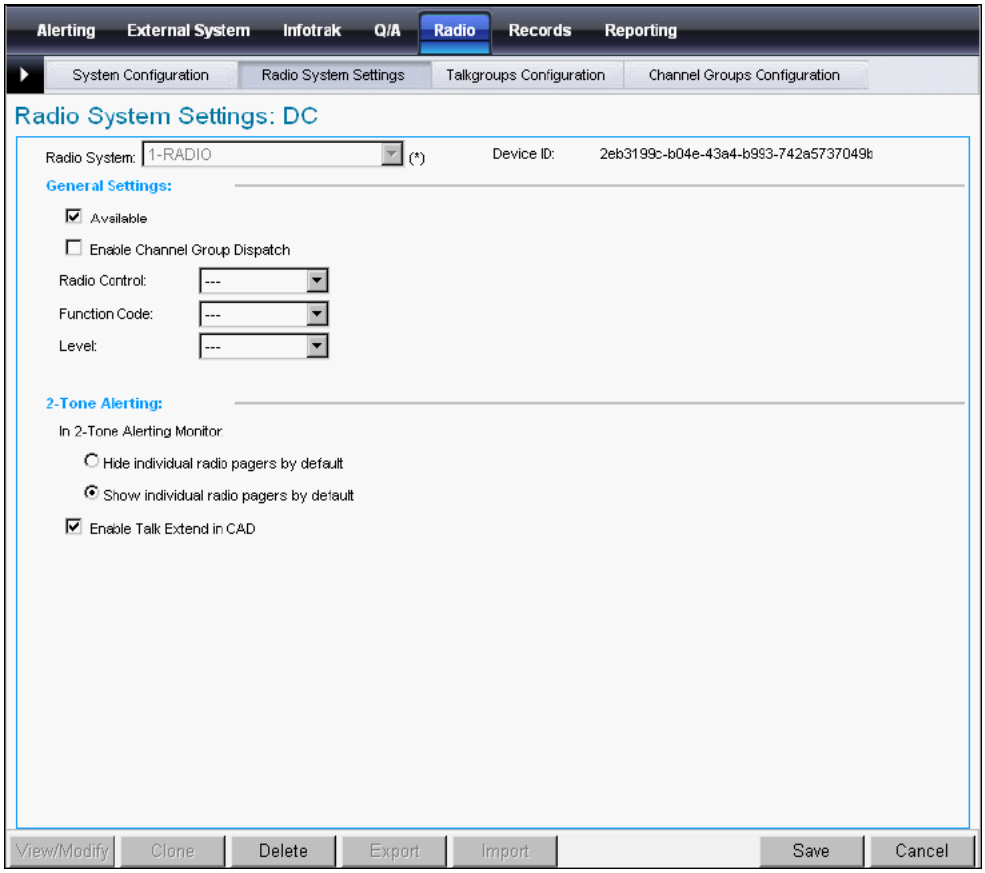


Figure 22-23 Radios Form – Radio System Settings Tab

To configure two-tone alerting:

1. Select how to show pager groups on the radio console:

   a. To show pager groups collapsed on the radio console, select Hide individual radio pagers by default.

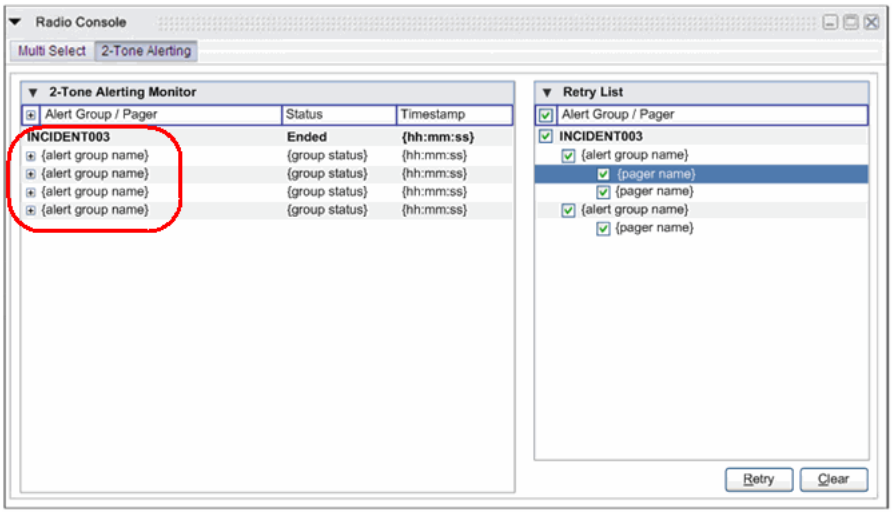


Figure 22-24 Radio Console Showing Pager Groups Collapsed

When the pager groups are collapsed (whether this was done manually or automatically), the Status and Timestamp columns display the group's status and timestamp.

   b. To show pager groups expanded on the radio console, select Show individual radio pagers by default.

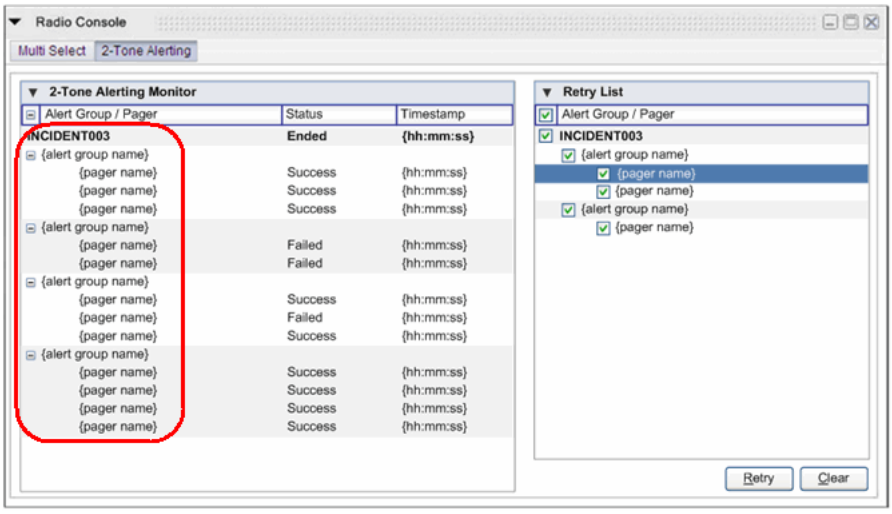


Figure 22-25 Radio Console Showing Pager Groups Expanded

When the pager groups are expanded (whether this was done manually or automatically), the *group's* Status and Timestamp columns are blank but the *individual* pager information (Pager name, status, timestamp) is displayed.

2. If you want to use Talk Extend, select the Enable Talk Extend in CAD check box.

   Talk Extend allows the tone to be followed by a voice message from a dispatcher. Your system must support this feature.

3. Click **Save**.

Configuring Talkgroups

A talkgroup is a radio frequency that is used by radio operators to communicate on a trunk radio system.

To configure a talkgroup:

1. Access the form for Radios. For instructions, see "Configuring System Configuration Settings" on page 22-45.

   The System Configuration tab of the Radio form appears (see Figure 22-21).

2. Select the Talkgroups Configuration tab.

3. At the bottom of the form, click the **View/Modify** button.

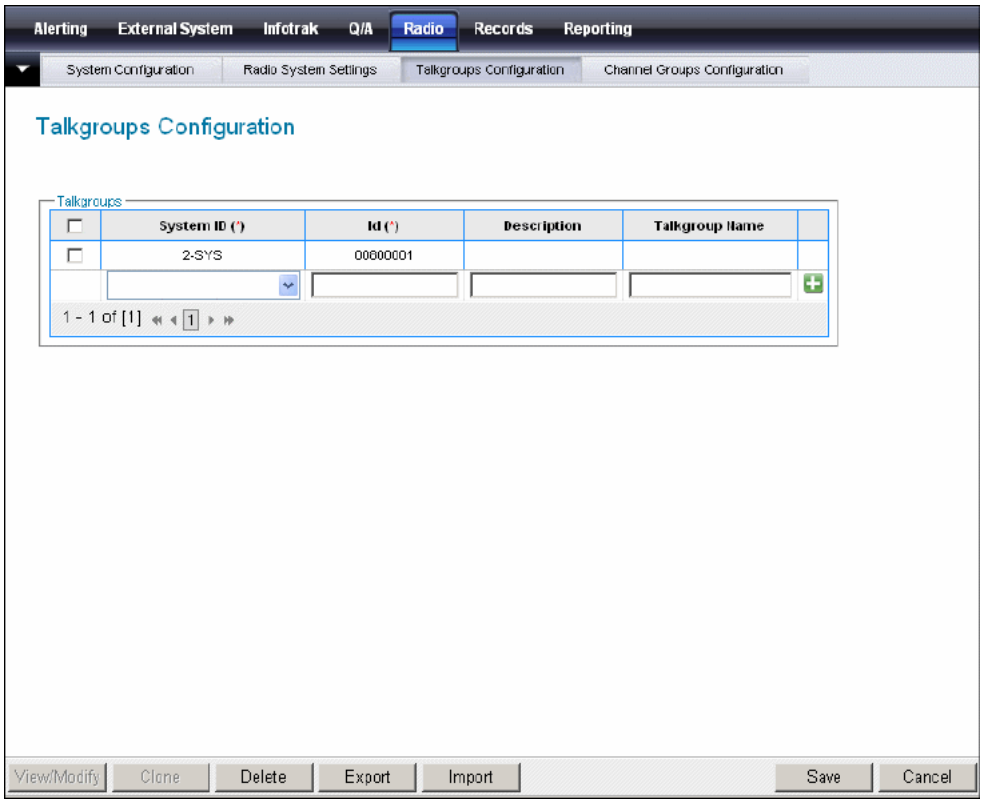


Figure 22-26 Radios Form – Talkgroups Configuration Tab

4. From the System ID list, select the radio system to which you are adding talkgroups.

5. In the ID field, enter the ID for the talkgroup.
6. In the Description field, enter a description for the talkgroup.
7. In the Talkgroup Name field, enter an alias for the talkgroup (optional).

   Aliases are the names that are used to identify the radio when a PTT (push-to-talk) transmission occurs. The ID and the alias name cannot be the same value within a radio system.
8. Click the plus symbol to the right of the talkgroup to save the talkgroup and add another row.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the agency information, even after you click Save.
9. Repeat the procedure to add any additional talkgroups.
10. Click **Save**.

Configuring Channel Groups

Channel Groups are groups of radio channels or talkgroups that a radio console operator can use to transmit an APB or other notifications. Channel Groups only function with radio systems that allow the CAD client to co-exist on the same workstations as the control application provided by Motorola.

Channel group information consists of the radio system ID, channel group name, type of channel group, description, and channels within the channel group. For details on enabling channel groups, see “Configuring Radio System Settings” on page 22-47.

To configure a channel group:

1. Access the form for Radios. For instructions, see “Configuring System Configuration Settings” on page 22-45.

   The System Configuration tab of the Radio form appears (see Figure 22-21).
2. Click the Channel Groups Configuration tab.

   Existing Channel Groups display on the left side of the form.

3. At the bottom of the form, click the **New** button.

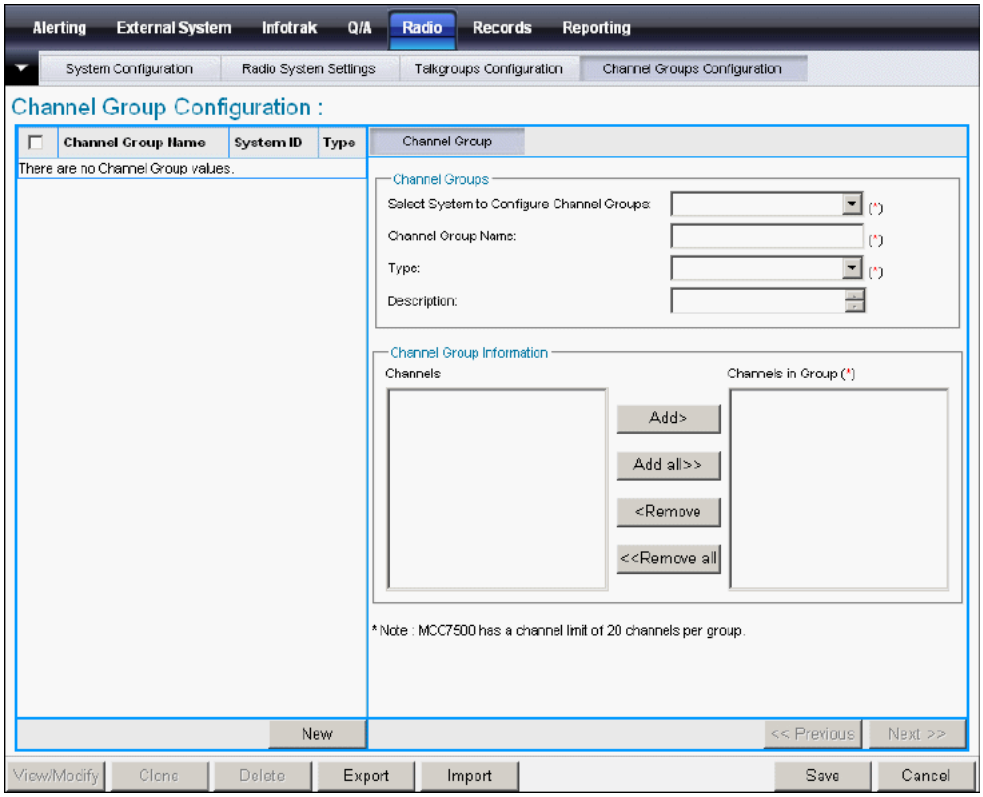


Figure 22-27 Radios Form – Channel Groups Configuration Tab

4. From the Select System to Configure Channel Groups list, select the radio system you are configuring channel groups for.

5. In the Channel Group Name field, enter a name for the channel group.

6. From the Type field, select the type of channel group:

   - Geographic. Geographic types are based on areas, teams, and beats.
   - Standard. Standard groups are not based on geographic criteria.

   These group names display within the Radio Channel Groups dialog box in the Group and Geographic tabs.

7. In the Description field, type a description for the Channel Group.

8. In the lower part of the window, select the channels (talk groups) you want to add to the Channel Group and select the **Add** button to add the channels to the Channel Group.

9. Click **Save**.

Configuring the Records Interface

If your system is integrated with PremierOne Records, you can configure PremierOne CAD to send incident information to Records. When the CAD to Records interface is enabled, *all* incidents are sent from CAD to Records. These incidents are sent at the time of creation and on all updates (including updates after the incident is closed). Records receives the CAD incidents as Calls for Service.

When the CAD to Records interface is enabled, you to set whether incident or report numbers are sent to Records from CAD when Records requests a number.

To configure the Records interface:

1. From the Navigation panel, select **Interface**, and then **Records**.

   The Records form appears.

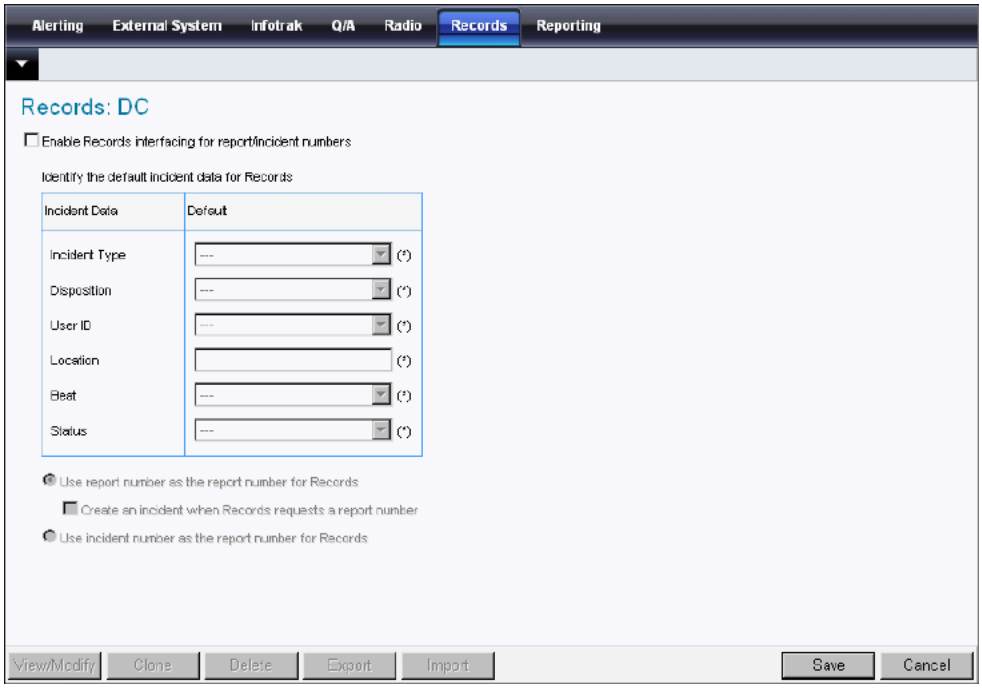


Figure 22-28 Records Form

2. Select the **Enable Records interfacing for report/incident numbers** check box.

3. In the default incident data section, select the defaults for all the incident data fields. These are used for every incident number pulled by Reports.

> **NOTE**
> The Incident type must have a valid IRF. Additionally, if the incident type creates an active incident, the incidents will show up in the CAD pending queue.

4. Do one of the following:

   - If you want to use a CAD *report* number for the Records case number, select **Use report number as the report number for Records**. CAD supplies Records the next report number for the agency when a Records user requests a new case folder number.

     If you also want a CAD incident to be created when you generate the report number, select the **Create an incident when Records requests a report number** check box. The incident data that you entered (disposition, incident type, and so on) are used to create the incident. This prevents any gaps in report numbering in CAD.

     The generated CAD incident type, disposition, user ID, location, beat, and status are always the same for every incident that is created in CAD. Only the incident number or report number are unique.

   - If you want to use a CAD *incident* number as the Records report number, select **Use incident number as the report number for Records**. When the Records user requests a new case folder number, the user will receive an incident number from CAD (not a report number).

Configuring Names and Descriptions of Reporting Data Warehouses

In Provisioning, you can edit the Name, Description, and URL of any data warehouses that have been configured through the use of the Reporting Configuration tool (contact Motorola for assistance with running this tool). The Name and Description you enter display in the Reporting application and in the Provisioning on the Reporting tab under Roles. For details on configuring roles for reporting, see “Adding Reporting Permissions” on page 8-16.

To configure names and descriptions of Reporting Data Warehouses:

1. From the Navigation panel, select **Interface**, and then **Reporting**.

   The Reporting form appears (see Figure 22-29).

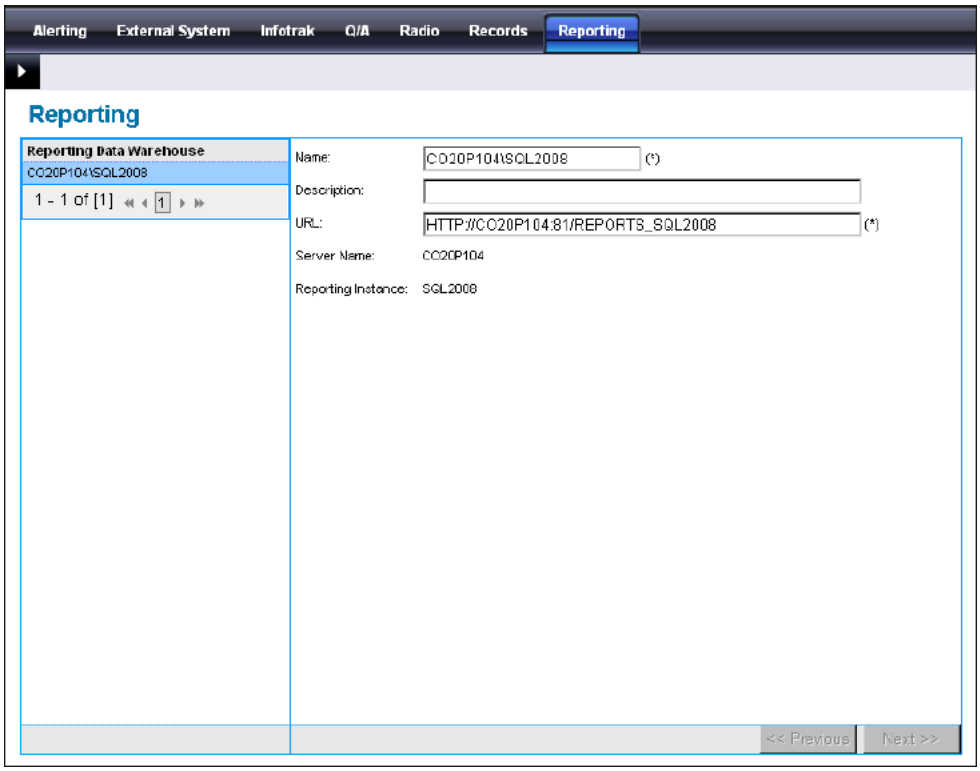


Figure 22-29 Reporting Form

2. On the left of the form, select the RDW you want to modify.
3. At the bottom of the form, click **View/Modify**.
4. In the Name field enter the name of the RDW.
5. In the Description field, enter a description of the RDW.
6. In the URL field, enter the URL to the reporting server.

> **CAUTION**
> Do not change the URL to the reporting server unless you are certain that the reporting server URL has changed.

7. Click **Save**.

CHAPTER 23

Configuring Jurisdictions

The Jurisdiction configuration item contains the following items:

- Area – Where you assign a response class and a default location to an area. Provisioning default locations for jurisdictional assignments allows units that are not GPS-equipped to be considered for ARL recommendations. For details, see "Setting the Default Location for Areas, Beats, and Sectors" on page 23-1.
- Beat – Where you assign a response class and a default location to a beat. For details, see "Setting the Default Location for Areas, Beats, and Sectors" on page 23-1.
- Location – Where you provision response classes for locations (addresses, intersections, street house number ranges, and common places). For details, see "Defining Response Classes for Locations" on page 23-4.
- Sector – Where you assign a response class and a default location to a sector. For details, see "Setting the Default Location for Areas, Beats, and Sectors" on page 23-1.
- Station – Where you set general station information, and preferred recommendation order for a station. For details, see "Setting the Information for Stations" on page 23-6.

Setting the Default Location for Areas, Beats, and Sectors

Use the Area, Beat, or Sector configuration item to do the following tasks:

- Assign a response class to an area, beat, or sector
- Assign a default location to an area, beat, or sector

Provisioning default locations for jurisdictional assignments allows units that are not GPS-equipped to be considered for ARL recommendations. PremierOne uses the coordinates of the default location in place of the geoverified location of a GPS-equipped unit. You provision a default location based on a primary beat, sector, or area assignment.

Assigning the Default Locations and Response Classes

Assign a default location to each area, beat, and sector. PremierOne uses the default location for all non-GPS equipped units that are assigned to this jurisdiction and that do not have their own geoverified location. Once you assign a default location, those units can be considered for ARL recommendations.

Assign a response class to a jurisdiction when that class is applicable to the entire jurisdiction.

The procedures for setting the default geoverified location are the same for areas, beats, and sectors, as are the fields used.

To assign a default location or response class:

1. From the navigation panel, select **Jurisdiction**, and then select either **Area**, **Beat**, or **Sector**.

   The Area, Beat, or Sector form appears. A list of existing jurisdictions displays on the left side of the form.

The procedures for setting the default geoverified location are the same for areas, beats, and sectors, as are the fields used.

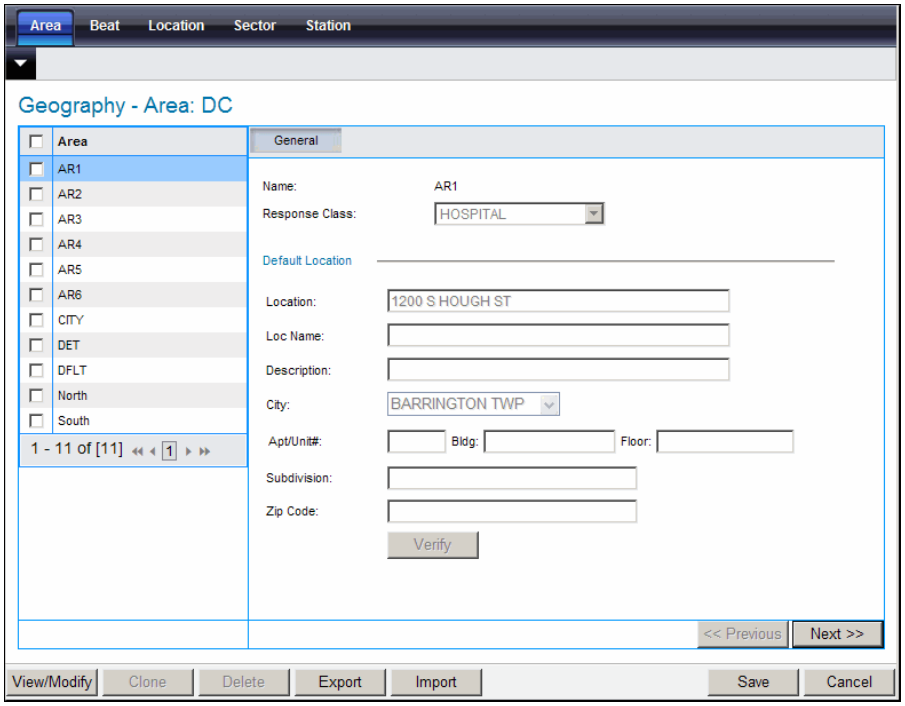


Figure 23-1 Area Form

2. From the list on the left, select the jurisdiction for which you want to assign a default location.

3. Click **View/Modify**.

4. In the Response Class field, select a response class for this jurisdiction, if needed.

5. In the Default Location section, type the location information, and then select the city. Click **Verify** to verify the address.

6. Click **Save**.

7. Repeat this procedure for additional jurisdictions.

Defining Response Classes for Locations

Use the Location configuration item to provision response classes for locations (addresses, intersections, street house number ranges, and common places).

Provisioning response classes for locations allows your agency to alter the response assignments based on a geographic value. If the location of the incident falls under a response class assignment, you can use a different run card, rather than the normal run card associated with the geography.

Example:

The location (address) of 4225 Wolf Road is McClure Junior High School. It gets the response class of school rather than the usual response class of other addresses along Wolf Road. (Because 4225 Wolf Rd is defined as a common place, PremierOne displays it as McClure Jr High after address verification.)

Adding and Modifying Response Classes for Locations

Assign a response class to locations that have needs based on their specific location.

To add or modify a response class for a location:

1. From the navigation panel, select **Jurisdiction**, and then select **Location**.

The Location form appears. A list of existing jurisdictions displays on the left side of the form.

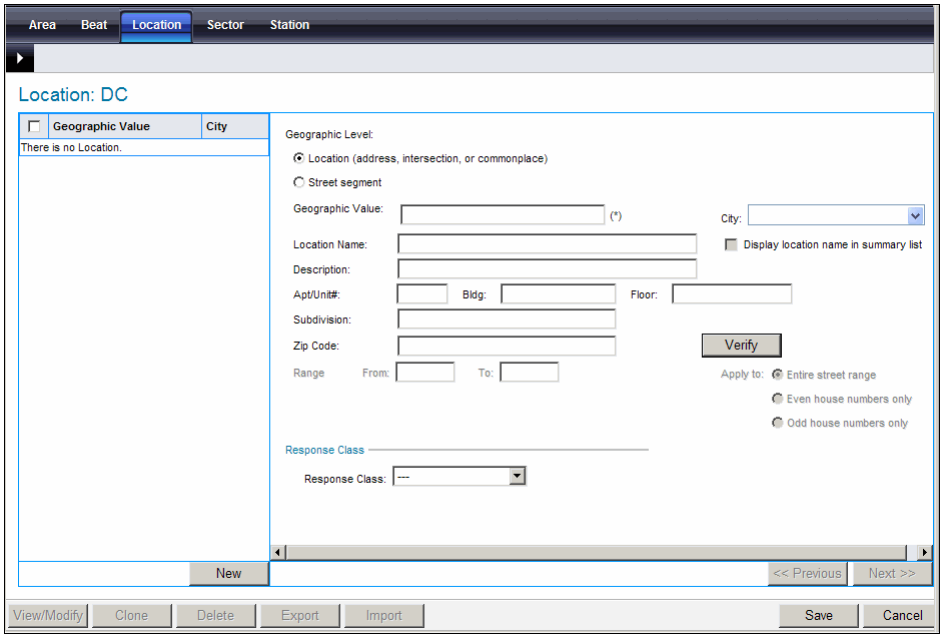


Figure 23-2 Location Form

2. To add a location:

   a. Click the **New** button at the bottom of the Geographic Value list on the left side of the form.

   b. Select the Geographic Level you want: **Location** (address, intersection, or common place) or **Street segment**.

   c. In the **Geographic Value** field, type any valid GIS location, and then select the city. If the location you type is a defined common place, PremierOne displays the common place name in the Location Name field. Click **Verify** to verify the location. The value you type appears in the list on the left when you click Save.

   d. If you selected Street segment for your Geographic Level, the Range fields appear so you can fill in your street number range and indicate whether to apply that range to the entire street, even house numbers only, or odd house numbers only. The response class will apply only to the specified segment.

> **NOTE**
> If the response class should apply to intersections within these street segments, you must add the intersections individually as locations.

3. To modify an existing location:
   a. From the list on the left, select the location you want to modify.
   b. Click **View/Modify**.
   c. Make any necessary changes.
4. From the **Response Class** list, select the response class to assign to this location.
5. Click **Save**.

Setting the Information for Stations

Use the Station configuration item to set the following information for the stations in your jurisdiction:

- General – Station ID, description, address, city, and beat
- Recommendations – Preferred recommendation order

Adding Station General Information

Use the General tab to add station information.

To add station general information:

1. From the navigation panel, select **Jurisdiction**, and then select **Station**.

The Station form appears. A list of existing stations displays on the left side of the form.

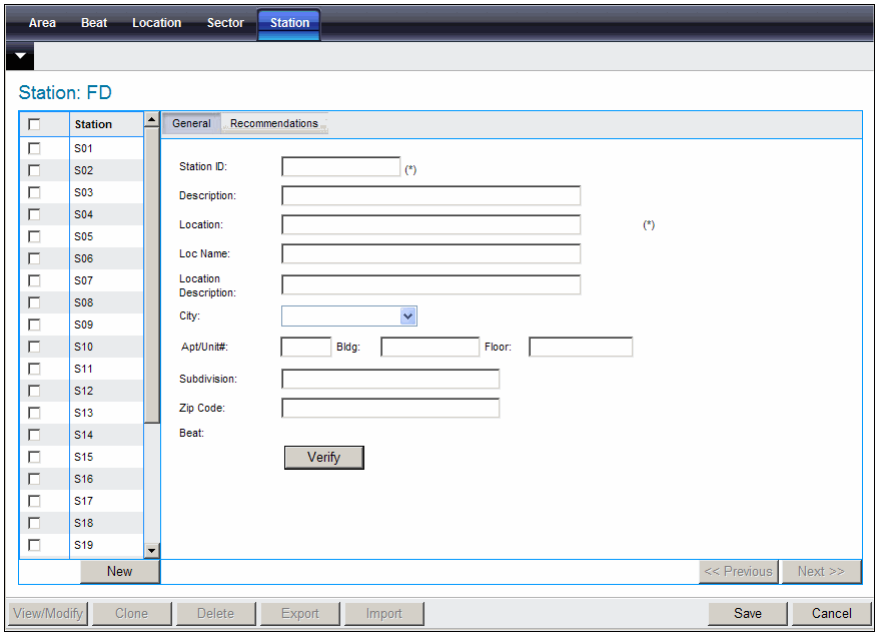


Figure 23-3 Station Form – General Tab

2. From the Station filter, select **Add New**.
3. Click **New** at the bottom of the Station list.
4. In the Station ID field, type a name for the new station.

   The name must be unique within your agency.
5. If needed, in the Description field, type a description for the station.
6. In the Address field, type the address for the station.
7. Optionally, in the City field, select the city, and then click **Verify** to have PremierOne verify the address and city combination.

   After verifying the address, PremierOne populates the Beat field. The beat is taken into account when a dispatcher signs onto an area.

If the address is a multi-beat intersection, a dialog box displays prompting you for the beat. Select the Beat and click the Select button.

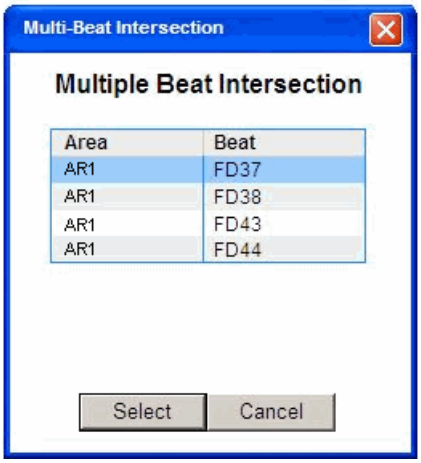


Figure 23-4 Multiple Beat Intersection Dialog Box

8. Click **Save**.

Adding Station Preferred Recommendation Order

Use the Recommendations tab to add the preferred recommendation order.

When units with the same capabilities reside in the same station and are available to be dispatched, some agencies prefer to dispatch one of these units over the others. You can provision a predefined list of units to be recommended when multiple units with the same capability are located at the same station or post.

The Preferred Recommendation Order only considers units while they are assigned to the station. The Preferred Recommendation Order is not considered for any unit that is in a Move-Up situation.

To add station preferred recommendation order:

1. Access the form for stations. For instructions, see “Adding Station General Information” on page 23-6.

2. Select **Add New**.

3. From the list of stations on the left, select the station with the recommendation order you want to set so it is highlighted. You do not need to select the check box.

4. Select the Recommendations tab.

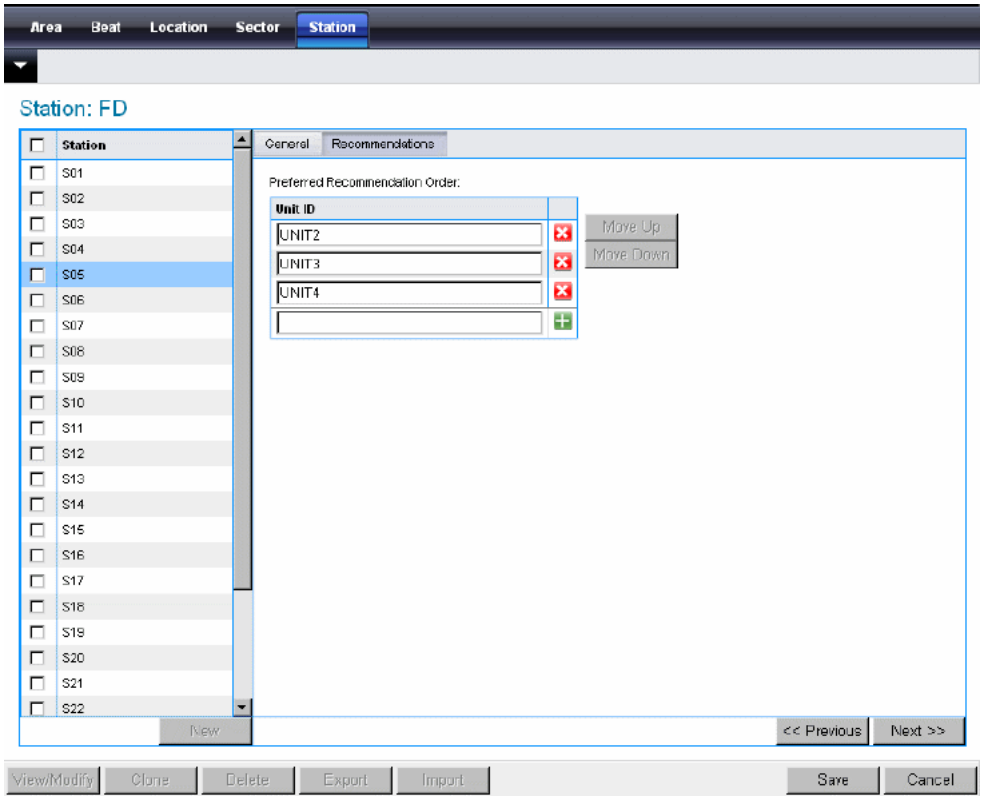


Figure 23-5 Station Form – Recommendations Tab

5. Click **View/Modify**.

6. In the Unit ID field, type the ID of the first unit you want in your recommendation order, and then click the plus symbol at the end of the row. The unit must be for your agency (the provisioning agency).

7. Continue to add units until your recommendation order is complete.

   You can change the recommendation order by selecting a unit so the row is highlighted, and then clicking the **Move Up** or the **Move Down** button.

8. Click **Save**.

CHAPTER 24

Configuring Notifications

The Notification configuration item contains the following items:

- Emergency Notification – Where you create notifications for when an officer has an emergency and needs immediate assistance. For details, see “Configuring the Emergency Notification Message” on page 24-1. Temporary units can also be created off duty radios during an emergency.
- Manual Notification – Where you create messages used to notify the appropriate people of an situation, whether it is routine or an emergency. For details, see “Configuring Manual Notifications” on page 24-3.

Configuring the Emergency Notification Message

Use the Emergency Notification form to configure who receives an emergency notification message and what the message contains when a Mobile Alert is activated.

The Mobile application contains an Alert button that when activated issues an emergency notification message to configured users and Mobile units that are within a specified distance. The message contains information about the unit, such as unit ID, last known location, and when the alert was initiated.

To configure an emergency notification message:

1. From the navigation panel, select **Notification**, and then select **Emergency Notification**.

The Emergency Notification form appears.

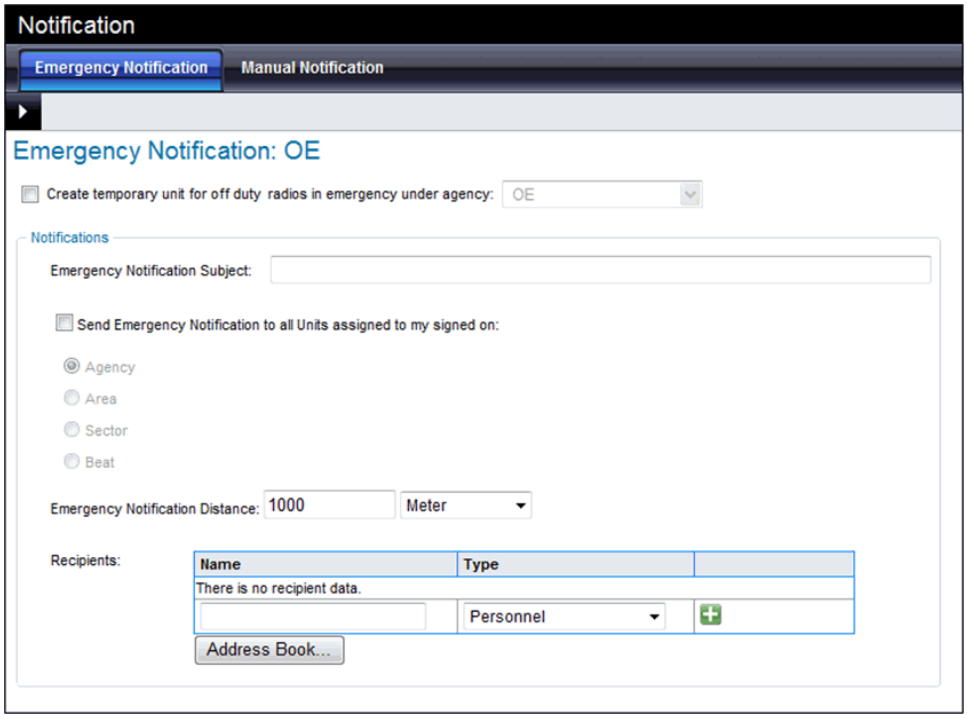


Figure 24-1 Emergency Notification Form

2. Select the **Create temporary units for off-duty radios in emergency under agency** check box, and then choose the agency to assign the radios to.

> **CAUTION**
> Sometimes radios are assigned to an equipment only agency. If this is so, when the Emergency button is activated by an off-duty officer, there may be no response because no dispatchers are assigned to equipment only agencies.

3. In the Emergency Notification Subject field, type the subject of your notification, such as `Shots fired`. `Officer needs help`.

4. To send an emergency notification to all units assigned to your signed on agency, area, sector, or beat, select the **Send Emergency Notification to all Units assigned to my signed on** check box, and then select the jurisdiction.

5. Select the distance to other units in the vicinity that will receive the message, and then select the unit of measurement (feet or meters).

6. In the Recipients area, do the following:

   a. Type or select from the Address book others that you want to receive this message.

   b. In the Type field, select the type of recipient: personnel, console, unit, or group.

c. Click the plus symbol to the right of the recipient information to save the information and add another row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the recipient information, even after you click Save.

7. Click **Save**.

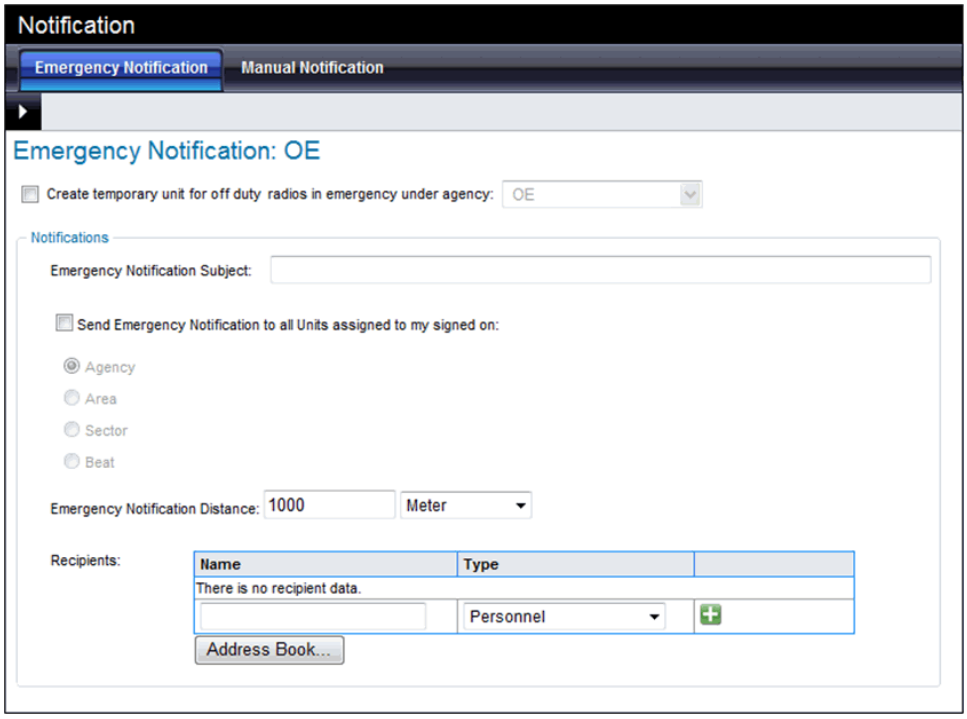


Figure 24-2 Emergency Notification Form

Configuring Manual Notifications

You can provision PremierOne to send notification messages to personnel or groups that need to be notified as part of an incident response. Once you create notification messages, you attach them to IRFs so that the message is sent when an incident of the IRF type is initiated. For more information on IRFs, see "Configuring Incident Response Factors" on page 13-37.

Notifications are delivered using the following methods:

- CAD users – As notification email messages. These messages can be read with the NT command.

- Mobile users – As messages in a pop-up dialog box.
- External users – As emails.

PremierOne supports interfacing to an SMTP (Simple Mail Transfer Protocol) mail server and to a domain name (for example, `@DenverCty.gov`). This allows PremierOne to send messages to external email accounts or text messages to mobile phones and PDAs as long as the connected mail server is properly provisioned and supports forwarding all required domain names to external network service providers as required. For more information, see Chapter 21 “Using Messaging” in the *PremierOne CAD User Guide*.

When the recipient list contains Short Message Service (SMS/text message) users, your email server forwards the SMTP email messages to the appropriate network provider’s SMS gateway. PremierOne provides the notification messages to a single SMTP server. You are responsible for ensuring and completing the network transaction from the SMTP server to the appropriate carrier network(s) on which the messages are to be received.

SMTP mail requires a valid domain and mail server. If multiple domains are required, it is your responsibility to configure the SMTP server to support all outbound domains (`@tmomail`, `@sprint.com`, `@vtext.com`) and all inbound domains (`Denver.org`, `ci.westminster.co.us`).

PremierOne supports sending outbound email to multiple external systems; however, your equipment (or hosted services) must also be set up to send email addresses with each external domain, if that is also required.

You can add, modify, clone, and delete notifications. For details on modifying, cloning, and deleting notifications, see “Working With Configuration Items” on page 2-9.

To add a manual notification:

1. From the navigation panel, select **Notification**, and then select **Manual Notification**.

The Manual Notification form appears. A list of existing manual notifications displays on the left side of the form.

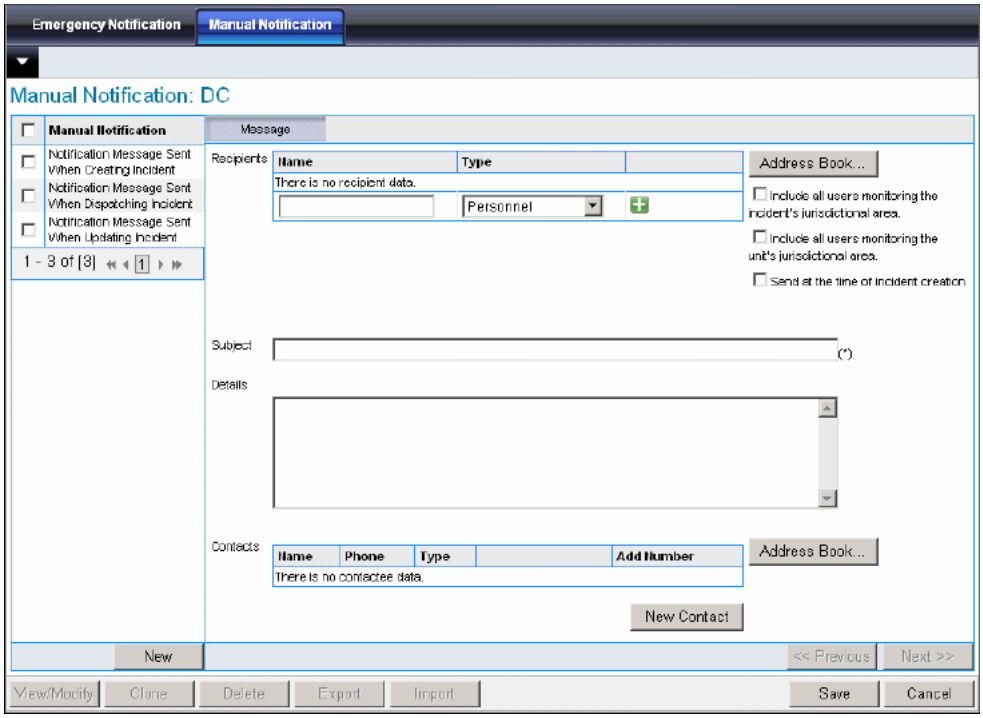


Figure 24-3 Manual Notification Form

2. At the bottom of the Manual Notification list, click the **New** button.

3. In the Recipients fields, type the full recipient address, such as RSmith@DC.

   You can select multiple recipients, creating a group to receive the notification message.

   a. Click **Address Book** to select the recipients from an agency or global address book.

   b. From the Type list, select the type of recipient: **Personnel**, **Console**, **Unit**, or **Group**.

   c. In the Name field, enter the name of the recipient.

   d. Click the plus symbol to the right of the recipient information to save the information and add another row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the recipient information, even after you click Save.

e. From the selections below the **Address Book** button, select who to include and select Send at the time of incident creation.

> **CAUTION**
> You **must** select Send at the time of incident creation. If you do not select this option, no notifications are sent. You may select one or both of the other options as well.

4. In the Subject field, type a subject for the notification.

   The subject appears in the Manual Notification list at the left of the form and in the lists from which users choose notifications when configuring IRFs. Therefore, make your subject as meaningful as possible.

5. In the Details field, type the text of the message.

6. To add a manual notification contact, do the following:

   A manual notification contact is a person to be contacted by telephone, such as the mayor, sheriff, or Public Information Officer.

   a. Click **New Contact**.

   b. In the first New Contact field, type the name of the new contact.

   c. In the second New Contact field, type the phone number.

   d. From the list, select what type of number the phone number references: **Fax**, **Home Phone**, **Mobile**, **Pager**, **Phone**, **Radio**, or **Work**.

   e. To add a contact or group using the address book, click **Address Book**.

   f. Click **Submit**.

      Each unsaved notification appears in the Manual Notification list in blue text.

7. Click **Save**.

   The notifications you added appear in the Manual Notification list in black text.

   When a notification is sent upon incident initiation, an entry appears in that incident's history showing that a notification was associated with the incident. The History shows who sent the notification, from which console, the time and date, the subject, and any other information such as status, contactee, and comments.

CHAPTER 25

Configuring Mapping

The Mapping configuration item contains the following items:

- GIS Data – Where you set the active geodatabase, and verify and reverify addresses in the GIS database.
- Location Verification – Where you set the details for location verification.
- MUD Setting – Where you set the multi-unit display settings for each role.
- Route solving – Where you set the default impedance for route solving.
- Icons – Where you set icons for incidents, call locations, units, and cameras.
- Cadence – Where you set the cadence for units and vehicle types.
- Agency Setting – Where you set display attributes for maps for each agency.
- Person Location – Where you set when a person icon displays and the information it contains.
- Configure ARL History Playback Defaults – Where you set the maximum time period value and the maximum number of units that a user can specify when performing an ARL playback request.
- Configure Gate Status – Where you set the timeout value for gate status or disable timeout completely. You can also specify when the gate icons are removed from the map.

Setting the Active GIS Database

Use the GIS Data configuration item to set the active database. Place your inactive database into restrictive mode while you are updating, and then place it back to All Users when you are finished.

To set the active geodatabase:

1. From the navigation panel, select **Mapping**, and then select **GIS Data**.

   The GIS Data form appears.

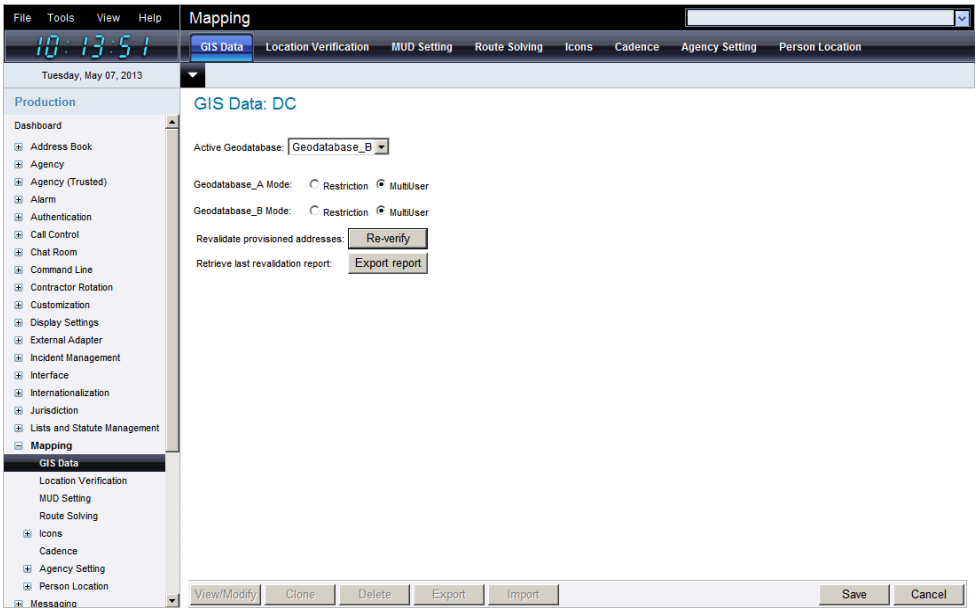


Figure 25-1 Mapping – GIS Data Form

2. Select **Restrictive Mode** for your inactive database while you are importing/staging a GIS update.

   Although the provisioning is done at the agency level, the setting is applied to all the agencies in a multi-agency environment.

3. From the Active Geodatabase list, select the geodatabase you want to activate.

4. Select **MultiUser Mode** for the inactive database.

5. Click **Save**.

Revalidating Provisioned Addresses

Use the GIS Data configuration item to revalidate addresses in the active Geodatabase. You can also export the latest revalidation report from this screen.

The revalidation checks all address related records, as follows:

- Alarm > Alarm Records
- Incident Management > Premise Hazard > Premise Hazard Record
- Incident Management > Response Message
- Jurisdiction > Area
- Jurisdiction > Beat
- Jurisdiction > Location
- Jurisdiction > Sector
- Jurisdiction > Station
- Unit Recommendation > Response Card > Incident Response Factor
- Unit Recommendation > Response Card > Response ID
- Unit Recommendation > Run Card

A report is generated for all provisioned addresses that failed to revalidate.

The revalidation may take some time depending upon the size of the database. While the revalidation is in progress, you can continue to use Provisioning for other purposes. A message appears letting you know when the process is running.

To revalidate an active geodatabase:

1. From the navigation panel, select **Mapping**, and then select **GIS Data**.

   The GIS Data form appears.

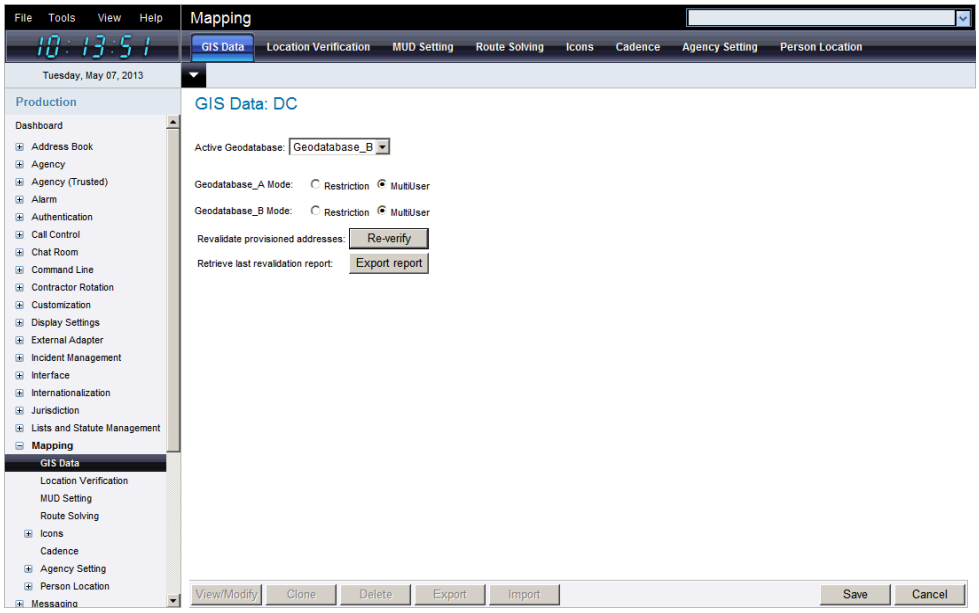


Figure 25-2 Mapping – GIS Data Form

2. In the Active Geodatabase field, select the database you want to revalidate, and then click **Re-verify**.

   The process begins, and a `Revalidation is in progress` message appears to the right of the Re-verify button.

Exporting the Geodatabase Revalidation Error Report

Use the GIS Data configuration item to export an Error report for invalid Geodatabase addresses. When you run a Geodatabase revalidation, the report is generated. See "Revalidating Provisioned Addresses" on page 25-2. The Error Report is a text file.

To export the Geodatabase Revalidation Error Report:

1. From the navigation panel, select **Mapping**, and then select **GIS Data**.

   The GIS Data form appears.

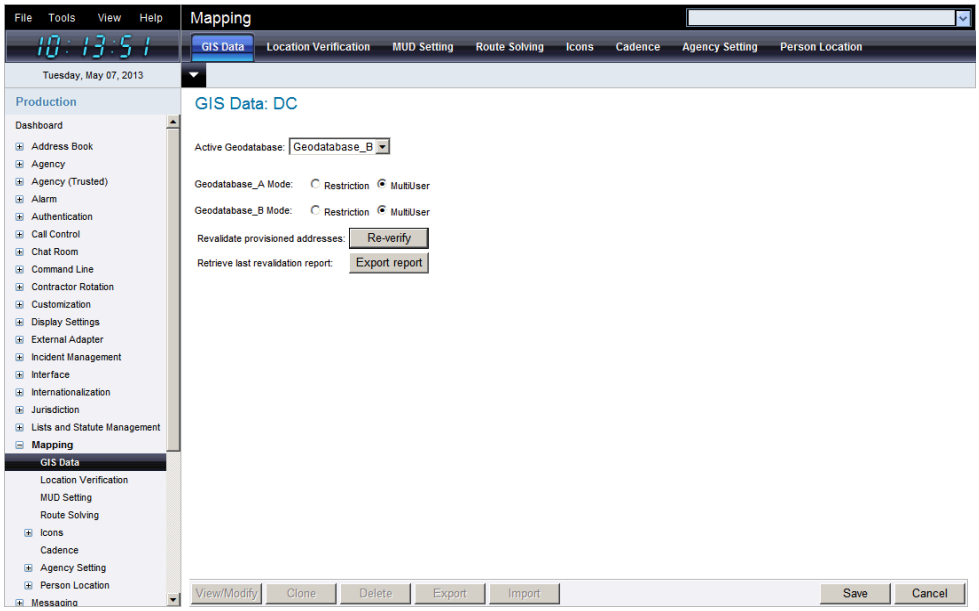


Figure 25-3 Mapping – GIS Data Form

2. If you have not run the revalidation, do so. See "Revalidating Provisioned Addresses" on page 25-2.

3. In the Active Geodatabase field, ensure you have the Geodatabase file you want, and then click **Export Report**.

The report appears as a text file.

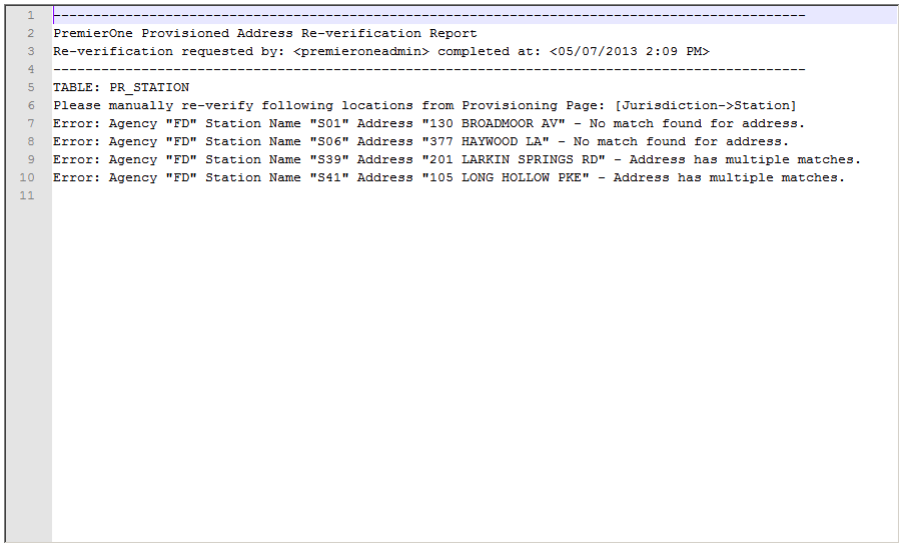


Figure 25-4 Revalidation Address Error Report

Configuring Location Verifications

Configure location verification information when you need to change any location verification properties such as wildcard characters, intersection delimiter characters, maximum number of search results to display, and whether to display high and low cross streets.

To configure location verification information:

1. From the navigation panel, select **Mapping**, and then select **Location Verification**.

   The Location Verification form appears.

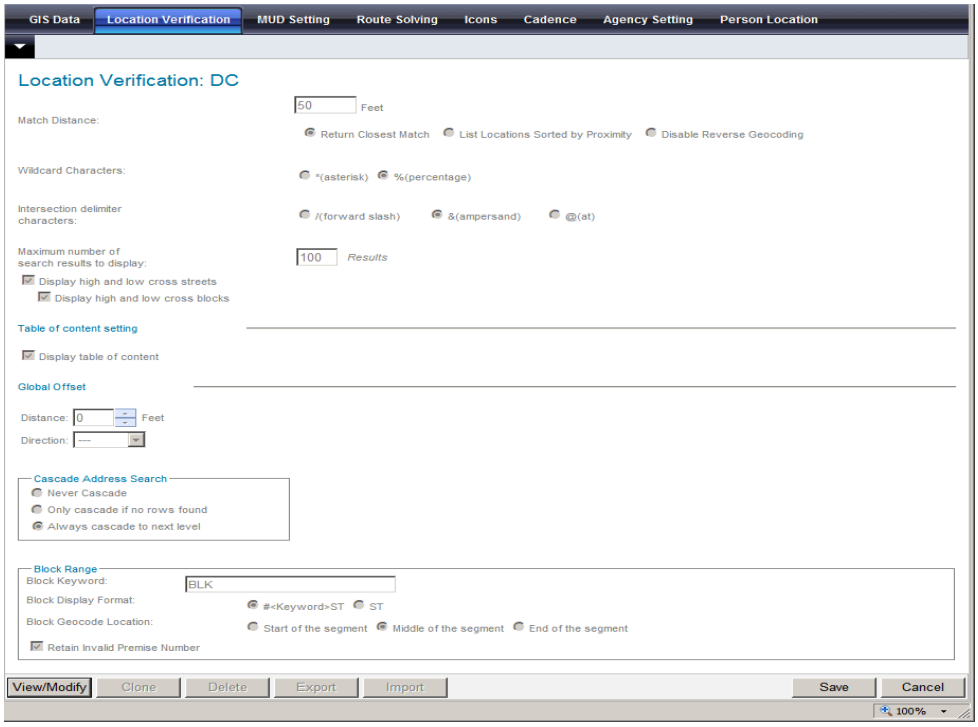


Figure 25-5 Mapping – Location Verification Form

2. Click **View/Modify** to edit the fields.

3. In the Match Distance field, enter the maximum distance a location can be from a lat/long value to be considered a match.

4. Select one of the following:

   - Return Closest Match – CAD searches for the closest address, intersection, or common place using the map coordinate. The closest location populates the Location field and the entered map coordinate is moved to the Description field.

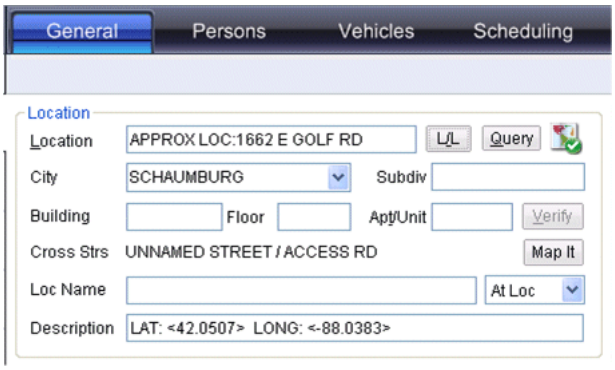


Figure 25-6 Results Of Return Closest Match

   - Disable Reverse Geocoding – CAD searches for the closest address, intersection, or common place using the map coordinate. The map coordinate is used as the location and populates the Location field.

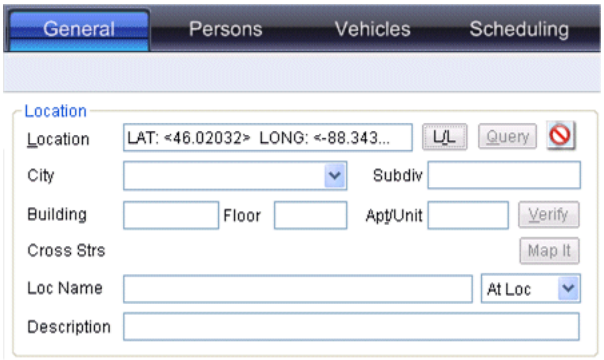


Figure 25-7 Results Of Disable Reverse Geocoding

   - List Locations Sorted by Proximity – CAD returns all of the addresses, intersections, or common places within the Match Distance radius and sorts them by distance from the map coordinate in the Address Verification list.

5. In the Wildcard Characters field, enter the character to use as a wildcard in the address, such as `Maple*` or `Maple%`.

6. In the Intersection delimiter characters field, enter the character that is used to specify intersections, such as `Main&Broadway` or `Main/Broadway`.

If your agency has a large number of addresses with fractions in them, you may want to use a different delimiter than /.

NOTE
For a Suite environment, you must use the & delimiter. Records only supports the & delimiter for intersections.

7. In the Maximum number of search results to display field, enter the maximum number of addresses to be returned.

NOTE
Because CAD filters the addresses for duplicates *after* the maximum is reached, the Search results can appear to be considerably less than expected.

8. To display the cross streets with returned addresses, select the **Display high and low cross streets** check box. For example, 103RD AVE / CHURCH RANCH BLVD.

9. To have cross street blocks precede street names, select the Display high and low cross blocks check box. For example, 12000 103RD AVE / 7200 CHURCH RANCH BLVD.

10. To display the colors for different layers, select the **Table of Contents Setting** check box.

    The legend indicates the different colors for different layers.

11. In the Global Offset section, set whether the intersection location is offset by the specified amount and to the specified direction if there are multiple beats at the location that belong to the agency you are provisioning. When you specify an offset, only one record is generated per intersection using the intersection point plus the amount and distance of offset you enter.

    - Distance – Enter the distance in feet or meters, depending on your agency configuration (Agency – Agency Details).
    - Direction – Select the direction for the offset. Options include --- (for None), North, South, East, West, NE, NW, SE, SW. A direction value is required if the global offset distance value is greater than zero.

    If there are multiple agencies for the intersection, this setting is not used.

12. Select one of the following:

    - Never cascade – An address search only occurs for the address exactly as it was entered. For example, a premise search will search for premise only, a street search will search for streets only, and so on.

      For example: `43 GOODMAN CL, BASINGSTOKE`

The search is initiated at the PREMISE level. If there is no match for `43 GOODMAN CL`, then no addresses are returned.

- Only cascade if no rows found – An address search occurs for the address as it was entered, but if no matches are returned, the search will continue to the next level search.

  A search is initiated at the PREMISE level. If there is no match for `43 GOODMAN CL`, then a search is made at the STREET level for `GOODMAN CL`. If there is no match for `GOODMAN CL`, then a search is made at the District/Town level for `BASINGSTOKE`.

  At any point, the cascade search does not continue if at least one address is matched.

- Always cascade – An address search automatically continues to search to the next search level, even if matches are returned.

13. In the `Block Keyword` field, type a keyword. The keyword must be a single word made up of alphabetic characters.

    The keyword is used in CAD and Mobile to identify when a user wants to validate a block range, such as `700 BLK CEDAR AVE`, or `700 BLK CEDAR AVE`, depending upon the display format setting.

14. For the `Block Display Format`, select one of the following:

    - #<Keyword>ST – The resulting display of the verified block shows the keyword and the street name, such as `700 BLK CEDAR AVE`.

    - ST – The resulting display of the verified block shows the street name only, such as `700 CEDAR AVE`.

15. For the `Block Geocode Location`, select one of the following.

    - Start of the segment – The geocode location will be set to the start of the selected segment.

    - Middle of the segment – The geocode location will be set to the middle of the selected segment.

- End of the segment – The geocode location will be set to the end of the selected segment.

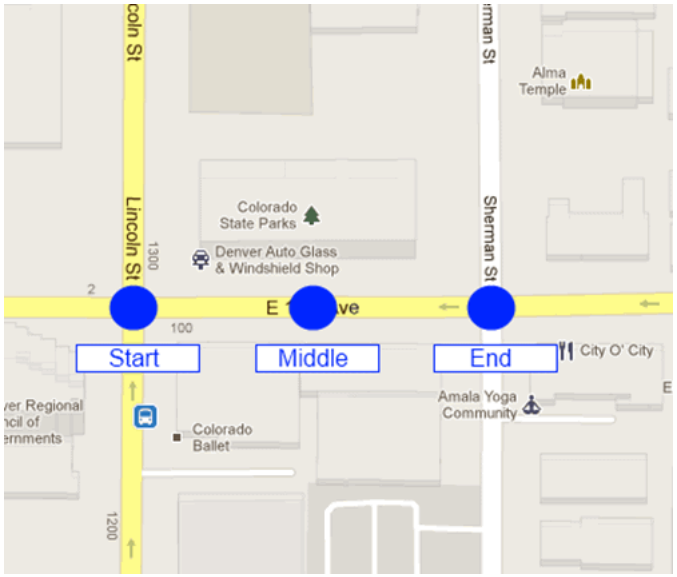


Figure 25-8 Block Geocode Location

16. To retain the street number when it was not found as part of an address, select the **Retain Invalid Premise Number** check box.

    When this option is selected, the invalid street number is retained and depending on the block display format chosen, may be enclosed by parentheses based on the following format of the Block Display Format setting:

    - Number and Block format – invalid street number enclosed by parentheses

      ```
      (250) 200 BLOCK E MAIN ST
      ```

    - Street Only format – invalid street number not enclosed by parentheses

      ```
      250 E MAIN ST
      ```

17. Click **Save**.

Configuring Additional Verification Settings

You can configure the following additional verification settings in the System Management Portal Configuration. These items should be configured before doing Provisioning.

- StreetSearchEnabled – Verify an address when only a street name is entered
- SoundexSearchEnabled – Always use Soundex on street searches

- BestMatchFirstEnabled – Rate the address results that are returned with the best match first

To configure additional verification settings:

1. From the System Management Portal, select the **Configuration** icon.

   A list of Managed Entities displays.

2. Click the Edit tab.

3. In the navigation pane on the left, scroll to the item `Addressing`.

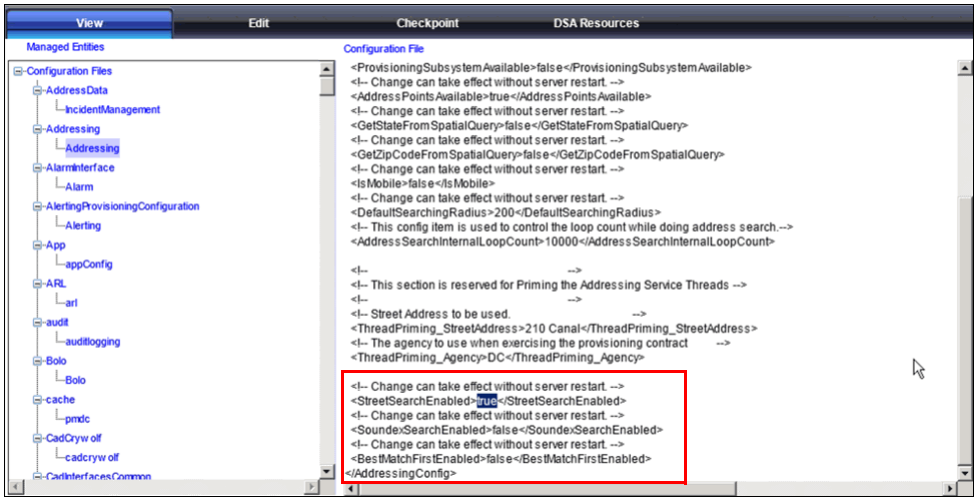


Figure 25-9 Configuration Window – Edit Tab For Addressing

4. Select the `Addressing` item.

5. In the right window pane, scroll to the bottom of the file.

6. Change any of the following:

   - StreetSearchEnabled – default is `True`
   - SoundexSearchEnabled – default is `False`
   - BestMatchFirstEnabled – default is `False`

7. Click **Save**.

   You do not need to restart the server to see the changes.

Configuring the MUD Setting

Use the MUD Setting configuration item to specify multi-unit display (MUD) settings on the mobile map. Vehicles can be displayed for selected jurisdictions or agencies.

To configure multi-unit display settings:

1. From the navigation panel, select **Mapping**, and then select **MUD Setting**.

   The MUD Setting form appears. A list of existing roles displays on the left side of the form.

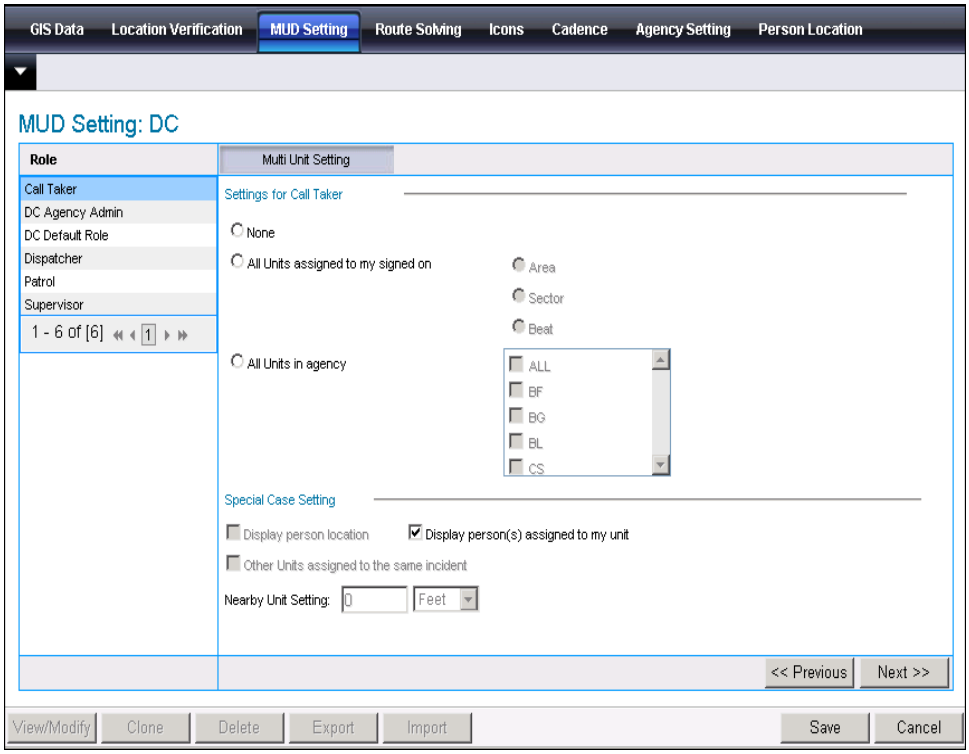


Figure 25-10 Mapping – MUD Setting Form

2. From the Role list, select the role with the settings you want to modify.

3. Click **View/Modify** to edit the fields in the form.

   The form refreshes, and the Settings for {Role} field appears.

4. In the Settings for {Role} section, select which unit display settings you want the role to have.

   a. To have no display of other units on the map for the role, select **None**.

   b. To display other units on the map for the role based on jurisdiction, select **All Units assigned to my signed on** button and then select Area, Sector, or Beat.

c. To display other units on the map for the role based on agency, select the **All Units in Agency** button, and then select the agencies.

5. To display all person locations when they are away from the vehicle, select **Display person location**.

   The person location is determined by GPS in the person's portable radio or portable radio microphone.

6. To display only the person location of individuals assigned to your unit, make sure only the **Display person(s) assigned to my unit** check box is selected (it is selected by default).

7. To display units and persons on the map that are assigned the same incident regardless of whether they meet the area, agency, or beat criteria, select the Other Units assigned to the same incident check box. Then enter the distance that the units must be within in the Near By Unit Setting field.

   As an example, this option would be used when a unit was out of its jurisdiction or close to a jurisdictional boundary, and wanted to display other units assigned to the same incident as the unit. Under normal circumstances, the units wouldn't display.

8. Click **Save**.

Configuring Route Solving

Use the Route solving configuration item to control shortest route calculations.

Modify route solving settings when you need to change or add a time or travel distance cost, change the day and time settings for when the cost settings are in effect, or change default restrictions.

To modify route solving settings:

1. From the navigation panel, select **Mapping**, and then select **Route Solving**.

The Route Solving Setting form appears.

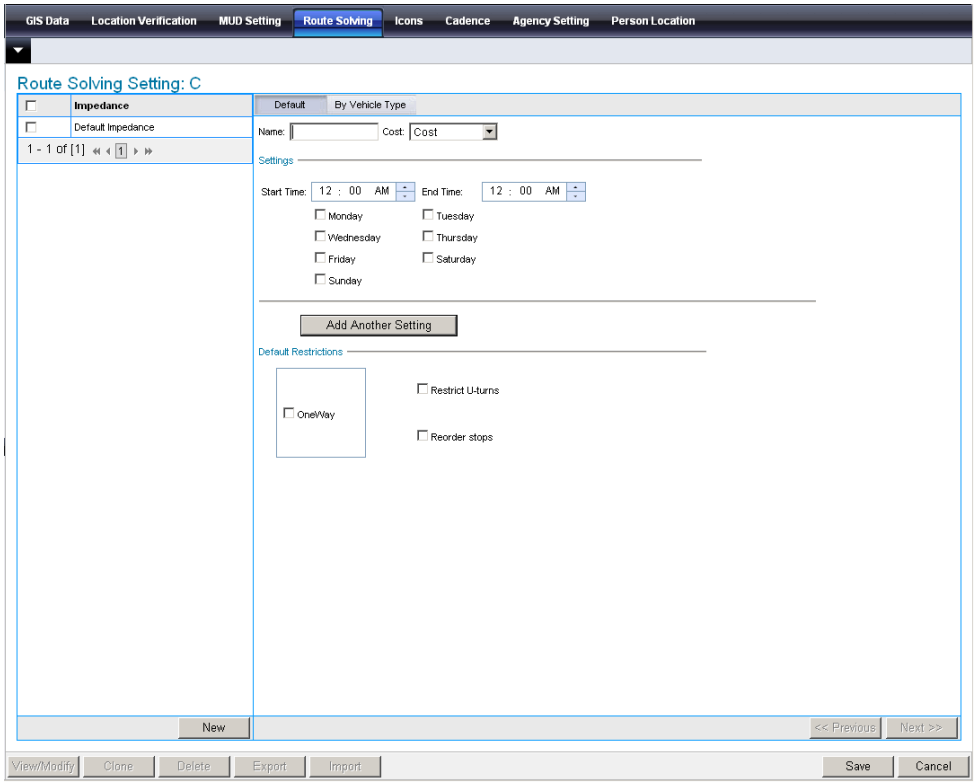


Figure 25-11 Mapping – Route Solving Setting Form

2. Do one of the following:

   - To modify the Default Impedance values, click **View/Modify**.
   - To create a custom set of restrictions, click **New**.

3. In the Name field, type a new name if you are creating a custom set of restrictions.

4. From the Cost list, select the cost factor.

   The cost factor is a relative value describing the amount of total distance or the time required to traverse the distance. The value is calculated using the total path length or the required travel time based on an average speed and length of each segment in the path.

5. In the Settings section, set or modify the days of the week and time of day for which the settings will be in effect.

   To add multiple settings, for example, different times for different days of the week, click **Add Another Setting**.

6. In the Default Restrictions section, select whether to use default restrictions for one way streets, and then select whether to restrict U-turns and to Reorder stops.

7. Click **Save**.

Modifying Route Solving By Vehicle Type

You can limit the vehicle types for which an Impedance Definition is applied. For example, if you want to use a different travel cost attribute for heavier vehicles, you can create an Impedance Definition just for those vehicle types.

To modify route solving by vehicle type:

1. Access the Route Solving Setting form as described in "Configuring Route Solving" on page 25-13.

2. Click the By Vehicle Type tab.

   The Vehicle Types form appears.

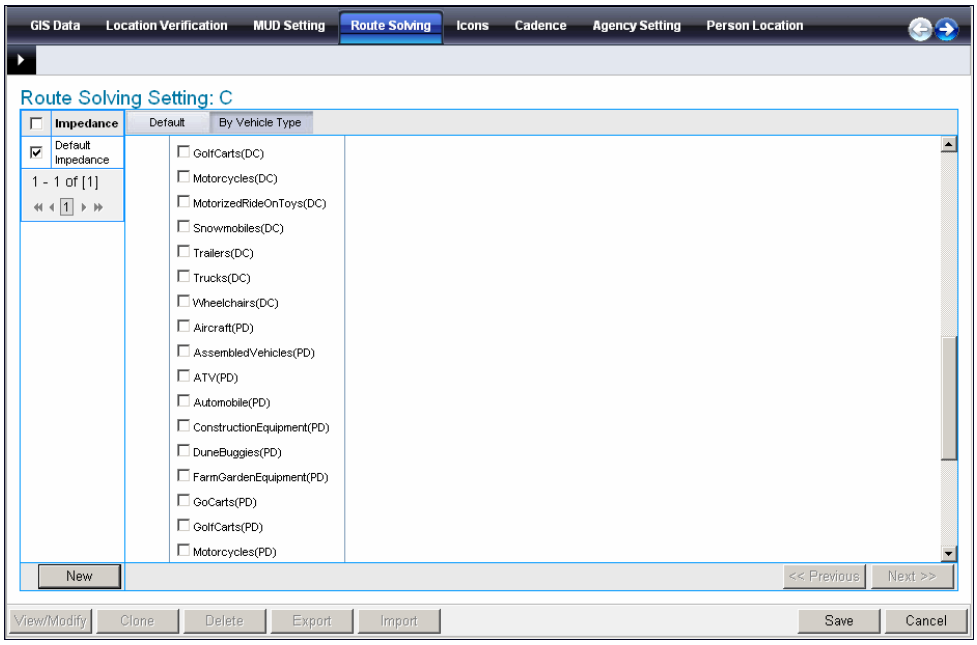


Figure 25-12 Mapping – Route Solving By Vehicle Type Form

3. In the Vehicle Types section, select the vehicle type you want to restrict.

4. In the Restriction setting for selected vehicle type(s) section, select the level of restriction for the vehicle type:

   - One Way – The route honors one-way roads.
   - Restricted U-turns – The route will not ask the driver to make a u-turn.
   - Reorder stops (Future use) – If the route has multiple destinations (i.e. a deputy has to deliver multiple summons), the route solver will find the best route regardless of the order in which destinations are defined.

5. Click **Save**.

Configuring Incident and Unit Icons

Use the Icons configuration item to select the icons that display for incidents, call locations, cameras, and units. You can use different icons depending on the situation. When you add or modify icons, you enter information on one of the following tabs:

- Incident – Where you select icons for a combination of the individual incident type (or all incident types) and the status. You also determine if the same setting applies to both Mobile/Handheld settings and CAD settings or if you want different settings for Mobile/Handheld and CAD.
- Call Location – Where you select icons for call location and ANI/ALI for both Mobile and CAD.
- Unit – Where you select icons for vehicle capabilities based on status for both Mobile/Handheld and CAD.
- Camera Icon – Where you select icons for camera type and status. This is for use in CAD only.

Adding and Modifying Incident Icons

Add or modify incident icons when you need a new or different incident icon to display on your maps. The icon is applied to the display of all incident icons.

NOTE
Labels for icons on the CAD and Mobile/Handheld maps use the colors as defined for status monitors.

To add or modify incident icons:

1. From the navigation panel, select **Mapping**, and then select **Icons**.

   The Icons form appears with the Incident tab in focus.

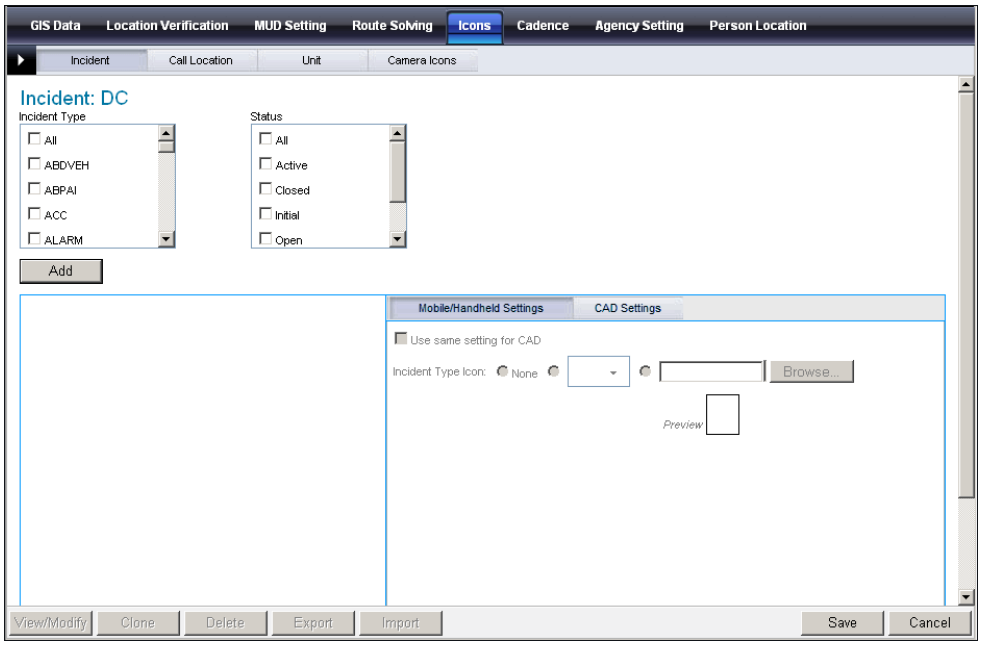


Figure 25-13 Mapping – Icons Form, Incident Tab

2. Click **View/Modify**.

3. Select the incident type and status.

   a. From the Incident Type list, select the incident type to which you want the icon to apply. You can select more than one incident type or select **All**.

   b. From the Status list, select the status to which you want the icon to apply. You can select more than one status. Alternatively, select **All**.

   NOTE
   You must select and Incident Type and Status.

   c. Click **Add**.

A row appears in the table for each incident type and status you selected.

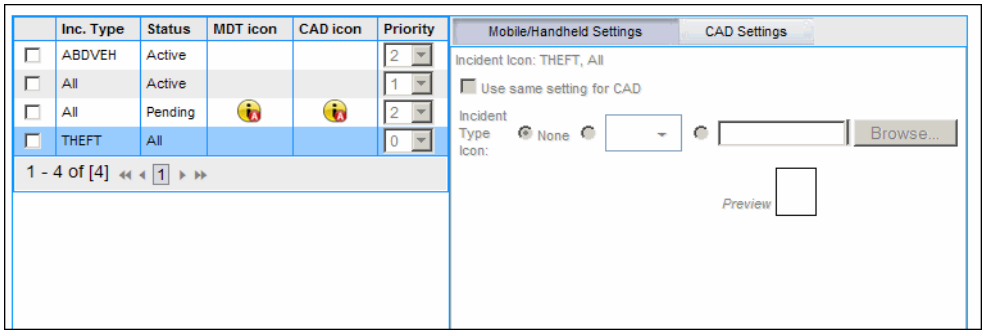


Figure 25-14 Icons Form – Icon Incident Table

4. To use the same settings for Mobile/Handheld as CAD, select the **Use same setting for CAD** check box.

5. Click the CAD Settings tab.

6. In the list of icons in the summary list, select the row you want to select an icon for.

7. To add the icon:

   a. In the box to the right of the Summary list of icons, select the button to the right of None, and then select the icon you want to use.

   b. Alternatively, you can select the **Browse** button and navigate to the location of the new icon and click **OK**. Your selected icon will appear in the Preview box.

8. To use different settings for Mobile/Handheld, select the Mobile/Handheld Settings tab, make sure the **Use same setting for CAD** check box is clear, and repeat this procedure.

9. Click **Save**.

   You can use the Priority setting to control the icon that is used when there is not an exact match for an Incident Type and Status. For example, assume an incident of type THEFT and a status of PENDING. PremierOne will try to use an icon that was provisioned specifically for a Theft-Pending incident. Instead, PremierOne finds an icon provisioned for ALL incident types in a Pending status, and another for THEFTS in ALL statuses. In this case the Priority value is used to determine which icon to use (lowest value has the highest priority). The priority is not the incident priority.

Adding and Modifying Call Location Icons

Add or modify call location icons when you need a new or different call location or ANI/ALI icon to display on your maps. The icon is applied to the display of all call location icons.

To add or modify call location icons:

1. Access the Icons form. For details, see "Configuring Incident and Unit Icons" on page 25-16.

   The Icons form appears with the Incident tab in focus (see Figure 25-13).

2. Click the Call Location tab.

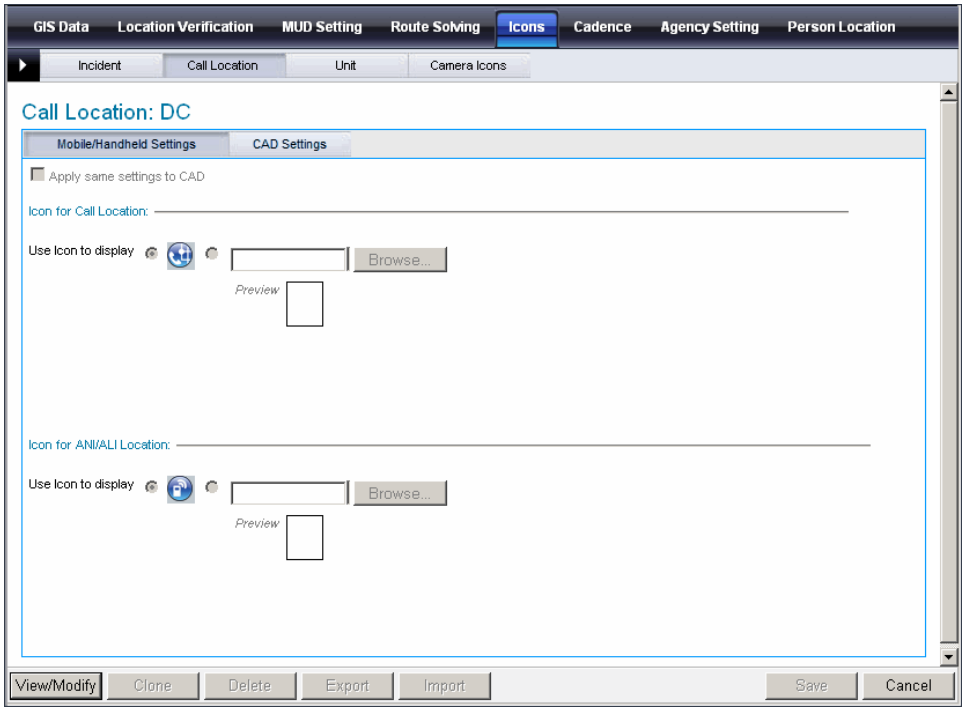


Figure 25-15 Icons – Call Location Tab

3. Click **View/Modify**.
4. Select whether you want to use the same settings for CAD.
5. To change or add an icon for any of the call types:

   a. In the appropriate Use Icon to display field, click the second option, and then click **Browse**.

   b. Navigate to the location where your new icon is located, and click **OK**.

      Your selected icon appears in the preview area and the path shows in the display text field between the option and the **Browse** button.

6. Repeat the operation for each call type if necessary.

7. Click **Save**.

Adding and Modifying Unit Icons

Add or modify unit icons when you need a new or different unit icon to display on your maps. The icon is applied to the display of all unit icons.

NOTE

Labels for icons on the CAD and Mobile maps use the colors as defined for status monitors.

To add or modify unit icons:

1. Access the Icons form. For details, see "Configuring Incident and Unit Icons" on page 25-16.

   The Icons form appears with the Incident tab in focus (see Figure 25-13).

2. Select the Unit tab.

   The Mobile/Handheld Settings tab appears.

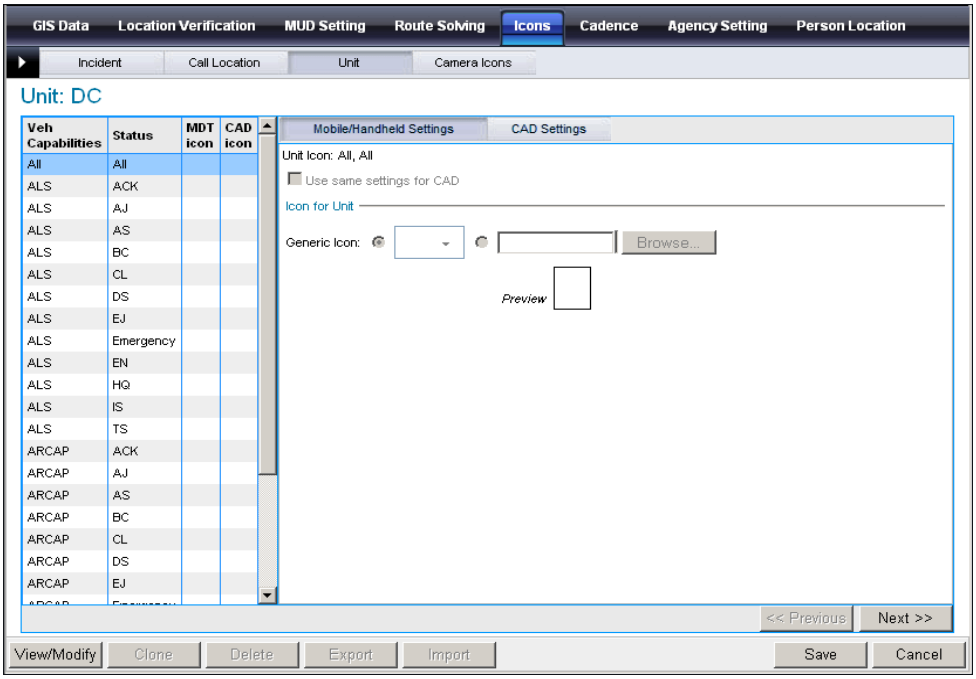


Figure 25-16 Icons Unit Tab

3. From the Vehicle Capabilities table, select the vehicle capability and status combination with the icon you want to modify.

4. Click **View/Modify**.
5. To apply the changes to CAD, select the **Use same settings for CAD** check box.
6. To change or add an icon, complete one of the following:
   a. Select the **Generic Icon** option and then select one of the system-provided icons.
   b. Select the option to use your own icon. To use your own icon, click the **Browse** button, navigate to the location where your new icon is located, and then click **OK**.

      Your selected icon appears in the preview area and the path shows between the option and the Browse button.
7. To make change the settings for CAD, click the CAD Setting tab.
8. To apply the changes to CAD, select the **Use same settings for MDT/Handheld** check box.
9. To change or add an icon, follow the step 6.
10. Click **Save**.

Adding and Modifying Camera Icons

Add or modify camera icons when you need a new or different camera icon to display on your maps. The icons are applied to camera locations by camera type.

From the map window, users can show or hide the location of cameras, and request a status update of one or more cameras if this feature is available from the third-party application. If available, a third-party application can be configured to provide feeds from the camera.

To add or modify camera icons:

1. Access the Icons form. For details, see “Configuring Incident and Unit Icons” on page 25-16.

   The Icons form appears with the Incident tab in focus (see Figure 25-13).

2. Select the Camera Icons tab.

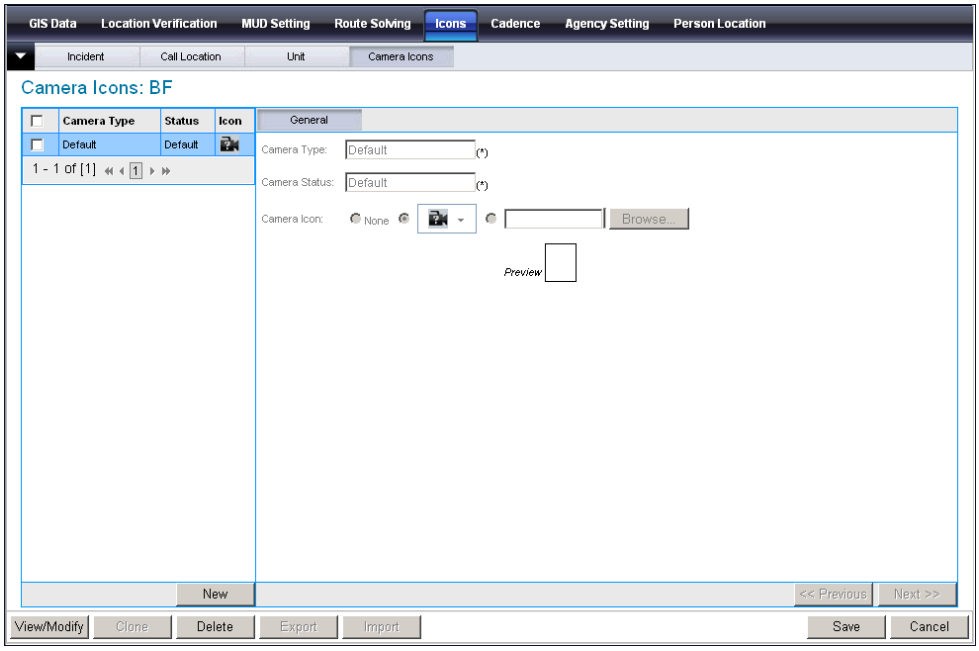


Figure 25-17 Icons – Camera Icons Tab

3. Click **New** to add a new icon, or **View/Modify** to change an icon.

4. Type the camera type, the camera status, and select the icon to use. You can choose an icon from the list, or browse for an icon.

5. Click **Save**.

Configuring GPS Cadence

Use the Cadence configuration item to set the cadence value for GPS-equipped vehicles. Cadence is the rate at which the GPS for a GPS-equipped unit reports its location. You can change the minimum and maximum reporting times, and the maximum reporting distance for your agency, for units, and for vehicle types.

Modify cadence when you need to change minimum reporting time, maximum reporting time, and maximum distance traveled; minimum reporting time, maximum reporting time, and maximum distance traveled for individual units; and minimum reporting time, maximum reporting time, and maximum distance traveled for individual vehicle types in specific statuses.

To configure cadence:

1. From the navigation panel, select **Mapping**, and then select **Cadence**.

   The Cadence form appears.

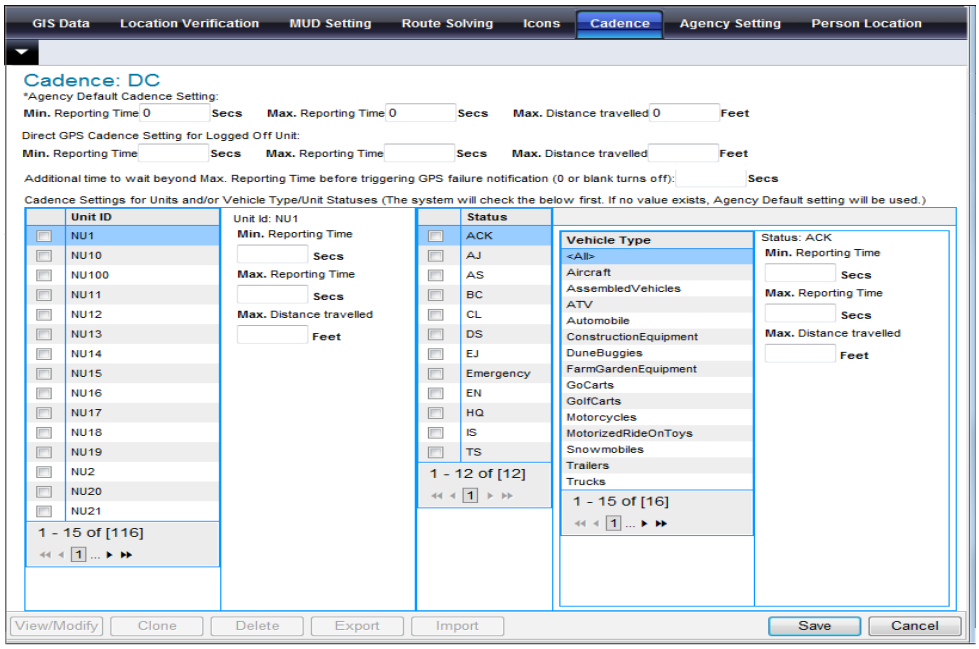


   Figure 25-18 Mapping – Cadence Form

2. Click **View/Modify**.

3. Do the following to set the default cadence for your agency:

   - To enter cadence time values:

     In the Min. Reporting Time field, enter the minimum time in which a vehicle is scheduled to report its location.

     In the Max. Reporting Time field, enter the maximum time in which a vehicle is scheduled to report its location.

> **NOTE**
> The MUPS (Motorola Universal Processing Server) is used with ASTRO radios and only uses the Max Reporting Time, not the minimum.

   - To enter cadence distance values:

     In the Max. Distance Traveled list, enter the maximum distance the vehicle can travel before reporting its location.

   Both cadence values are used.

   You can also set the values for a unit ID or for a type of vehicle in a specific status.

4. If your agency uses Direct gps Reporting, repeat the previous step for the **Direct GPS Cadence Setting for Logged Off Unit**.

   Direct GPS reporting allows GPS devices in Mobile to directly communicate with the PremierOne ARL (Automatic Resource Location) Service.

   You must also enable the **Trimble Direct feature**. For details, see "Configuring GPS Devices" on page 11-64.

5. To send GPS failure notifications when a unit's GPS device stops reporting its location, enter a value in the **Additional time to wait beyond Max Reporting Time before triggering GPS failure notification** field (0 or blank disables notifications).

   Notifications are sent to the CAD client as a Priority notification.

6. Click **Save**.

Configuring Mapping Agency Settings

The Agency Setting configuration contains the following tabs for CAD and Mobile:

- General Settings – Where you set whether to display associated units on the CAD mapping client, whether icons cascade, the information incident and unit information that displays on the map, and the number of digits of the incident number to display on the map.
- Map Zoom Behavior – Where you set whether the CAD map display should center upon a location associated with the specified command and the scale to which the map display should zoom when centering on the location, and where you set the scale for the map when the user selects the Map It button for a location.
- Mouse Hover Display – Where you provision the information that displays when CAD and Mobile users hover over an icon on the map.
- Non-GPS Equipped Units – Where you set whether a unit icon of non-GPS units displays on the map. The choices are always, when assigned to an incident, and never.

Adding and Modifying General Settings – CAD

Use the Agency Setting – General Settings CAD form to set whether to display labels for associated units on the CAD mapping client (associated units are those units assigned to associated incidents), the incident fields that display, unit fields that display, and the number of digits of the incident number to display.

This form also control the labels shown on the map when a 9-1-1 call displays.

To add or modify general CAD settings:

1. From the navigation panel, select **Mapping**.
2. Select **Agency Setting**, and then select **General Settings**.

   The Agency Settings window appears.

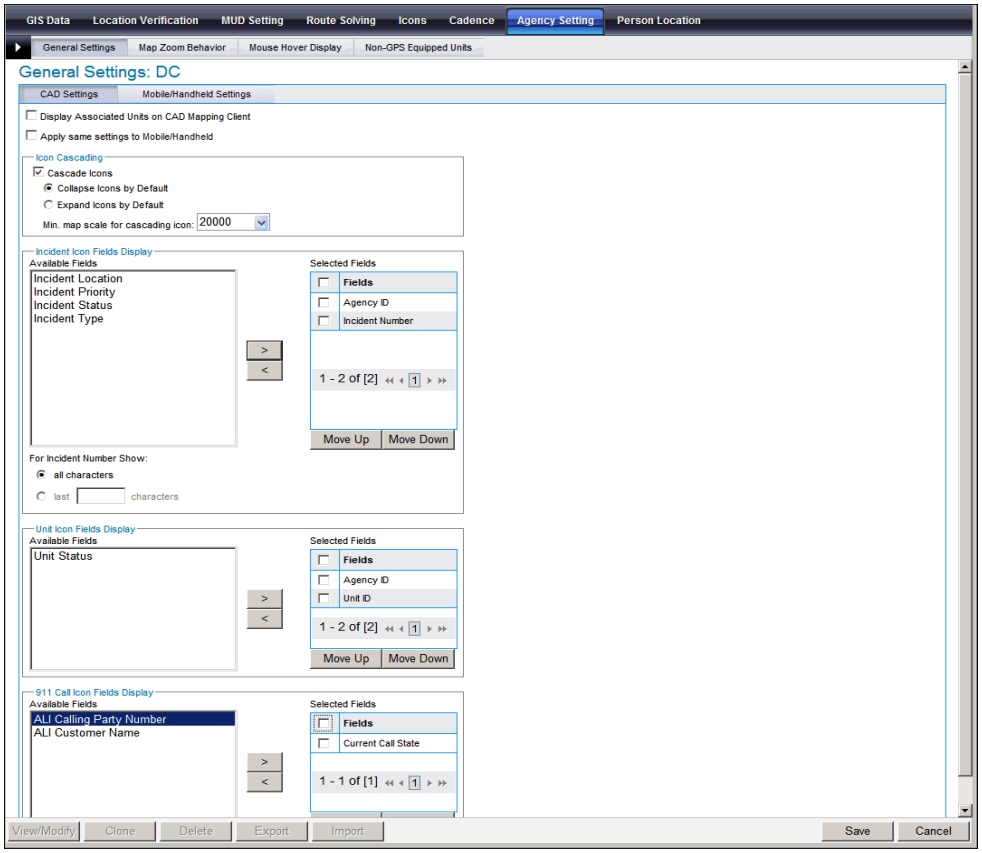


Figure 25-19 Agency Settings – General Settings Form for CAD

3. Click **View/Modify**.
4. To display associated units on the map, click the **Display Associated Units on CAD Mapping Client** check box.

   In this case, the ID of the primary unit for any associated incidents will display under the incident label.

5. To apply the CAD settings to Mobile/Handheld, click the **Apply same settings to Mobile/Handheld** check box.

6. In the Icon Cascading section, select whether you want cascaded icons to be expanded or collapsed by default.

7. In the Min. map scale for cascading icon field, select the minimum scale size when cascading icons will display on the map.

8. In the Incident Icon Fields Display section, select the incident fields that you want to display on the map and add them to the Selected Fields list.

   You can order the fields by selecting the field and then clicking the Move Up and Move Down buttons.

9. Select one of the following for the For Incident Number Show option:

   - To display all characters in the incident number on the map, select the **All Characters** button.

   - To only display a set number of characters, select the **Last** button and enter the number of characters to display (up to eight).

10. In the Unit Icon Fields Display section, select the unit fields that you want to display on the map and add them to the Selected Fields list.

    You can order the fields by selecting the field and then clicking the Move Up and Move Down buttons.

11. In the 911 Call Icon Fields Display section, select the 9-1-1 information labels that you want to display on the map and add them to the Selected Fields list.

    You can order the fields by selecting the field and then clicking the Move Up and Move Down buttons.

12. Click the Mobile/Handheld Settings tab.

13. To apply the Mobile/Handheld settings to CAD, click the **Apply same settings to CAD** check box.

14. Repeat this procedure for any Mobile/Handheld settings.

15. Click **Save**.

Adding and Modifying General Settings – Mobile/Handheld

Use the Agency Setting – General Settings Mobile/Handheld form to set the incident fields that display, the unit fields that display, and the number of digits in the incident number to display on the mobile map.

NOTE
This feature is not yet enabled in the Mobile client.

To add or modify general Mobile/Handheld settings:

1. From the navigation panel, select **Mapping**.
2. Select **Agency Setting**, and then select **General Settings**.

   The General Settings window appears.
3. Click **View/Modify**.
4. Select the Mobile/Handheld Settings tab.

   The Mobile/Handheld Settings window appears.

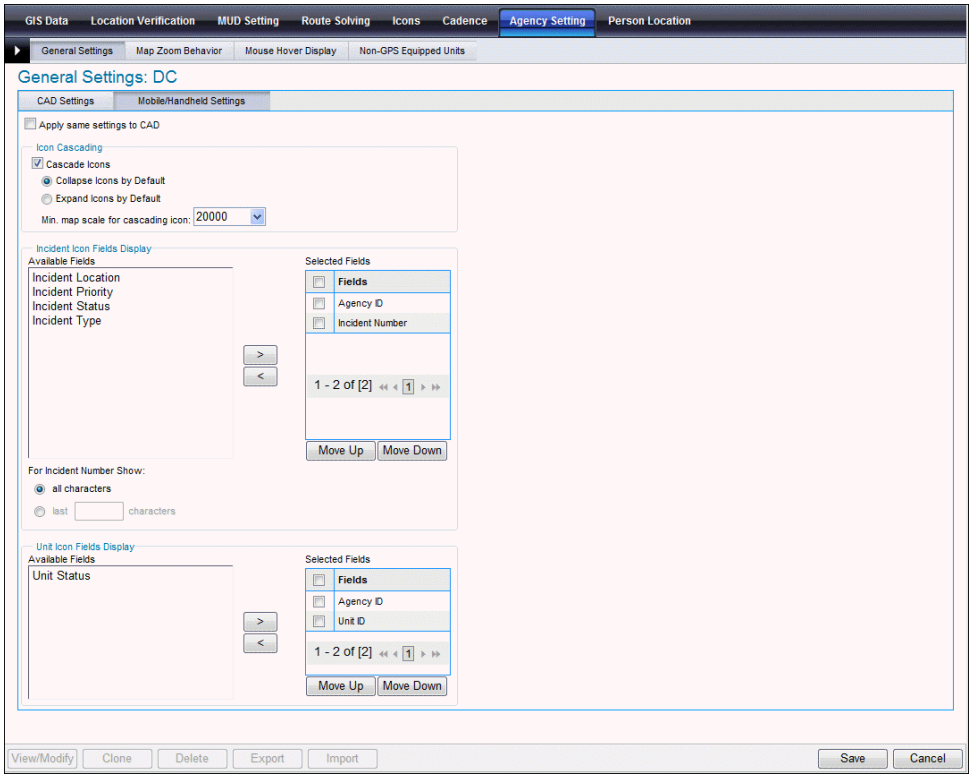


Figure 25-20 Agency Settings – General Settings Form For Mobile

5. To apply the Mobile/Handheld settings to CAD, click the **Apply same settings to CAD** check box.

6. In the Icon Cascading section, select whether you want cascaded icons to be expanded or collapsed by default.

7. In the Min. map scale for cascading icon field, select the minimum scale size when cascading will display on the map.

8. In the Incident Icon Fields Display section, select the incident fields that you want to display on the map and add them to the Selected Fields list.

   You can order the fields by selecting the field and then clicking the Move Up and Move Down buttons.

9. Select one of the following for the For Incident Number Show option:

   - To display all characters in the incident number on the map, select the **All Characters** button.

   - To only display a set number of characters, select the **last _ characters** button and enter the number of characters to display (up to eight).

10. In the Unit Icon Fields Display section, select the unit fields that you want to display on the map and add them to the Selected Fields list.

    You can order the fields by selecting the field and then clicking the Move Up and Move Down buttons.

11. Click **Save**.

Setting CAD Map Zoom Behavior

Use the Agency Setting–Map Zoom Behavior form to indicate whether the CAD map display should center upon the location associated with the specified command, the scale to which the map display should zoom when centering on the location, and the scale to use on the map when the user selects the Map It button from the CAD client.

To control the map zoom behavior:

1. From the navigation panel, select **Mapping**.

2. Select **Agency Setting**, and then select **Map/Zoom Behavior**.

   The General Settings window appears.

The Agency Settings – Map Zoom Behavior form appears.

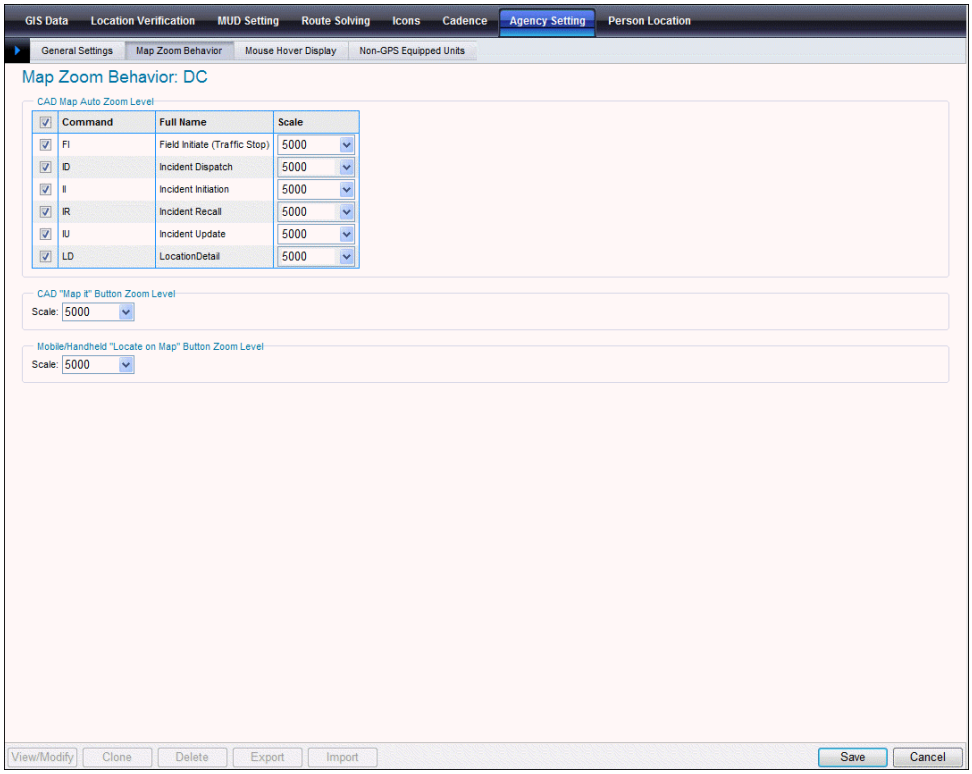


Figure 25-21 Agency Settings – Map Zoom Behavior Form

3. Click **View/Modify**.

4. To cause the map to automatically zoom to the location involved with a command, select the check box to the left of that command. To select all available commands, click the check box at the top of the column next to the word “Command.”

5. To set the scale to which the map display zooms when centering on the location specified in the previous step, select a scale from Scale list for the specified command.

6. From the CAD “Map it” Button Zoom Level list, select the scale to use in displaying locations when the user selects the **Map It** button for a selected location on a CAD map.

7. From the Mobile “Locate on Map” Button Zoom Level list, select the scale to use in displaying locations when the user selects the **Map It** button for a selected location on a Mobile map.

8. Click **Save**.

Setting the Mouse Hover Display

Use the Agency Setting–Mouse Hover Display form to provision the information that displays when CAD and Mobile/Handheld users hover over an icon on the map. When you set the mouse hover display, you enter information on two tabs of the Agency Setting–Mouse Hover Display form:

- CAD Settings – Where you provision the information to display when hovering over an incident icon or a unit icon on a CAD user's map.
- Mobile/Handheld Settings – Where you provision the information to display when hovering over an incident icon or a unit icon on a Mobile user's map.

Note that the fields on both tabs are identical. The Incident Icon Mouse Hover fields are the same set of fields that may be provisioned in the Incident status monitor for incidents. The Unit Icon Mouse Hover fields are the same set of fields that may be provisioned in the Unit status monitor for units.

To set the mouse hover display for CAD or for Mobile/Handheld:

1. Access the form for **Agency Setting.**

   For details, see "Adding and Modifying General Settings – CAD" on page 25-25,

2. Select **Mouse Hover Display**.

The Agency Setting-Mouse Hover Display form appears with the CAD Settings tab in focus.

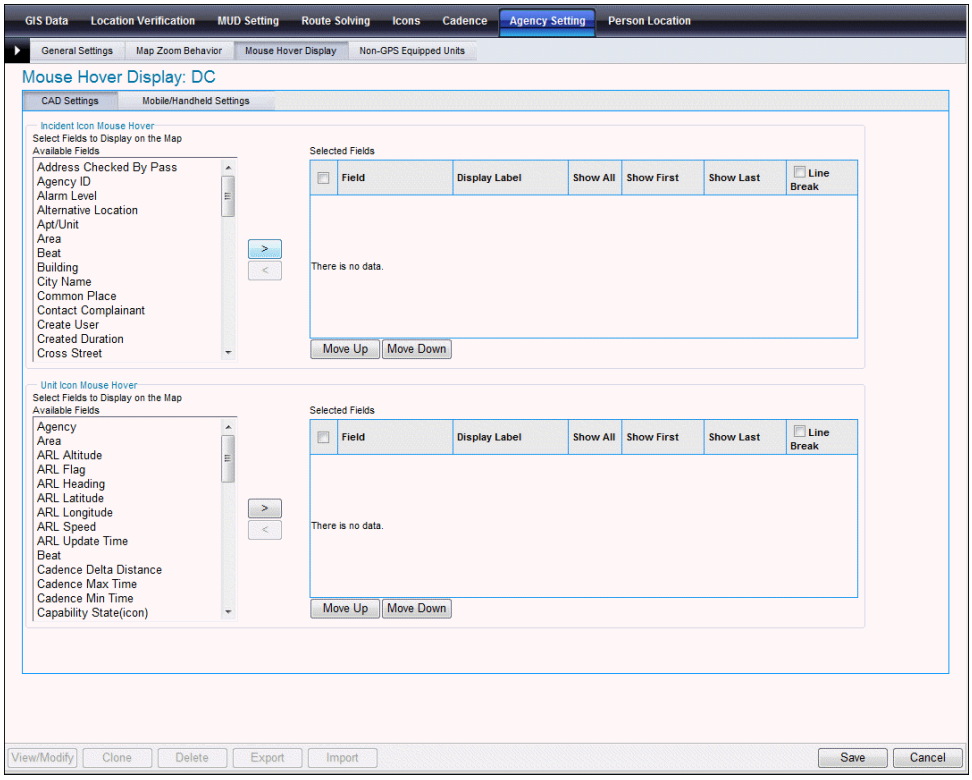


Figure 25-22 Agency Setting – Mouse Hover Display – CAD Settings Tab

3. In the Incident Icon Mouse Hover section, select the fields to display on the map when a user hovers over an incident icon.

   a. From the Available Fields box, select all fields you want to display when the user hovers over the incident icon, and then click the right arrow.

      Your choices appear in the Selected Fields box.

   b. To change the order of the display, select a field by clicking the check box next to the field name, and the click the **Move Up** and **Move Down** buttons until the field is where you want it to display.

   c. To optionally define a display label that precedes the data being displayed, select the field.by clicking on it. You do not have to select the check box. In the Display Label field that appears, type the label you want to appear before the data when the user hovers over the incident icon.

   d. To show all of the data in a field, ensure that the button in the Show All column is selected. This field is selected by default.

   e. To show only some number of leading characters of the field, select the button in the Show First column, and then in the field that appears indicate how many characters to show.

f. To show only some number of trailing characters of the field, select the button in the Show Last column, and then in the field that appears indicate how many characters to show.

g. To cause a line break to occur after the field information (rather than the information for the next field starting on the same line), select the check box in the Line Break column.

4. In the Unit Icon Mouse Hover section, start at step 3 on page 25-31 and repeat the steps to select the fields to display on the map when a user hovers over a Unit icon.

5. In the 911 Call Icon Mouse Hover section, start at step 3 on page 25-31 and repeat the steps to select the fields to display on the map when a user hovers over a 9-1-1 Call icon.

6. Click **Save**.

7. Select the Mobile/Handheld Settings tab and repeat this procedure.

Configuring Non-GPS Equipped Units Display

Use Agency Setting– Non-GPS Equipped Units form to provision the default setting for when non-GPS equipped units are displayed on the CAD and Mobile map. Individual users can manually override the setting.

To configure the non-GPS equipped units display:

1. Access the form for **Agency Setting.**

   For details, see “Adding and Modifying General Settings – CAD” on page 25-25.

2. Select **Non-GPS Equipped Units Display**.

   The Non-GPS Equipped Units Display form appears.

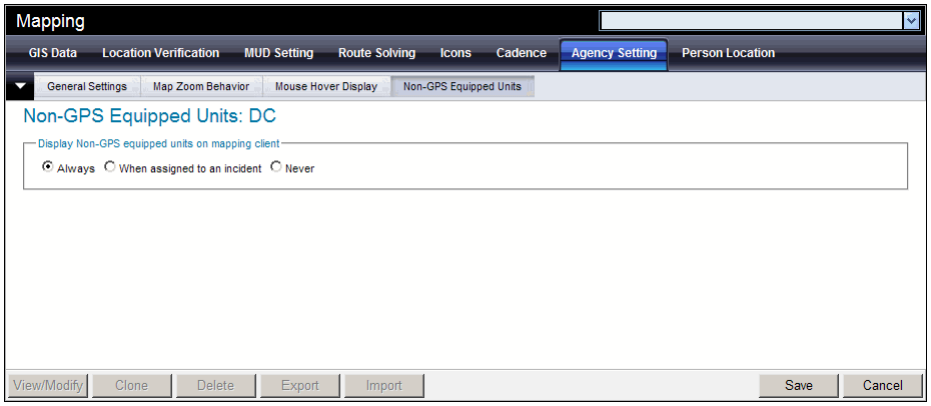


Figure 25-23 Agency Setting – Non-GPS Equipped Units Form

3. Select one the choices, and then click **Save**.

Configuring Person Location

The person location of each first responder can be displayed on the PremierOne CAD and Mobile maps. To accomplish this, the system displays the person location using the GPS location provided by the person's portable radio when the person is out of the vehicle. The Person Location icons display when the person is determined to be out of the vehicle.

Out of vehicle status is determined by the following:

- Unit status – The Out-of-Vehicle condition can be set for each unit status type, which automatically displays the Person Location icon on the map.
- Out of Vehicle Status – The Out of Vehicle status button on the Mobile client sets the status to display the Person Location icon on the map. The status is manually selected by the person in the Mobile unit. This only overrides an "In vehicle" condition to make it "Out of vehicle", not vice versa.
- Emergency status – The unit status is set to Out-of-Vehicle when the Emergency button is selected in the Mobile client or radio. This status can also be set by the dispatcher on the CAD client. This automatically displays the Person Location icon on the map.

The Agency Setting configuration contains the following tabs for CAD and Mobile:

- Icon Display – Where you set the criteria for displaying an out of vehicle condition. You can choose options here to determine when the person icon displays on the map.
- Person Icon – Where you set the text information that displays on the person icon on the map.
- Icon Hover – Where you provision the information that displays when a CAD or Mobile user hovers the mouse over a person icon on the map.
- Person Location Cadence – Where you set the minimum and maximum time, or maximum distance for refreshing a person location.

Setting When Person Location Icons Display

Use the Person Location–Icon Display form to provision when the person location icon displays on the CAD and Mobile/Handheld map. An “Out of vehicle” condition is the minimum requirement to display a Person icon on the map.

To set when the person location icon displays:

1. From the navigation panel, select **Mapping**, then select **Person Location**, and then select **Icon Display**.

   The Icon Display form appears.

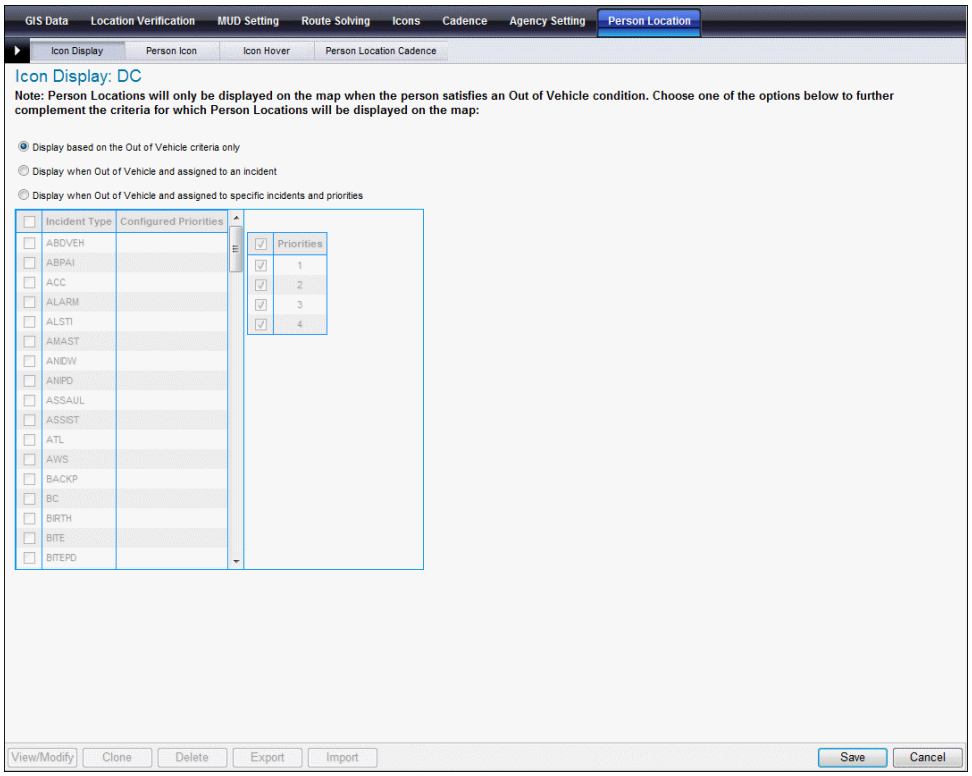


Figure 25-24 Person Location Icon Display Form

2. Select **View/Modify**.

3. Do one of the following:

   - **Display based on the Out of Vehicle criteria only** – The icon displays when the person is out of the vehicle. Out-of-vehicle status is determined by the unit status.

   - **Display when Out of Vehicle and assigned to an incident** – The icon displays when the person is out of the vehicle when any incident is assigned.

- **Display when Out of Vehicle and assigned to specific incidents** – The icon displays when the person is out of the vehicle for selected incident types. To configure specific incident types with different priorities, you have to select an incident type and priority, and then click **Save**. This must be done for each incident type.

4. Click **Save**.

Setting the Person Icon Display Information

Use the Person Location–Person Icon Display form to provision the person icon and icon labels that display on the map. Person location icons only display on the map when the status for the person is `Out of Vehicle`.

To set the person icon display information:

1. From the navigation panel, select **Mapping**, then select **Person Location**, and then select **Icon Display**.

   The Person Location form appears with the Icon Display tab in focus.

2. Select the Person Icon tab.

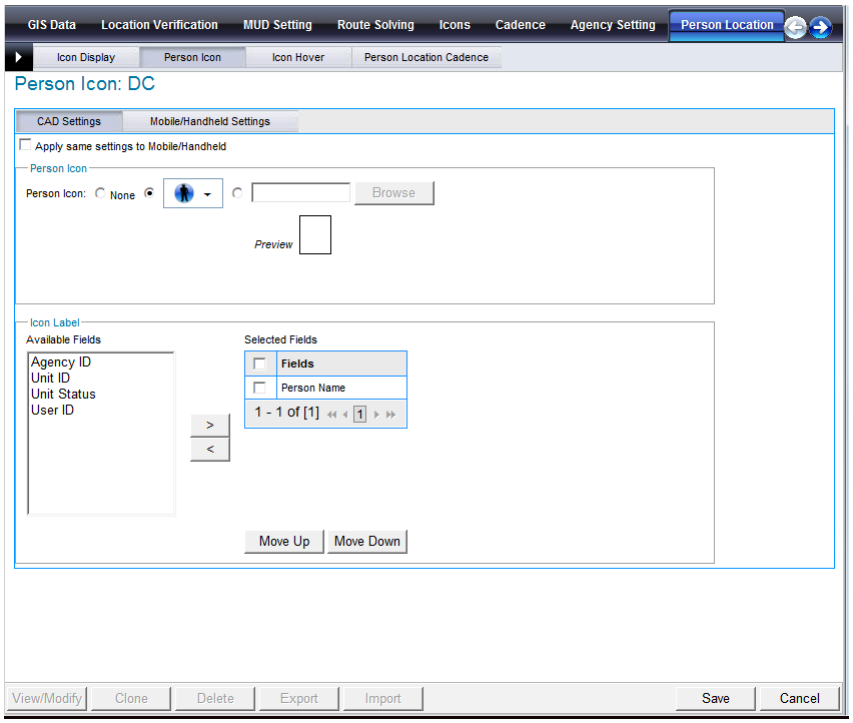


Figure 25-25 Person Location Icon Form

3. Select **View/Modify**.

4. To apply all the CAD settings to Mobile/Handheld, click the **Apply same settings to Mobile/Handheld** check box.

5. To add the icon, do one of the following:

   - Click the button to the right of None, and then select the icon you want to use.
   - Click the **Browse** button and navigate to the location of the new icon and click **OK**. Your selected icon appears in the Preview box.

6. Set the icon label:

   a. From the Available Fields box, select the fields you want to display as the icon label, and then click the right arrow.

      Your choices appear in the Selected Fields box.

   b. To change the order of the display, select a field by clicking the check box next to the field name, and the click the **Move Up** and **Move Down** buttons until the field is where you want it to display.

7. To use different settings for Mobile/Handheld, select the Mobile/Handheld Settings tab, make sure the **Use same setting for CAD** check box is clear, and repeat this procedure.

8. Click **Save**.

Setting the Mouse Hover Display Information

Use the Person Location–Icon Hover form to provision the information that displays when CAD and Mobile users hover the mouse over the Person icon on the map.

To set the mouse over display information:

1. From the navigation panel, select **Mapping**, then select **Person Location**, and then select **Icon Hover**.

2. Select the Icon Hover tab.

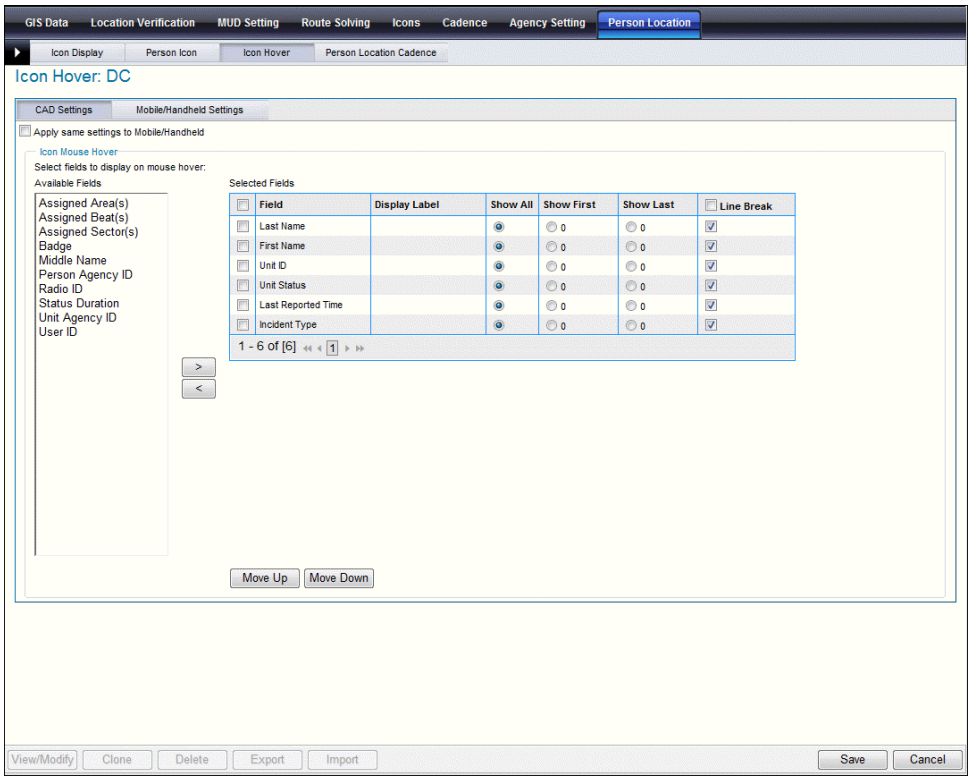


Figure 25-26 Person Location Hover Form

3. Select **View/Modify**.

   a. To apply all the CAD settings to Mobile/Handheld, click the **Apply same settings to Mobile/Handheld** check box.

   b. From the Available Fields box, select all fields you want to display when the user hovers over the Person icon, and then click the right arrow.

      Your choices appear in the Selected Fields box.

   c. To change the order of the display, select a field by clicking the check box next to the field name, and the click the **Move Up** and **Move Down** buttons until the field is where you want it to display.

d. To optionally define a display label that precedes the data being displayed, select the field by clicking on it. You do not have to select the check box. In the Display Label field that appears, type the label you want to appear before the data when the user hovers the mouse over the incident icon.

e. To show all of the data in a field, ensure that the button in the Show All column is selected. This field is selected by default.

f. To show only some number of leading characters of the field, select the button in the Show First column, and then in the field that appears indicate how many characters to show.

g. To show only some number of trailing characters of the field, select the button in the Show Last column, and then in the field that appears indicate how many characters to show.

h. To add line breaks after a field, select the **Line Break** check box for a field.

i. If you want different settings for Mobile/Handheld, click the Mobile/Handheld Settings tab and repeat the previous steps.

4. Click **Save**.

Setting Person Location Cadence

Use the Person Location Cadence configuration item to set the cadence value for GPS-equipped persons (portable radio or handheld device). Cadence is the rate at which the GPS reports it's location.

NOTE

A mixed deployment of Handhelds and Radios for Person Location is not supported at this time. The Person Location Cadence is used for either Handheld devices or for Radios.

Cadence can be set for each unit status based on reporting time and maximum distance traveled for each unit status. Cadence can be used to configure closer tracking for more critical situations, such as a pursuit, and less or no tracking when it is not necessary.

MUPS (Motorola Universal Processing Server) collects radio unit location reports for ASTRO 25 subscriber units that have GPS.

For radios, cadence settings are validated as follows:

- Values of both Min. Reporting Time and Max. reporting Time are validated to ensure that they either exceed or are equal to the minimum limit "MinReportingTime" specified in the ARL configuration file.
- The Max Distance traveled value is validated to ensure that it either exceeds or is equal to the "Address\InstanceName" value specified in the ARL configuration file.

When the Handheld Agency check box is selected, the radio system restrictions within the ARL configuration file are not enforced as defined above.

To set the person location cadence:

1. From the navigation panel, select **Mapping**, then select **Person Location**, and then select **Person Location Cadence**.

   The Person Location Cadence form appears.

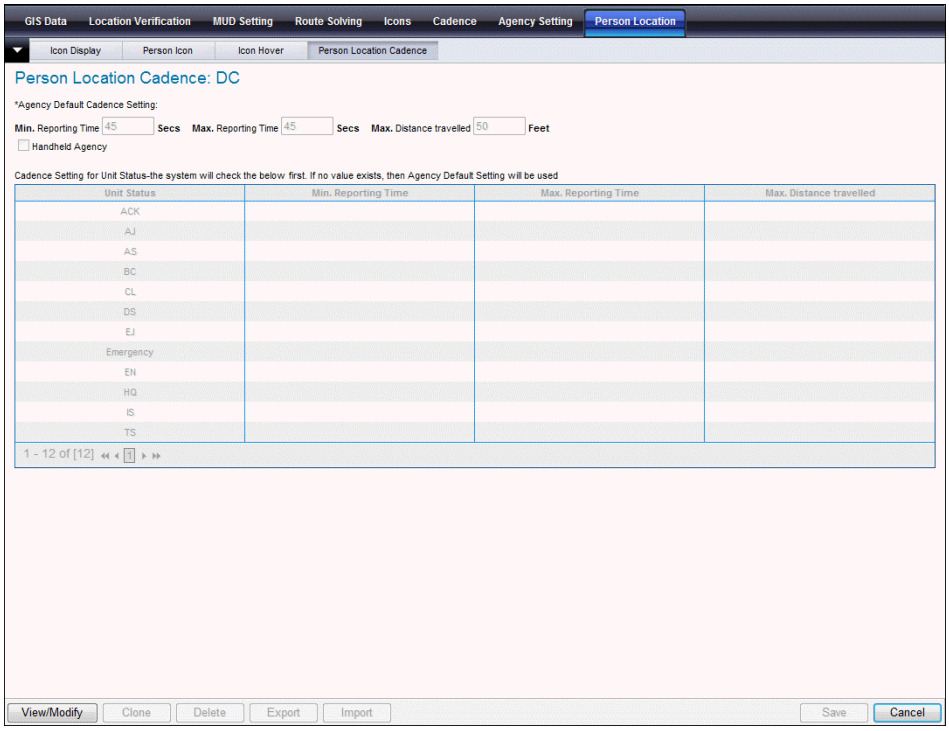


Figure 25-27 Person Location Cadence Form

2. Repeat the following process for each unit status.

   a. In the Unit Status field, select a unit status.

   b. To apply cadence settings to the Handheld agency, select **Handheld Agency**.

> **NOTE**
> If you clear the Handheld Agency check box after selecting it, all cadence values that are lower than the MUPS lower limit are set equal to that lower limit.

   c. In the Min and Max Reporting time fields, enter the time in seconds that you want to elapse before the person location is refreshed.

MUPS only accepts one time value, so the minimum time value is not used here. MUPS and PremierOne should have the same value.

NOTE

The MUPS (Motorola Universal Processing Server) is used with ASTRO radios and only uses the Max Reporting Time, not the minimum.

d. In the Max distance travelled field, enter the maximum amount in feet that a person can move from the last reported position before the person location is refreshed.

MUPS reports cadence on both time and distance intervals regardless which one is satisfied first.

If you are using MUPS (Motorola Universal Process Server), the minimum and maximum values must be the same as in MUPs `APIconfig.xml` file (`C:\Program Files\Motorola\Mups`). Set these values in the `Mups\MUPs_config.xml` file (from the **PremierOne Portal**, select **Configuration**).

3. Click **Save**.

Configuring ARL History Playback Defaults

Use the ARL configuration item to set the maximum time period value and the maximum number of units that a user can specify when performing an ARL playback request. You can also set whether the search results are compressed to help system performance.

There are three items that can be configured to minimize impact on the system performance while searching ARL history. These items are located in the ARL node of the configuration file.

- `ARLHistorySearchMaxTimePeriod` – controls the maximum time in hours that can be used in a ARL history search. The maximum allowable time is 12 hours. The default is 12 hours.
- `ARLHistorySearchMaxUnitNumber` – controls the maximum number of units that can be used in a ARL history search. The maximum allowable value is 10. The default is 5.
- `ARLHistorySearchIsCompressed` – determines if the search results are compressed or not. The default is compressed (true).

Configuring Railroad and Bridge Gate Status

The gate status of railroads crossings and bridges can be displayed on the PremierOne CAD map using icons on a map layer. The icons are controlled by status messages sent by the gate server to the AVL server which sends the information to PremierOne CAD to display the correct gate status icon on the map. Gate location is not pre-defined in Provisioning; a gate icon is displayed when a status message is received for it.

Icons are a only a **visual indicator** of gate status and have **no effect** on the shortest path route solving or AVL-based "Estimated Time of Arrival" calculations of PremierOne. Gate status is not available on Mobile maps.

Table 25-1 Gate Status Icons

Icon	Status
	Vehicle travel is not impeded
	Vehicle travel is impeded
	Status unknown

There are no direct settings in Provisioning for gate icon display on the Map, but setting timeout values is documented here because it affects the map display.

The `GateStatusTimeout` values determines how long before a gate status changes to the "Unknown" state if no status updates are received. The value controls how long the Travel is not Impeded or Travel is Impeded icons display (when there is no status change activity), before the Unknown Status icon displays.

The `GateOutOfServiceTimeout` value determines how long before the gate icons are removed from the map because there is no status change activity.

Both values are configured in minutes. Set this value in the System Management tool portal in the RoadClosure node.

To set the gate timeout value:

1. Open the System Management Tool portal.
2. Click the Configuration icon.
3. Select the **Edit** tab.

4. Select the **Roadclosure** node.

   The RoadClosure XML file appears.

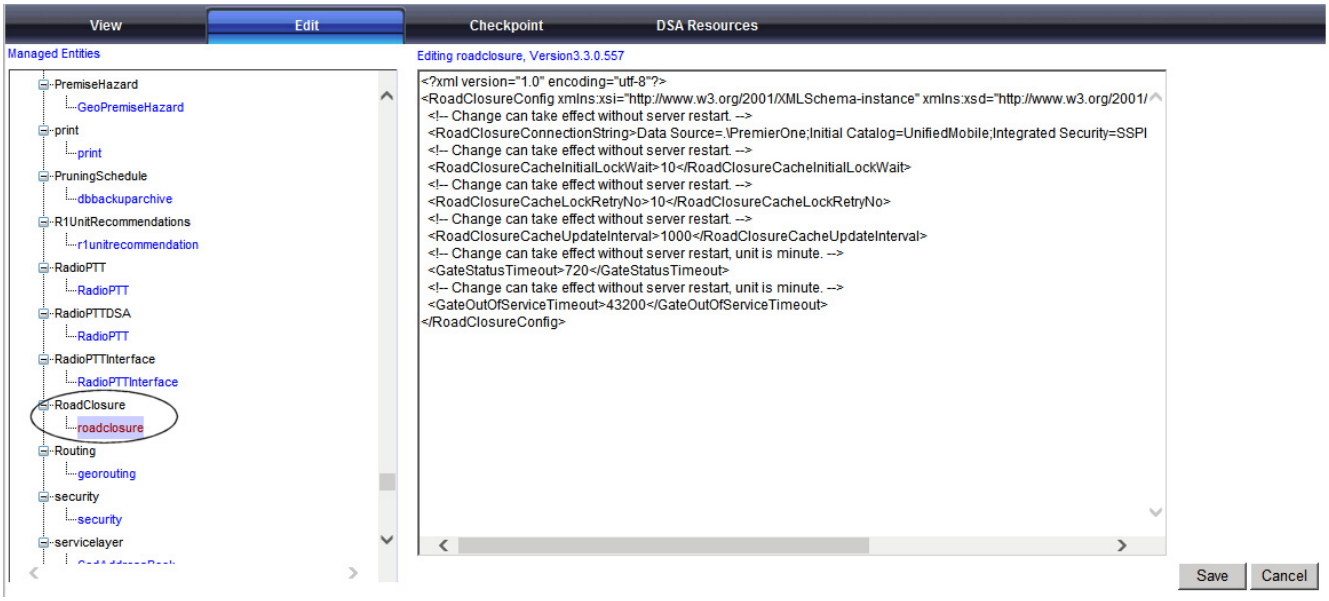


Figure 25-28 RoadClosure Node XML

5. For the `GateStatusTimeout` value, enter the amount of time (in minutes) that you want to wait (with no gate status change) before the gate status times out. Timeout is the amount of time before the status changes to `Unknown Status`.

> **NOTE**
> If you set the time to 0, the status stays in the present state until a new status message is received.

6. For the `GateOutOfServiceTimeout` value, enter the amount of time (in minutes) that you want to wait (with no gate status change) before the gate icon is removed from the PremierOne CAD map.

> **NOTE**
> If you set the time to 0, gate status icon will never be removed from the map.

7. Click **Save**.

CHAPTER 26

Configuring Messaging

The Messaging configuration item contains the following items:

- Agency Settings – Where you configure general, Mobile, CAD, Smart Client, and Handheld settings for email messages. The Smart Client is a separate application used for text messaging with ASTRO radios. For details, see “Configuring Agency Messaging Settings” on page 26-1.
- Message Types – Where you set general, Mobile, CAD, Smart Client, and Handheld settings for email, BOLO, notification messages, and query message types. For details, see “Configuring Message Types” on page 26-8.
- Folders – Where you set general mail folder settings, the download preview threshold, the procedure for when the folder is full, and the procedure for when the user logs off from either Mobile or CAD. For details, see “Configuring Message Folder Settings” on page 26-17.
- Alternative Routing – Where you configure alternative routing for messages when you need to route messages from one mail box to one or more other mail boxes. For details, see “Configuring Alternative Routing for Messages” on page 26-24.

Configuring Agency Messaging Settings

Use the Agency Settings configuration item to change general, Mobile, CAD, and Smart Client settings for email messages. Configuration settings are contained on the following tabs:

- General – Where you set items such as the prefix for replies and forwarded messages, whether to hold messages, settings for away messages, and general settings for personal folders and whether attachments are accepted.
- Mobile Settings – Where you configure messaging settings for Mobile units, such as when synchronization occurs, and limits on sent and received messages.
- CAD Settings – Where you configure messaging settings for CAD, such as when synchronization occurs, and limits on sent and received messages.

- Smart Client Settings – Where you configure messaging settings for the Smart Client, such as when synchronization occurs, and limits on sent and received messages.
- Handheld Settings – Where you configure messaging settings for Handheld devices, such as when synchronization occurs, and limits on sent and received messages.

Configuring General Agency Messaging Settings

Access the Agency Settings form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

To configure your agency settings:

1. From the navigation pane, select **Messaging**, and then select **Agency Settings**.

   The Agency Settings form appears.

2. Click **View/Modify**.

   The fields in the form become editable.

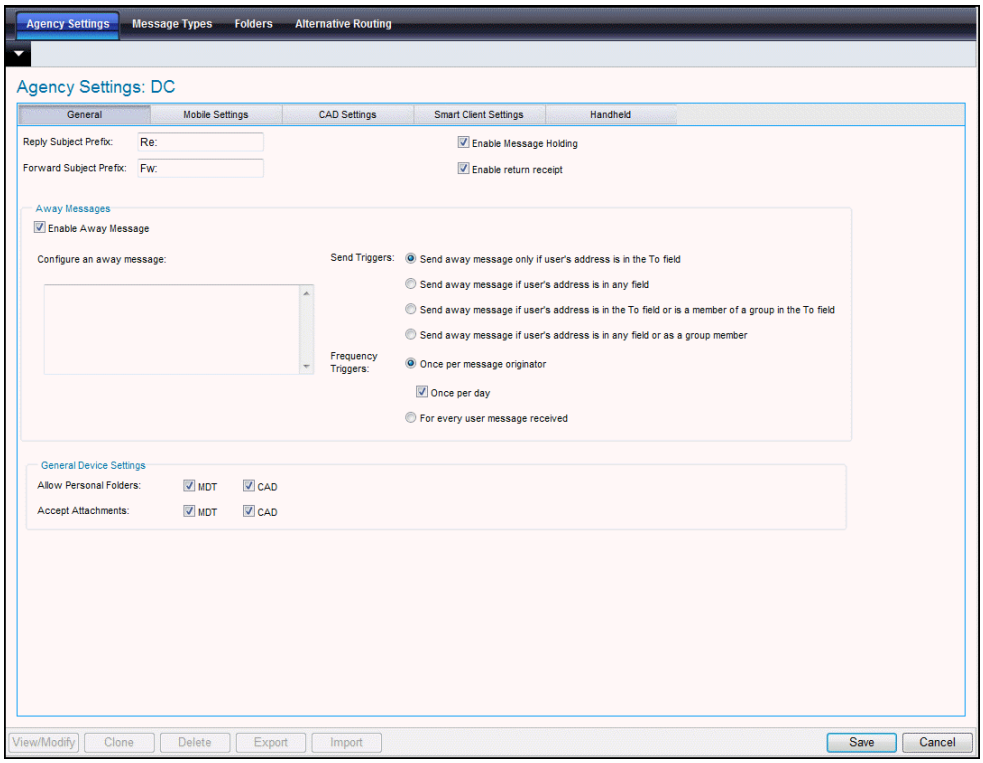


Figure 26-1 Messaging – Agency Settings Tab – General

3. In the Reply Subject Prefix field, enter a subject prefix for emails that are replied to, or accept the default of *Re:*.

4. In the Forward Subject Prefix field, enter a subject prefix for emails that are forwarded, or accept the default of *Fw:*.

5. To hold messages on the server while a user is away, select the **Enable Message Holding** check box.

6. To allow users to receive a notification message when a sent email is delivered, select the **Enable return receipt** check box.

7. In the Away Messages section, enable and configure auto-reply messages for when users are away.

   You can specify the text for the away message, the send triggers that will cause the message to be sent, and the frequency with which the message is sent.

8. In the General Device Settings section, specify for Mobile and CAD whether users can set up personal email folders and whether email attachments will be accepted.

9. Click **Save**.

Configuring Mobile Agency Messaging Settings

Use the Mobile Settings tab to schedule synchronization of central and local folders, and to specify maximum sizes for received and sent emails for Mobile users.

To configure Mobile agency messaging settings:

1. From the navigation pane, select **Messaging**, then **Agency Settings**, and then **Mobile Settings**.

   The Mobile Settings form appears.

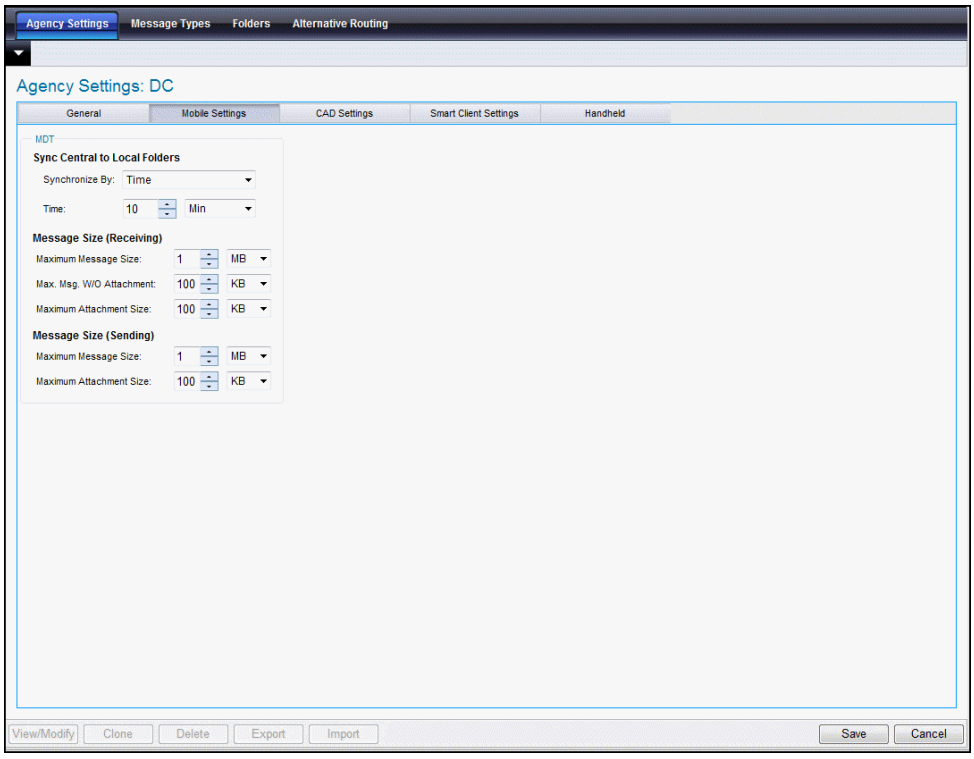


Figure 26-2 Messaging – Agency Settings Tab – Mobile Settings

2. In the Sync Central to Local Folders section, specify how local folders will be synchronized with the central server.

   Options are by time, manual action of the user, opening of the local folder, or with each successful login.

3. In the Message Size (Receiving) section, specify the maximum size for an incoming message, the maximum message size without an attachment, and the maximum attachment size.

4. In the Message Size (Sending) section, specify the maximum size for an outgoing message and the maximum attachment size.

5. Click **Save**.

Configuring CAD Agency Messaging Settings

Use the CAD settings tab to schedule synchronization of central and local folders, and to specify maximum sizes for received and sent emails for CAD users.

To modify CAD messaging settings:

1. From the navigation pane, select **Messaging**, then **Agency Settings**, and then **CAD Settings**.

   The CAD Settings form appears.

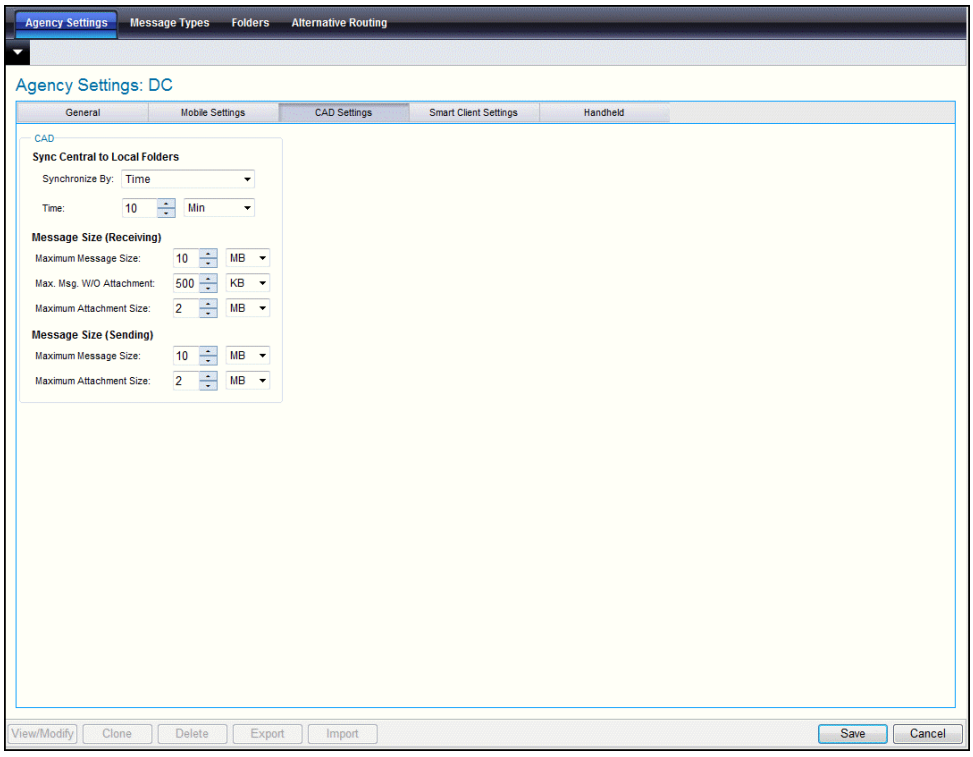


Figure 26-3 Messaging – Agency Settings Tab – CAD Settings

2. In the Sync Central to Local Folders section, specify how local folders will be synchronized with the central server. Options are by time, manual action of the user, opening of the local folder, or with each successful login.

3. In the Message Size (Receiving) section, specify the maximum size for an incoming message, the maximum message size without an attachment, and the maximum attachment size.

4. In the Message Size (Sending) section, specify the maximum size for an outgoing message and the maximum attachment size.

5. Click **Save**.

Configuring Smart Client Agency Messaging Settings

Use the Smart Client tab to schedule synchronization of central and local folders, and to specify maximum sizes for received and sent emails for Smart Client users.

To modify Smart Client agency messaging settings:

1. From the navigation pane, select **Messaging**, then **Agency Settings**, and then **Smart Client**.

   The Smart Client form appears.

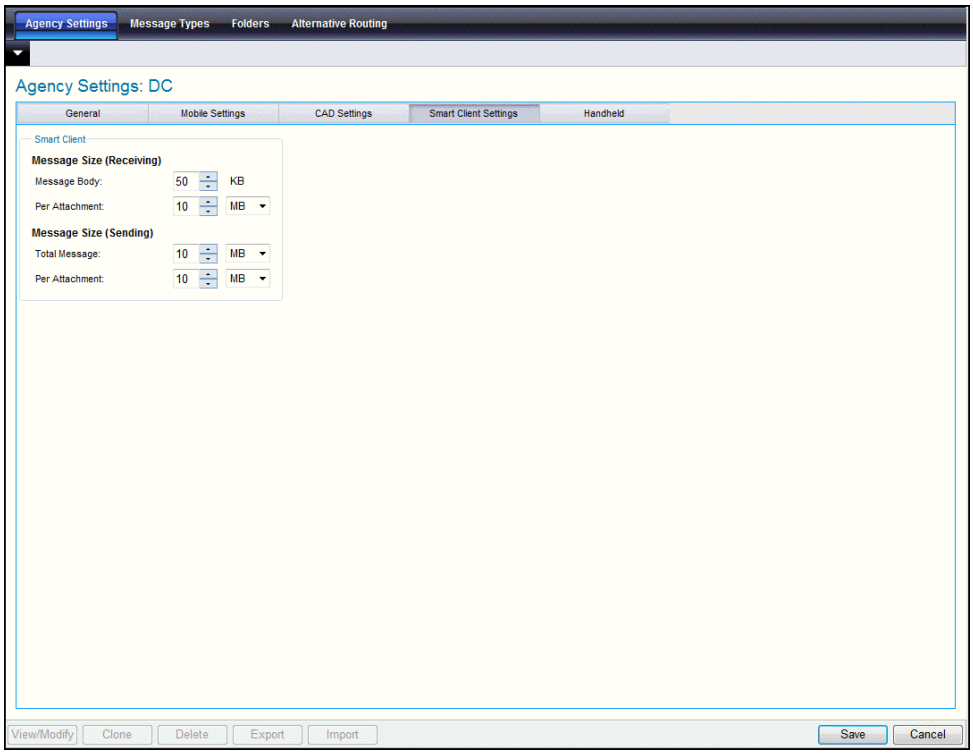


Figure 26-4 Messaging – Agency Settings Tab – Smart Client Settings

2. In the Sync Central to Local Folders section, specify how local folders will be synchronized with the central server. Options are by time, manual action of the user, opening of the local folder, or with each successful login.

3. In the Message Size (Receiving) section, specify the maximum size for an incoming message, the maximum message size without an attachment, and the maximum attachment size.

4. In the Message Size (Sending) section, specify the maximum size for an outgoing message and the maximum attachment size.

5. Click **Save**.

Configuring Handheld Agency Messaging Settings

Use the Smart Client tab to schedule synchronization of central and local folders, and to specify maximum sizes for received and sent emails for Smart Client users.

To modify Handheld agency messaging settings:

1. From the navigation pane, select **Messaging**, then **Agency Settings**, and then **Handheld**.

   The Handheld form appears.

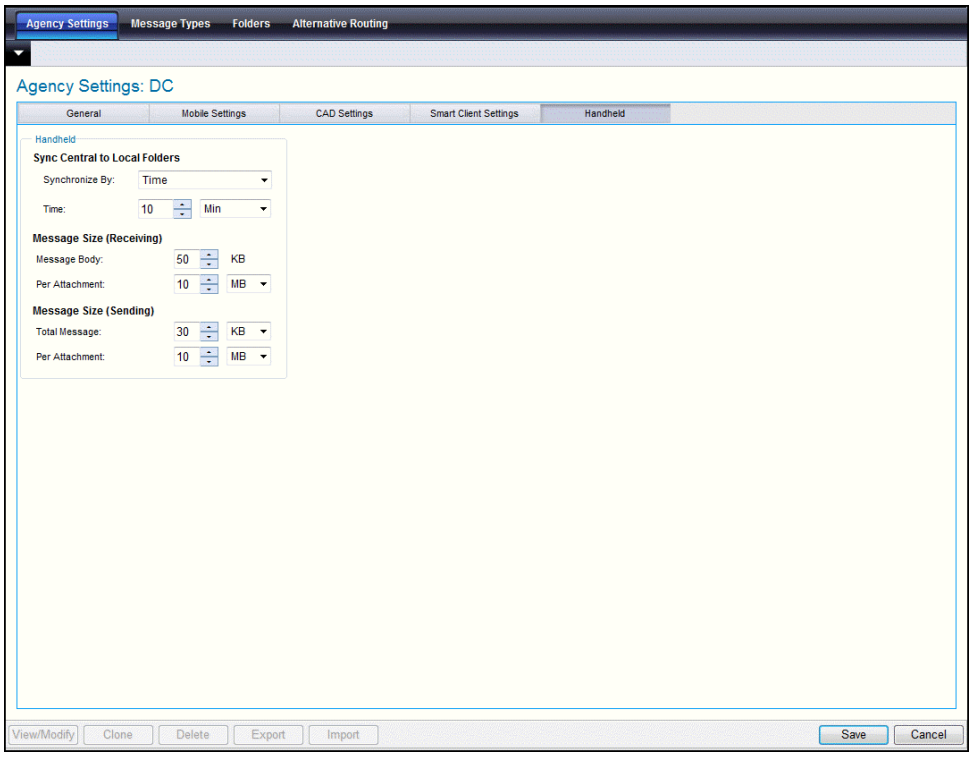


Figure 26-5 Messaging – Agency Settings Tab – Smart Client Settings

2. In the Sync Central to Local Folders section, specify how local folders will be synchronized with the central server. Options are by time, manual action of the user, opening of the local folder, or with each successful login.

3. In the Message Size (Receiving) section, specify the maximum size for an incoming message, the maximum message size without an attachment, and the maximum attachment size.

4. In the Message Size (Sending) section, specify the maximum size for an outgoing message and the maximum attachment size.

5. Click **Save**.

Configuring Message Types

Use the Message Types configuration item to configure Email, BOLO, Notification, and Query message types for Mobile, CAD, and the Smart Client.

- General – Where you set a description, priority, pre-delivery expiration, post-delivery expiration, and BOLO options.
- Mobile Settings – Where you configure general settings, delivery limitations, and alerts for new message arrivals for Mobile units.
- CAD Settings – Where you configure general settings, delivery limitations, and alerts for new message arrivals for CAD operators.
- Smart Client Settings – Where you configure general settings, delivery limitations, and alerts for new email and query arrivals for Smart Client users.
- Handheld Settings – Where you configure general settings, delivery limitations, and alerts for new email and query arrivals for Handheld users.

Configuring General Message Types

Access the Message Types form from the navigation panel. The General tab contains settings related to the Server.

To configure general message types:

1. From the navigation pane, select **Messaging**, and then select **Message Types**.

   The Message Types form appears with the General tab active.

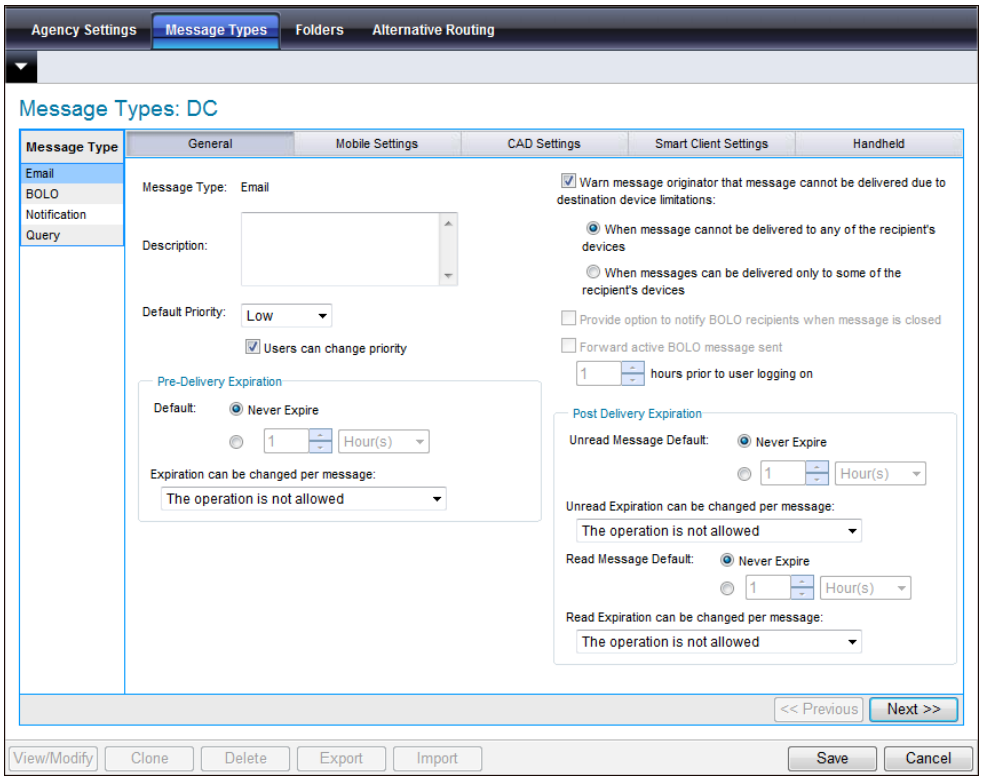


Figure 26-6 Messaging – Message Types Tab – General Subtab

2. From the Message Type list on the left side of the form, select the type of message for which you want to make changes.

   Options are Email, BOLO, Notification, or Query. Different fields may display depending on the option you select.

3. Click **View/Modify**.

   The fields become editable, with the selected message type displayed in the Message Type field.

4. In the Description field, type a description of the message type.

5. In the Default Priority field, enter a priority value of 0 through 9 for the message type.

In the CAD and Mobile clients, the priority values are Low, Medium, and High. For a Low priority, use a value in the 0-3 range. For a Medium priority, use a value in the 4-6 range. For a High priority, use a value in the 7-9 range.

To allow users to adjust this priority, select the Users can change priority check box.

6. To notify the sender when a message cannot be delivered, select the **Warn message originator that message cannot be delivered due to destination device limitations** check box.

   Specify whether the delivery problem is with all of the recipient's devices, or only some the recipient's devices.

7. For the BOLO message type, select any of the following:

   - To notify users when a BOLO is closed, select the **Provide option to notify message recipients when a BOLO message is closed** check box.
   - To forward any active BOLO messages to a newly logged on user, select the **Forward Active BOLO message sent** check box, and then enter the number of hours prior to the user's login for BOLO messages to be sent.

8. In the Post Delivery Expiration section, enter message expiration times for unread and read messages, and if and how these expiration defaults can be changed.

9. Click **Save**.

For scheduled BOLOs, the following configuration settings must be made:

1. Set the value of ScheduleBoloTimerInterval in the Provisioning->Configuration->Edit->BOLO item to 500.

2. Set the value of WorkThreadInterval in the `C:\Program Files\Motorola\PremierOne\CADClient\config\BoloConfig.xml` to 500.

Configuring Mobile Message Types

Configure Mobile message types when you need to change Mobile-specific general settings, or Mobile settings for delivery limitations or new message arrival.

To configure Mobile message types:

1. Access the Message Types form. For details, see Configuring General Message Types.

   The Message Types form appears with the General tab in focus (see Figure 26-6).

2. Select the Mobile Settings tab.

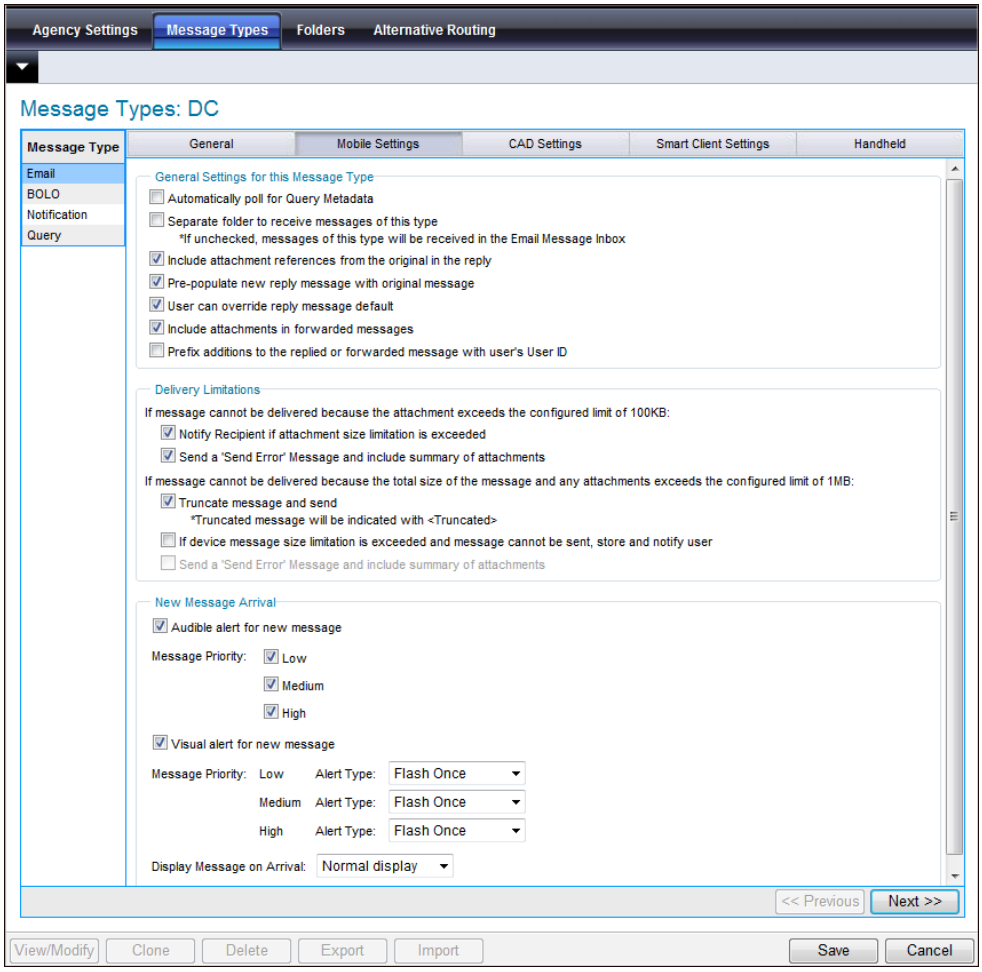


Figure 26-7 Messaging – Message Types Tab – Mobile Settings Subtab

3. From the Message Type list on the left side of the form, select the type of message for which you want to make changes.

   Options include Email, BOLO, Notification, or Query.

4. Click **View/Modify**.

   The fields relevant to the selected message type become editable. Fields that do not apply to the selected message type are inactive.

5. In the General Settings for this Message Type section, select the appropriate check boxes.

6. In the Delivery Limitations section, configure the handling of emails that exceed the provisioned attachment size or total email size.

7. In the New Message Arrival section, specify what alerts, if any, a user will receive upon receiving a new email.

   a. Select the message priority for which you want audible alerts to sound.

   b. Select the message priority for which you want visual alerts to sound, and then select Flash Once or popup window for each message priority.

   c. For Mobile, select one of the following:

      - Normal display – Add the message to the Message List view (default behavior for receiving message).

      - Auto display – Automatically display the message in the Message View window regardless of what the user doing.

      - Force display – Display a popup window asking if the user wants to display the message.

8. Click **Save**.

Configuring CAD Message Types

Configure CAD message types when you need to change CAD-specific general settings, or CAD settings for delivery limitations or new message arrival.

You can provision 100 unread messages on the server to be downloaded at a time. Unread messages currently download when the user logs on and after that, every 15 minutes. Users can force messages to be downloaded by selecting the **Download** command from the **Compose** menu in the Inbox of the Work Assist Area.

Messages sent when the user is online are still delivered immediately.

This setting applies to *each* folder that is available to the user (such as **Inbox**, **Outbox**, **Drafts**, and **Sent**).

For messages to be downloaded, no folder can have *more* than 300 unread and read messages. If the message count of unread and read messages in *any* folder is greater than or equal to 300, the next synchronization cycle will NOT download the next set of messages. For a user to receive all of the latest unread messages, users should delete old messages from their folders to make room for newer messages.

A folder can have more than 300 read and unread messages in some circumstances. For example, assume there are were 100 unread messages on the server awaiting download. The user has an **Inbox** folder with 300 messages and deletes two messages from the **Inbox** folder. At the next synchronization, 100 messages will be downloaded into the **Inbox** folder for a total of 398.

To configure CAD message types:

1. Access the Message Types form. For details, see "Configuring General Message Types" on page 26-9.

   The Message Types form appears with the General tab in focus (see Figure 26-6).

2. Select the CAD Settings tab.

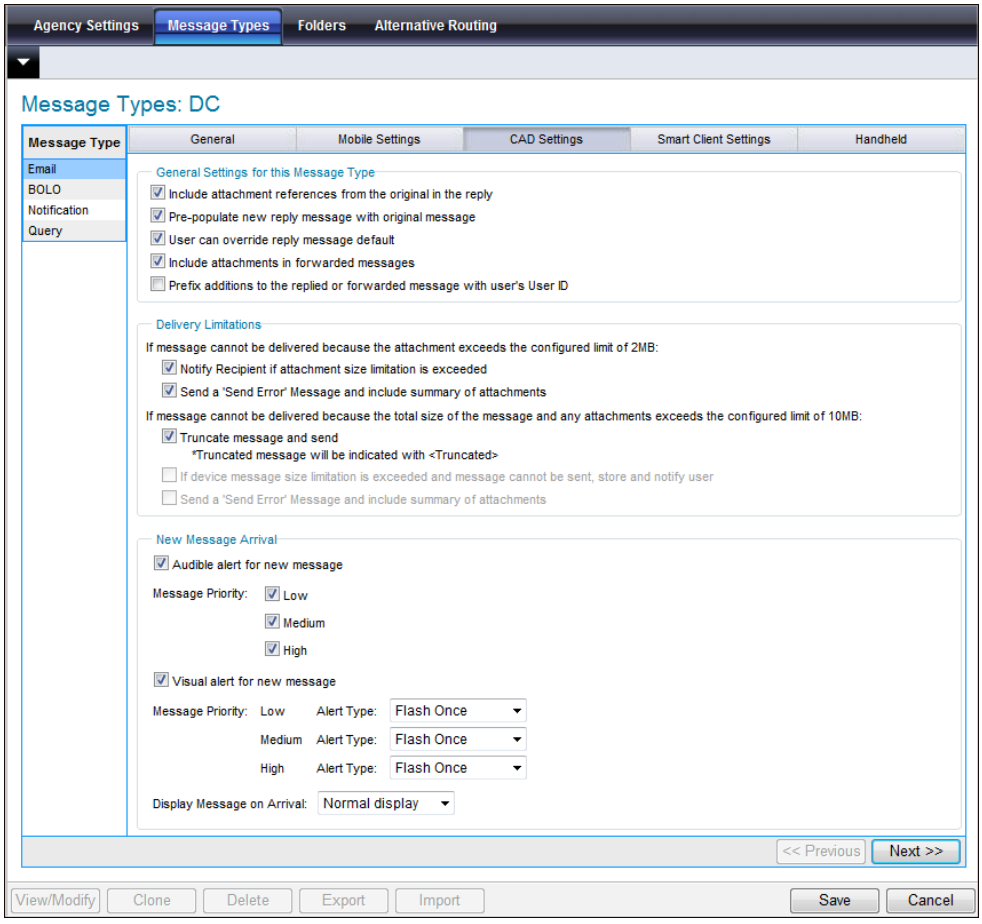


Figure 26-8 Messaging – Message Types Tab – CAD Settings Subtab

3. From the Message Type list on the left side of the form, select the type of message for which you want to make changes.

   Options include Email, BOLO, Notification, or Query.

4. Click **View/Modify**.

The fields relevant to the selected message type become editable. Fields that do not apply to the selected message type are inactive.

5. In the General Settings for this Message Type section, select the appropriate check boxes.

6. In the Delivery Limitations section, configure the handling of emails that exceed the provisioned attachment size or total email size.

7. For emails, in the New Message Arrival section, specify what alerts, if any, a user will receive when receiving a new email.

   The Display Messages on arrival is only functional for Mobile.

8. Click **Save**.

Configuring Smart Client Message Types

Configure Smart Client message types when you need to change Smart Client-specific settings, settings for delivery limitations, or new message arrival alerts.

To configure Smart Client Message types:

1. From the navigation pane, select **Messaging**, and then select **Message Types**.

   The Message Types form appears with the General tab active.

2. Select the Smart Client tab.

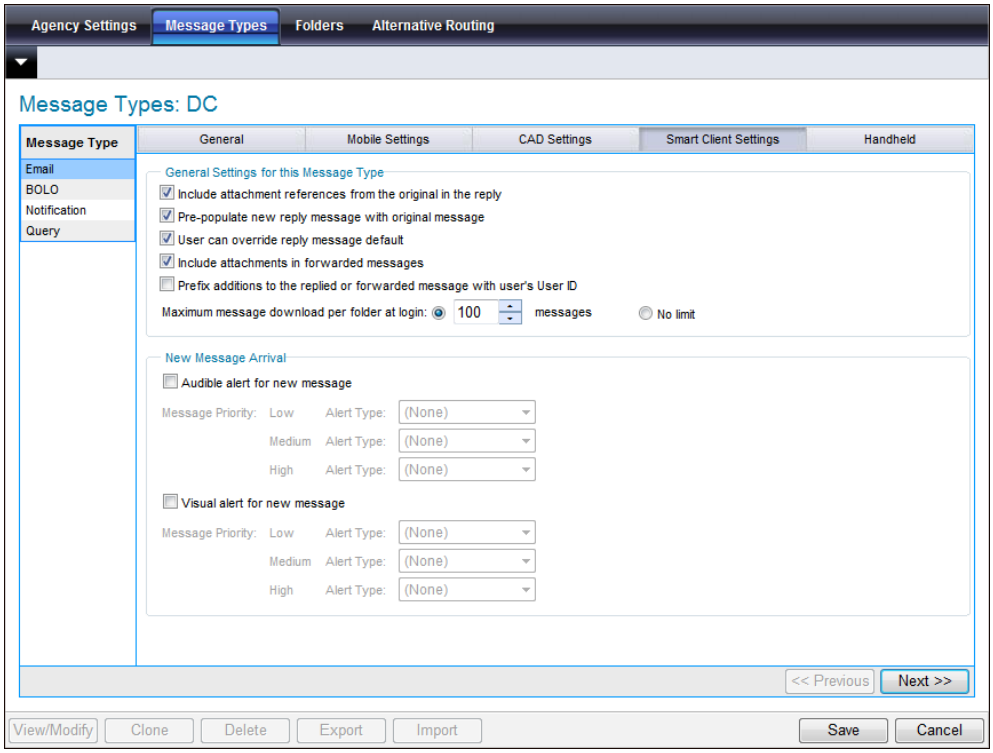


Figure 26-9 Messaging – Message Types Tab – Smart Client Subtab

3. From the Message Type list on the left side of the form, select the type of message for which you want to make changes.

4. Click **View/Modify**.

   The fields become editable, with the selected message type displayed in the Message Type field. Different options display, depending on the Message Type you select.

5. In the General Settings for this Message Type section, select the appropriate options.

6. In the New Message Arrival section, select the appropriate audible and visual alert types for low, medium, and high level priority messages.

7. Click **Save**.

Configuring Handheld Message Types

Configure Handheld message types when you need to change Handheld-specific settings, settings for delivery limitations, or new message arrival alerts.

To configure Handheld Message types:

1. From the navigation pane, select **Messaging**, and then select **Message Types**.

   The Message Types form appears with the General tab active.

2. Select the Handheld tab.

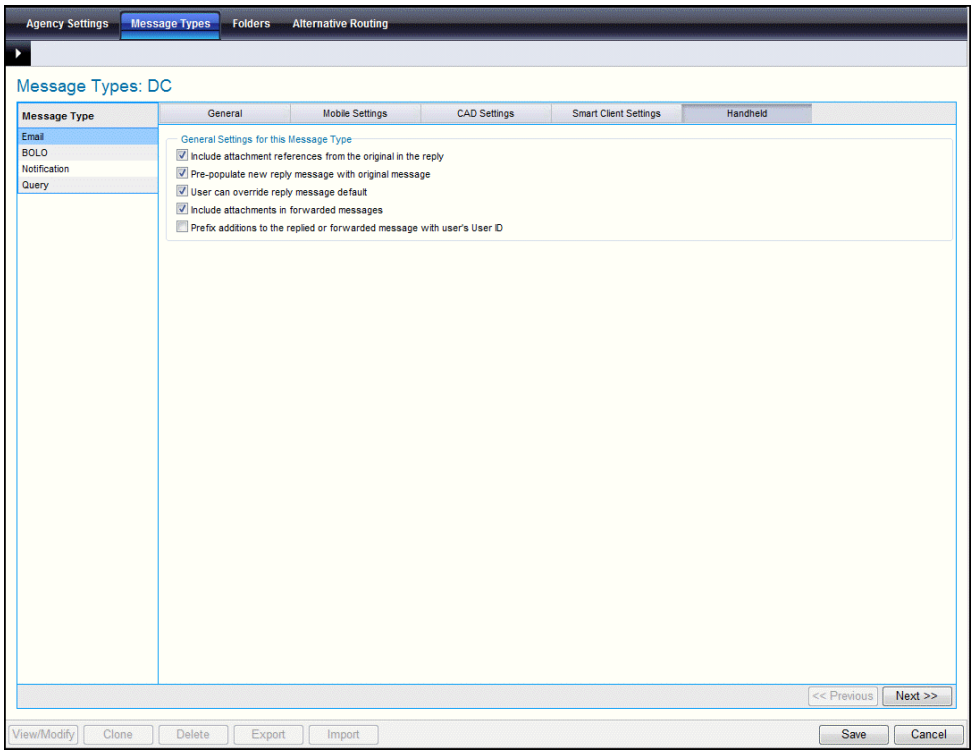


Figure 26-10 Messaging – Message Types Tab – Handheld Subtab

3. From the Message Type list on the left side of the form, select the type of message for which you want to make changes.

4. Click **View/Modify**.

   The fields become editable, with the selected message type displayed in the Message Type field. Different options display, depending on the Message Type you select.

5. In the General Settings for this Message Type section, select the appropriate options.

6. Click **Save**.

Configuring Message Folder Settings

The Message Folders configuration item has the following tabs:

- Mobile – Where you configure the general folder settings, the download preview threshold, the procedure for when the folder is full, or the procedure for when the user logs off from Mobile.
- CAD – Where you configure the general folder settings, the download preview threshold, the procedure for when the folder is full, or the procedure for when the user logs off from CAD.
- Smart Client – Where you configure the general folder settings, the download preview threshold, the procedure for when the folder is full, or the procedure for when the user logs off from the Smart Client.
- Handheld – Where you configure the general folder settings and the procedure for when the user logs off from the Handheld Client.

Configuring Mobile Message Folders

Configure Mobile message folders when you need to change the general folder settings, the download preview threshold, the procedure for when the folder is full, or the procedure for when the user logs off of Mobile.

You access the Folders form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

To configure Mobile message folders:

1. From the navigation pane, select **Messaging**, and then select **Folders**.

   The Folders form appears with the Mobile tab active.

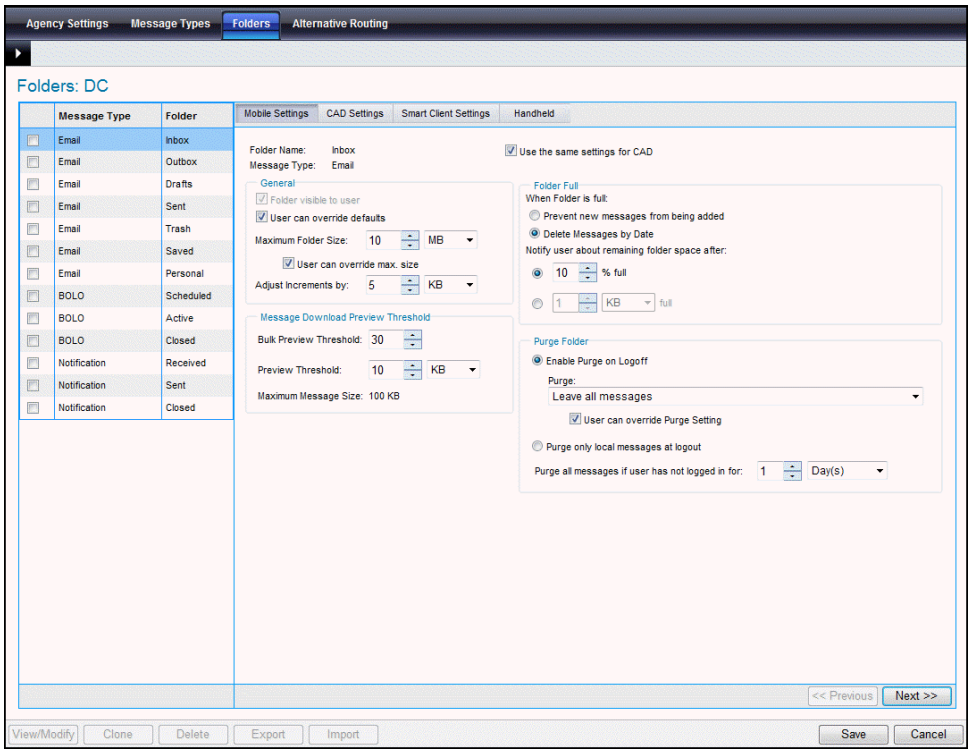


Figure 26-11 Messaging – Folders Tab – Mobile Settings

2. From the Folders list on the left side of the form, select the folder and type of message for which you want to make changes; for example, the Inbox folder for Email type messages.

3. Click **View/Modify**.

4. To make the same changes to CAD, select the **Use the same settings for CAD** check box at the top of the form.

5. In the General section, do any of the following:

   - To make the folder visible to the user, select the **Folder visible to user** check box.
   - To allow the user to override folder defaults, select the **User can override defaults** check box.
   - In the Maximum folder size list, enter the maximum size for the folder.
   - To allow the user to override the maximum size limit, select the **User can override max. size** check box, and then enter the increments by which the user can increase the size.

6. In the Message Download Preview Threshold section, enter any of the following:
   - In the Bulk Preview Threshold field, enter the maximum size for all messages being previewed.
   - In the Preview Threshold field, enter the maximum size of a message to preview.
7. In the Folder Full section, enter the actions to take when a folder reaches its maximum size.
8. In the Purge Folder section, enter the actions to take to purge messages when the user logs off.
9. Click **Save**.

Configuring CAD Message Folders

Configure CAD message folders when you need to change the general folder settings, the download preview threshold, the procedure for when the folder is full, or the procedure for when the user logs off of CAD.

To configure CAD message folders:

1. Access the Folders form. For details, see "Configuring Mobile Message Folders" on page 26-17.

   The Folders form appears with the Mobile tab active.

2. Select the CAD Settings tab.

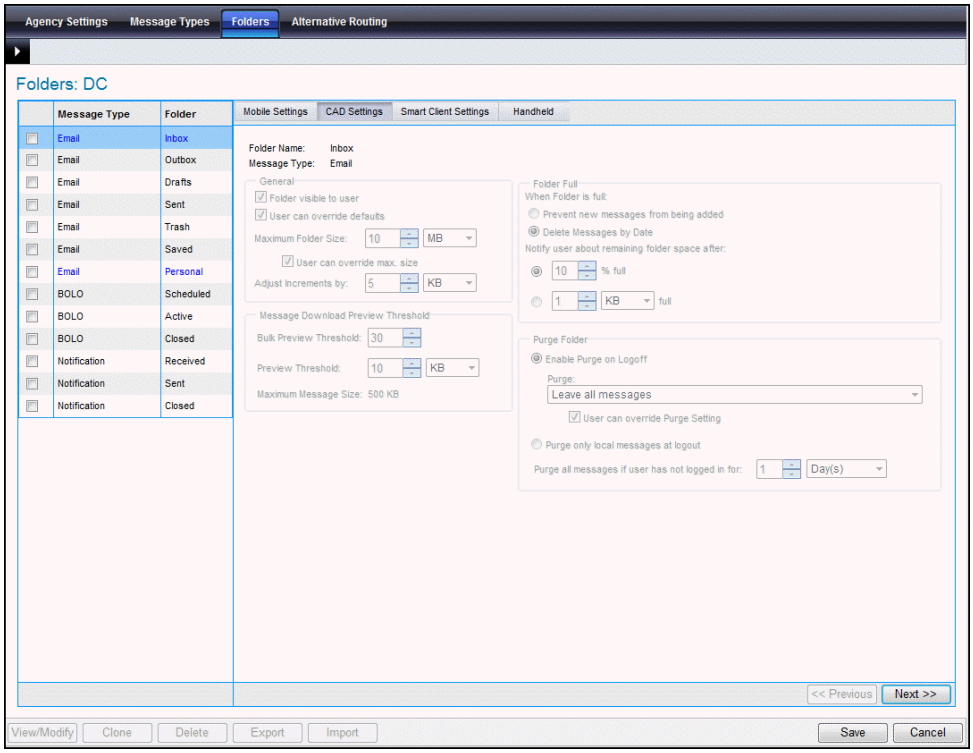


Figure 26-12 Messaging – Folders Tab – CAD Settings

3. From the Folders list on the left side of the form, select the folder and type of message for which you want to make changes; for example, the Inbox folder for Email type messages.

4. Click **View/Modify**.

5. In the General section, do any of the following:

   - To make the folder visible to the user, select the **Folder visible to user** check box.
   - To allow the user to override folder defaults, select the **User can override defaults** check box.
   - In the Maximum folder size field, enter the maximum size for the folder.
   - To allow the user to override the maximum size limit, select the **User can override max. size** check box, and then enter the increments by which the user can increase the size.

6. In the Message Download Preview Threshold section, enter any of the following:

   - In the Bulk Preview Threshold field, enter the maximum size for all messages being previewed.
   - In the Preview Threshold field, enter the maximum size of a message to preview.

7. In the Folder Full section, enter the actions to take when a folder reaches its maximum size.

8. In the Purge Folder section, enter the actions to take to purge messages when the user logs off.

9. Click **Save**.

Configuring Smart Client Message Folders

Configure Smart Client message folders when you need to change the general folder settings, the download preview threshold, the procedure for when the folder is full, or the procedure for when the user logs off of the Smart Client.

To configure Smart Client message folders:

1. Access the Folders form. For details, see "Configuring Mobile Message Folders" on page 26-17.

   The Folders form appears with the Mobile tab active.

2. Select the Smart Client Settings tab.

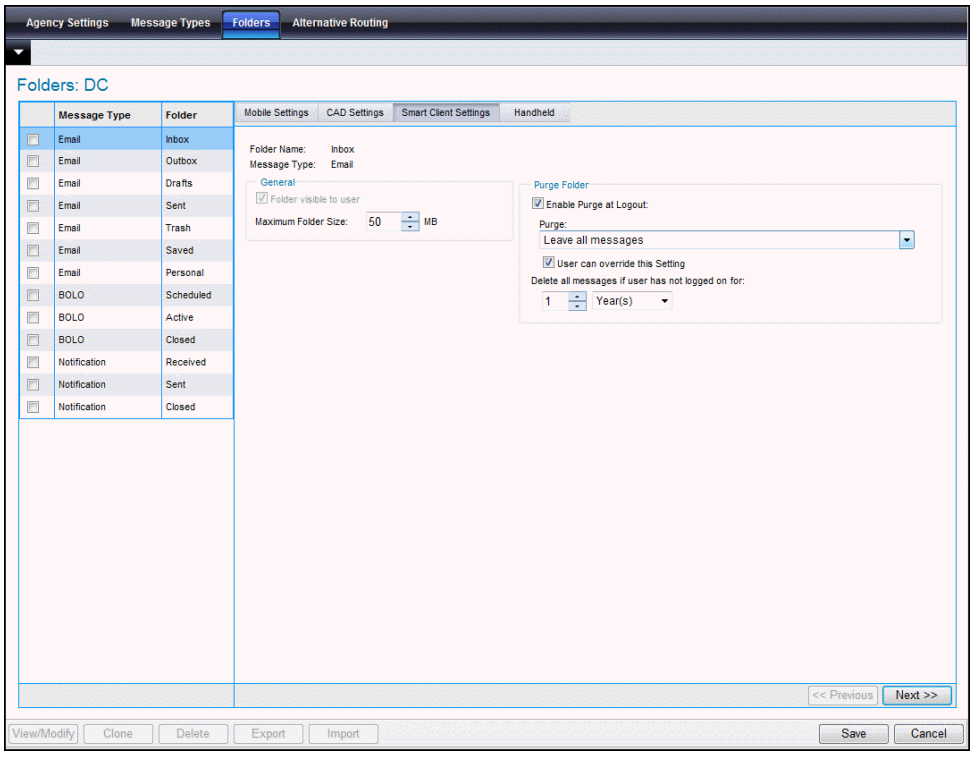


Figure 26-13 Messaging – Folders Tab – Smart Client Settings

3. From the Folders list on the left side of the form, select the folder and type of message for which you want to make changes; for example, the Inbox folder for Email type messages.

4. Click **View/Modify**.

5. In the General section, do any of the following:

   - To make the folder visible to the user, select the **Folder visible to user** check box.
   - To allow the user to override folder defaults, select the **User can override defaults** check box.
   - In the Maximum folder size field, enter the maximum size for the folder.
   - To allow the user to override the maximum size limit, select the **User can override max. size** check box, and then enter the increments by which the user can increase the size.

6. In the Message Download Preview Threshold section, enter any of the following:

   - In the Bulk Preview Threshold field, enter the maximum size for all messages being previewed.
   - In the Preview Threshold field, enter the maximum size of a message to preview.

7. In the Folder Full section, enter the actions to take when a folder reaches its maximum size.

8. In the Purge Folder section, enter the actions to take to purge messages when the user logs off.

9. Click **Save**.

Configuring Handheld Message Folders

Configure Handheld message folders when you need to change the general folder settings or the procedure for when the user logs off of the Handheld device.

NOTE
PremierOne Handheld devices use only the Inbox, Sent, and Trash folders.

To configure Handheld message folders:

1. Access the Folders form. For details, see “Configuring Mobile Message Folders” on page 26-17.

   The Folders form appears with the Mobile Settings tab active.

2. Select the Handheld tab.

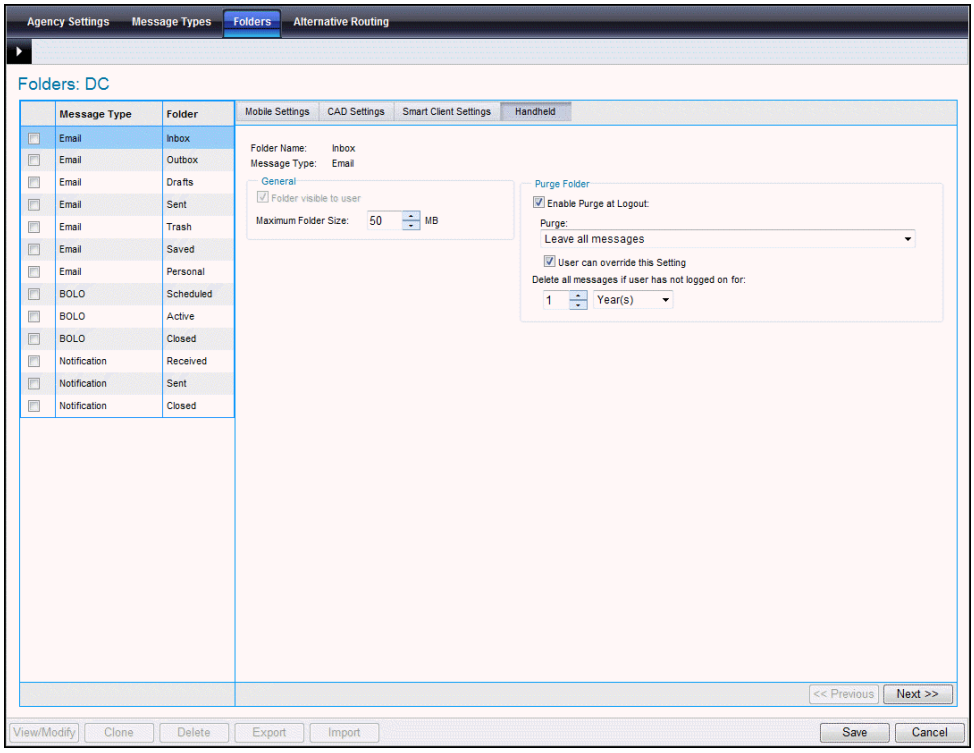


Figure 26-14 Messaging – Folders Tab – Handheld Settings

3. From the Folders list on the left side of the form, select the folder and type of message for which you want to make changes; for example, the Inbox folder for Email type messages.

4. Click **View/Modify**.

5. In the General section, do any of the following:

   - To make the folder visible to the user, select the **Folder visible to user** check box.

   - In the Maximum folder size field, enter the maximum size for the folder.

6. In the Purge Folder section, enter the actions to take to purge messages when the user logs off.

7. Click **Save**.

Configuring Alternative Routing for Messages

Configure alternative routing for messages when you need to route messages from one mail box to one or more other mail boxes. This feature could be used when a supervisor or someone in a similar role will not be receiving messages for some reason, but has a backup to cover his or her responsibilities.

To configure alternative routing for messages:

1. From the navigation panel, select **Messaging**, and then select **Alternative Routing**.

   The Alternative Routing form appears.

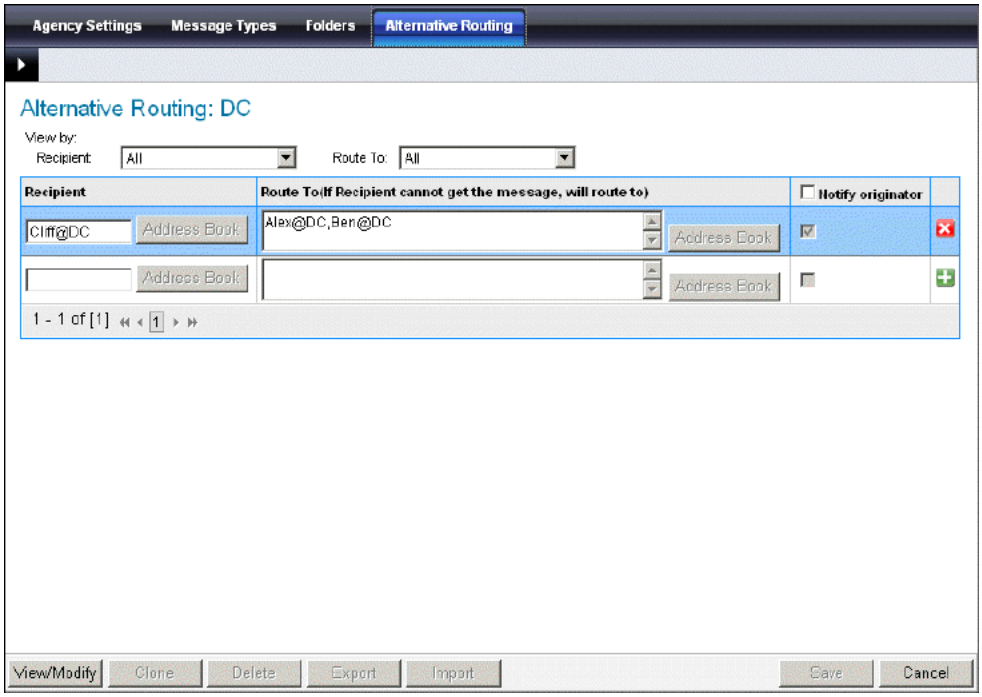


Figure 26-15 Messaging – Alternative Routing Form

2. Click **View/Modify**.

3. In the View by section at the top of the form, above the table, do the following:

   a. From the Recipient list, select how you want to view the information in the Recipient column of the table: All or Personnel.

   b. From the Route To list, select how you want to view the information in the Route From column of the table: All or the IDs entered in the Route To field.

4. In the Route To column of the table, click **Address Book** to use the Address book dialog to locate the recipients.

The Select Address book dialog appears.

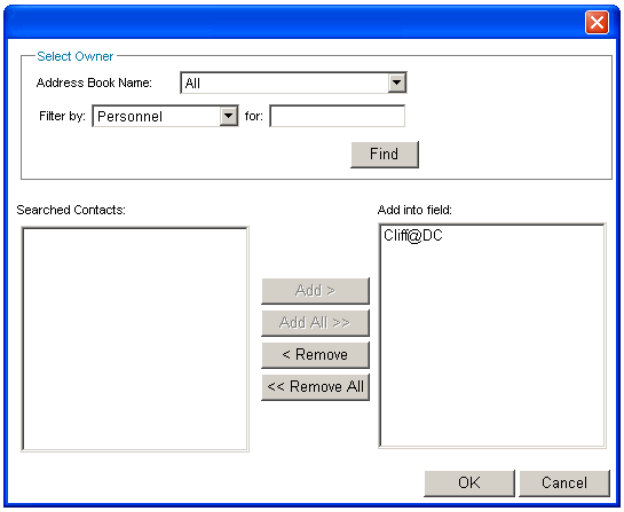


Figure 26-16 Address Book Dialog

a. Select the address book and the filter you want to use.

b. Type the name or ID you want to find, and then click **Find**.

   Contacts that match your search appear in the Searched Contacts box.

c. From the list in the **Searched Contacts** box, select the contact or contacts you want, and then click **Add** or **Add All**.

d. Click **OK** to return to the Alternative Routing form.

   The contact you selected appears in the Recipient column.

5. In the Route To column of the table, click **Address Book**.

   Follow the instructions in the previous step to add the persons to route the message to.

   The contacts you selected appear in the Route To field.

6. To notify the originator of the alternative routing, select the check box in the Notify originator column.

7. Click the plus symbol at the end of the row to save the information to save the information and add another row.

CAUTION
If you do not click the plus symbol, PremierOne does not save the alternative routing information, even after you click Save.

8. Click **Save**.

CHAPTER 27

Configuring Mobile Browsers

The Mobile Browser configuration item contains one configuration item:

Mobile Browser – Where you identify the Web sites that Mobile users can view. For details, see “Configuring Agency Settings for Mobile Browsers” on page 27-1.

Configuring Agency Settings for Mobile Browsers

Configure the agency settings when you want to add or change a Web site that can be viewed by Mobile users.

To configure agency settings for Mobile browsers:

1. From the navigation panel, select **Mobile Browser**.
2. Select **Agency Settings**.

The Agency Settings form appears.

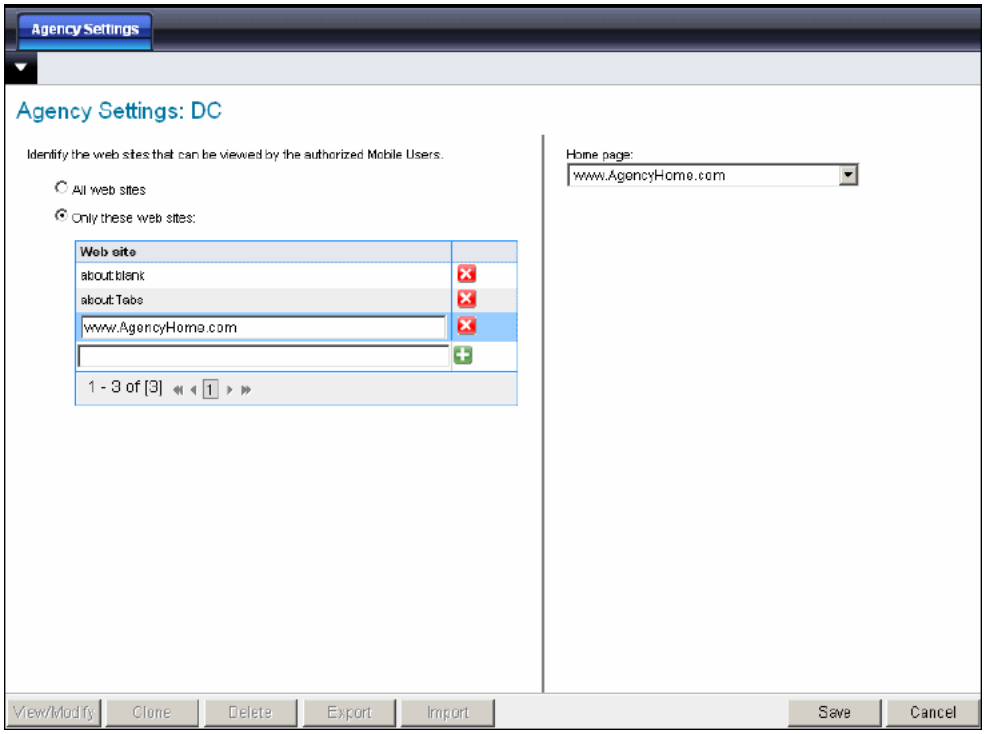


Figure 27-1 Mobile Browser – Agency Settings

3. Click **View/Modify**.
4. Select whether the Mobile users can view all Web sites or only selected Web sites.
5. If you specified to view only selected Web sites, type the URLs for the sites in the Web site table.

   To add another row, click the plus icon at the end of the final row.

   To remove an entry, click the X icon at the end of the row to remove it from the table.
6. From the Homepage list, select the Web page to be the home page for the users.
7. Click **Save**.

CHAPTER 28

Configuring Peripherals

The Peripherals configuration item contains the following items:

- Printers – Where you can view the configured printers for your agency. For details, see “Viewing Printers” on page 28-1.
- GPS Settings – Where you set the triggers that automatically update the location field and configure the cadence settings for selected vehicle types. For details, see “Configuring GPS Settings” on page 28-2.
- Magnetic Stripe Reader – Where you configure magnetic stripe readers for mobile units. For details, see “Configuring Magnetic Stripe Readers” on page 28-5.

Viewing Printers

View printer settings when you need to view the printers set up for an agency.

You access the Printer form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

To view printer settings:

1. From the navigation panel, select **Peripherals**, and then select **Printer**.

The Printer form appears. A list of existing printers displays on the left side of the form.

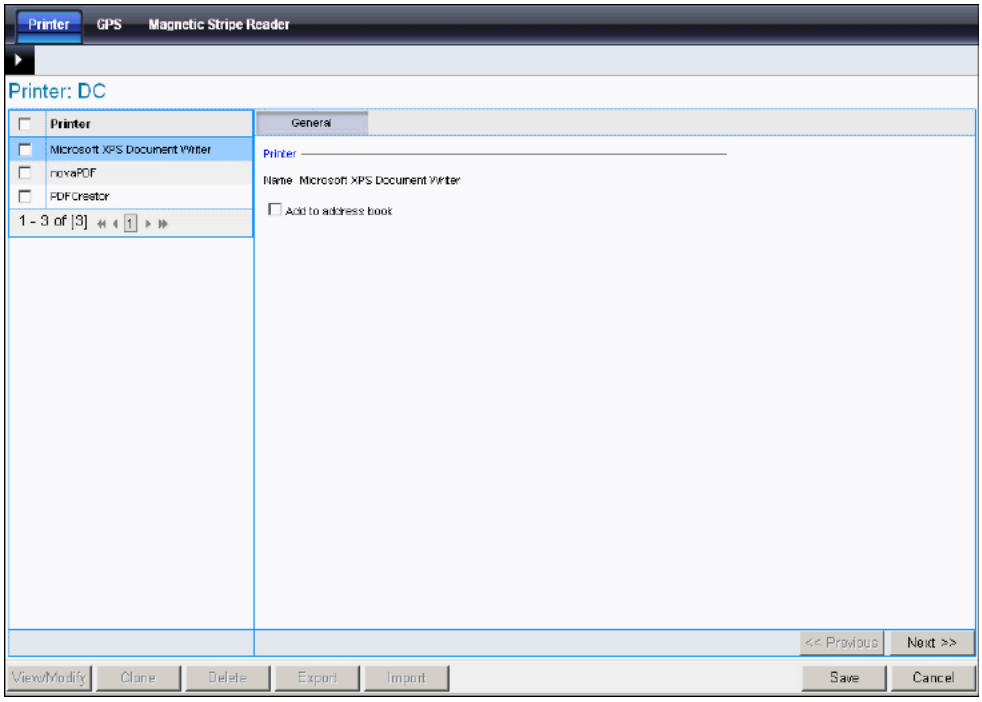


Figure 28-1 Peripherals Printer Tab

2. From the Printer list, select the printer you want to view.
3. Click **View/Modify**.
4. Click **Save** or **Cancel**.

Configuring GPS Settings

View GPS settings when you need to configure the following items:

- The triggers that automatically update the location field
- The cadence settings for selected vehicle types

You access the GPS Setting form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

To view GPS settings:

1. From the navigation panel, select **Peripherals**, and then select **GPS**.

   The GPS Setting form appears. A list of existing GPS devices displays on the left side of the form.

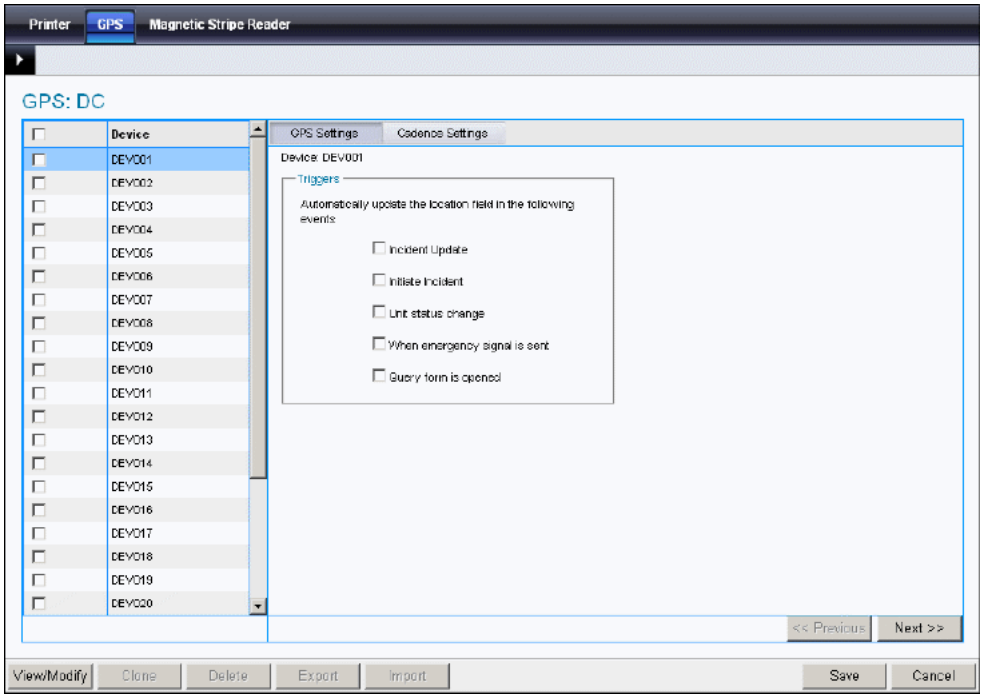


Figure 28-2 Peripherals GPS Settings Tab

2. From the Device list, select a GPS device to configure.
3. Click **View/Modify**.
4. Change the events in which the location information is updated as needed.
5. Click the Cadence Settings tab and change the cadence rules as needed.

- In the Min. Reporting Time field, enter the minimum time in which a vehicle is scheduled to report its location.
- In the Max. Reporting Time field, enter the maximum time in which a vehicle is scheduled to report its location.
- In the Max. Distance Travelled list, enter the maximum distance the vehicle can travel before reporting its location.

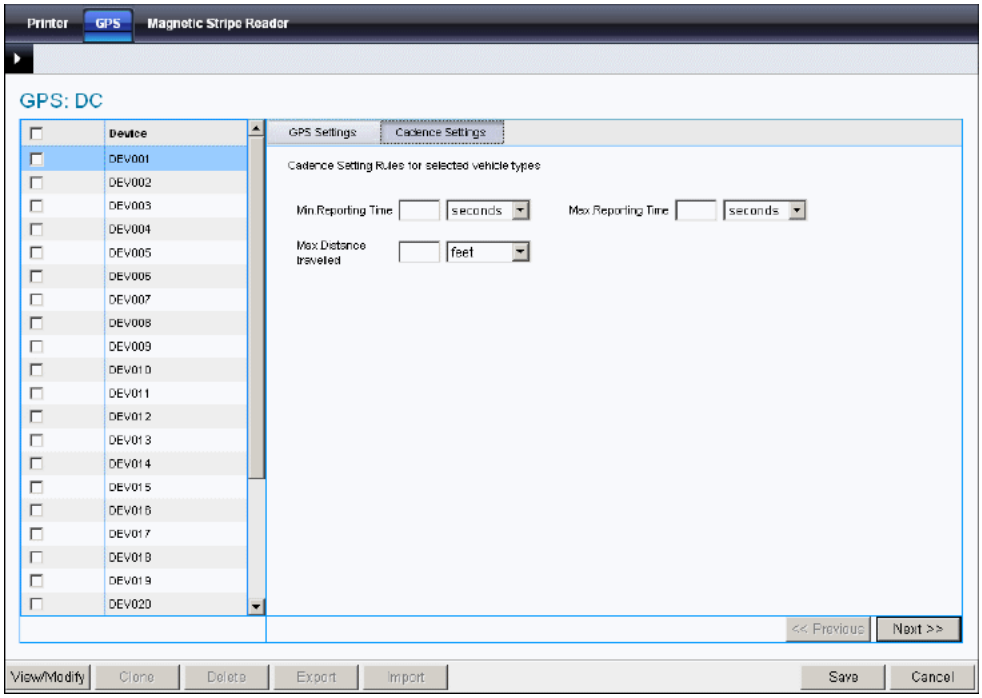


Figure 28-3 Peripherals – GPS Cadence Settings

6. Click **Save**.

Configuring Magnetic Stripe Readers

Use the Magnetic Stripe Reading configuration item to configure magnetic stripe readers for mobile users. Magnetic stripe readers allow the mobile user to swipe a driver's license. The license information and the results of any related queries associated with licenses are automatically sent to the mobile unit. This saves time for officers because they do not need to manually enter the license information or run the query.

You access the Magnetic Stripe reader form from the navigation panel. For details on using the filter display to access the form, see "Using Filters" on page 2-7.

To configure magnetic stripe reader settings:

1. From the navigation panel, select **Peripherals**, and then select **Magnetic Stripe Reader**.

   The Magnetic Stripe Reader form appears. A list of preconfigured run actions displays on the left side of the form.

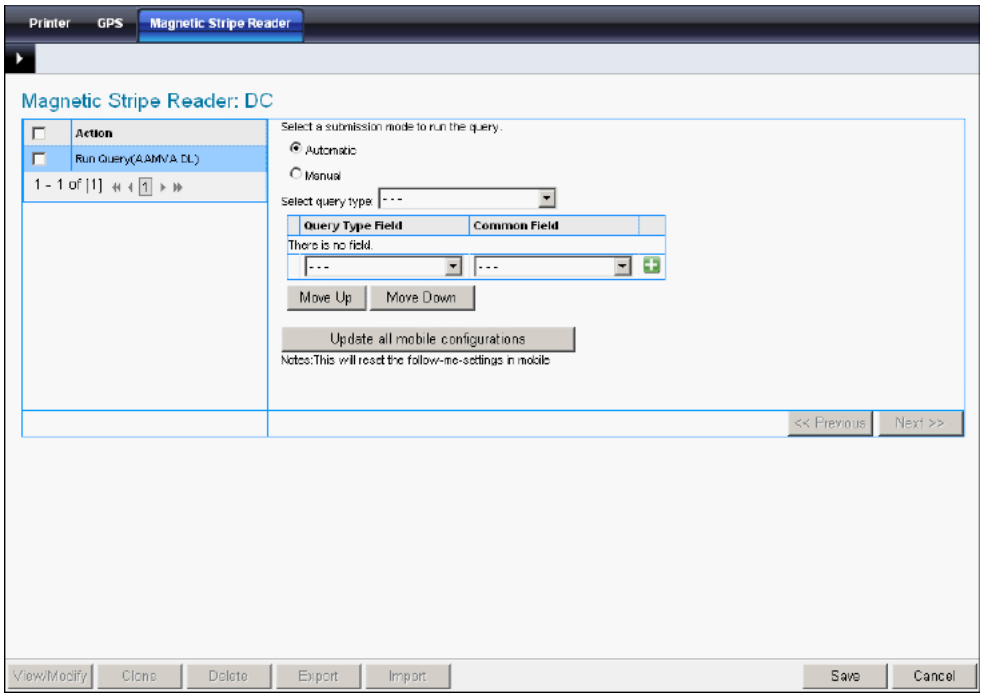


Figure 28-4 Peripherals Magnetic Strike Reader Tab

2. From the Action list, select the action you want to configure.

   Selecting the check box does not select the item.

3. Click **View/Modify**.

4. Do one of the following:
   - To have the submission run automatically, select **Automatic**.
   - To have the submission require manual intervention by the mobile user, select **Manual**.
5. From the Select query type field, select the query type to run.

   You can only have one query type per action.
6. From the QueryTypeField list, select the field name you want submitted to the state database.
7. From the CommonField list, select the equivalent field internal to PremierOne.

   This field is not sent to the external database.
8. Click the plus symbol at the end of the row.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the code information, even after you click Save.
9. Add any other fields you want submitted.
10. To reorder how the information is returned, select the check box next to the field and then select the **Move Up** or **Move Down** button until the field is in the correct location.
11. To update all mobile units with the query configuration, select the **Update all mobile configurations** button.

    This will reset the settings for the mobile user. Follow-me-settings are the settings that follow the mobile user between workstations.
12. Click **Save**.

CHAPTER 29

Configuring External Adapters

The External Adapters configuration item contains the following items:

- System Definition – Where you define external systems, such as message switches. For details, see “Configuring System Information for External Adapters” on page 29-1.
- External Agency – Where you define the external agencies that can log in from external systems such as PMDC. For details, see “Configuring External Agencies for External Adapters” on page 29-3.
- Entity Mapping – Where you set complementary information for routing related to the provisioning of PMDC fire-clients. For details, see “Configuring Entity Mapping for External Adapters” on page 29-4.

Configuring System Information for External Adapters

Use the System Definition page to define external systems. Currently only message switches are supported.

To configure system information for external adapters:

1. From the navigation panel, select **External Adapters**, and then select **System Information**.

The System Information tab of the External Adapters form appears.

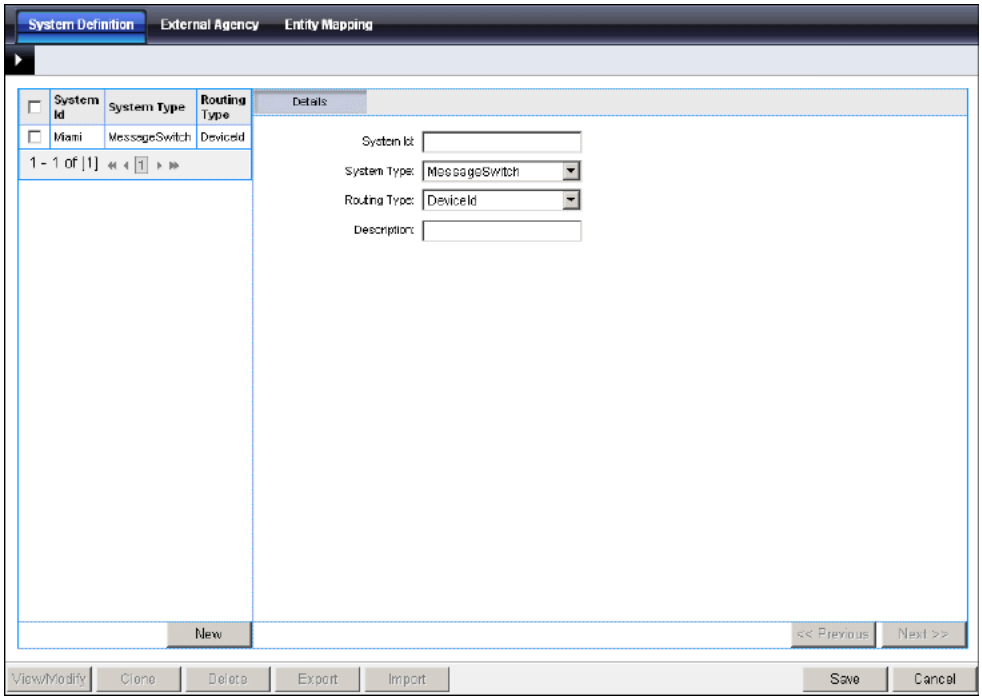


Figure 29-1 External Adapters Form – System Definition Tab

2. At the bottom of the form, click the **New** button.
3. In the System ID field, enter the system ID.
4. From the System Type field, select the system type.

   For PMDC, select MessageSwitch.
5. From the Routing Type field, select the routing type.

   The routing type is used to identify which field in the external system will be used as routing ID; it cannot be changed once defined. Three routing types are supported: Device ID, Unit ID, and User ID. They are mapped to the device ID, unit ID, and user ID in PremierOne. You can have more than one system with the same system type.
6. In the Description field, enter a description of the system.
7. Click the **Save** button.

Configuring External Agencies for External Adapters

Use the External Agency form to define the external agencies that can log in from external systems such as PMDC. The agency must first be created in Agency configuration item. The agency configuration type should be external type, such as P1 CAD with PMDC.

The external agency ID and system ID cannot be changed once defined. Agencies are saved in table [PMDC_ExAgency]. If the agency configuration type of existing agencies are not changed to `P1 CAD with PMDC` in agency settings, an error will occur when you edit the settings.

To configure an external agency:

1. Access the form for Adapters. For instructions, see "Configuring System Information for External Adapters" on page 29-1.

2. Click the External Agency tab.

   The External Agency tab of the External Adapters form appears.

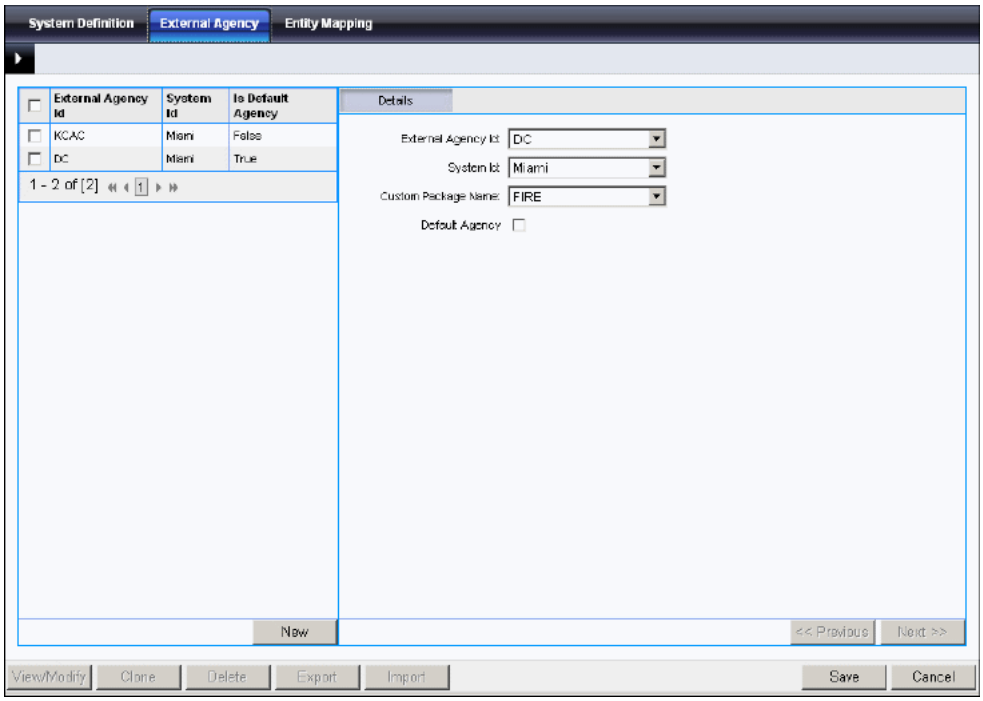


Figure 29-2 External Adapters Form – External Agency Tab

3. From the External Agency Id field, select the ID for the external agency.

4. From the System ID field, select the system ID.

5. In the Custom Package Name field, type either LAW or FIRE.

   The value is case-sensitive, so be sure to enter the value in capitals.

6. In the Agency Type Code field, enter the PremierOne agency type. Agency types are defined in the Agency configuration item.

7. To set the agency as the default, select **Default Agency** check box.

   The default agency is usually law. Only one agency can be set to default agency.

8. Click **Save**.

Configuring Entity Mapping for External Adapters

Use the Entity Mapping form to set complementary information for routing. This is only related to the provisioning of PMDC fire-clients and is an optional configuration. The created entity mapping is only the default value used by the login transaction in case the user ID or unit ID is not provided. Once the user ID or unit ID is provided, the entity mapping configuration is ignored.

For example, if agency law agency `X` is configured in the system, and it's routing type is `DeviceId`, `DEV005` can be used as its routing ID. You can configure an entity mapping to routing `DEV005` by adding `NUser1` to be `User` entity type. Then when a user in a fire agency logs in with `DEV005`, if the user ID is not provided, `NUser1` will be used to login CAD system. The configured entity mapping is saved in table [`PMDC_Entity_Mapping`].

To configure entity mapping:

1. Access the form for Adapters. For instructions, see "Configuring System Information for External Adapters" on page 29-1.

2. Click the Entity Mapping tab.

The Entity Mapping form appears.

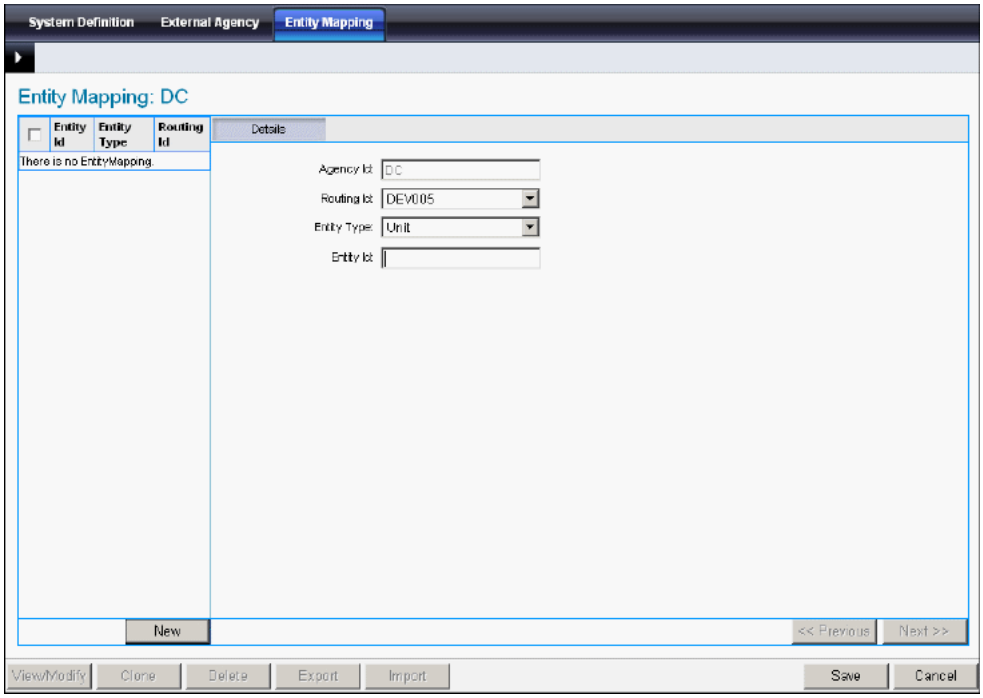


Figure 29-3 External Adapters Form – Entity Mapping Tab

3. From the Routing ID list, select the routing for the PMDC client.
4. From the Entity Type list, select the PMDC fire-related entity, such as unit, device, or user.
5. In the Entity ID field, enter the ID of the entity.
6. Click **Save**.

CHAPTER 30

Configuring Purge Operations

The Purge Operation configuration item contains the following items:

- Scheduled Purges – Where you can view the list of scheduled purges for online and warehouse records. For details, see “Viewing Scheduled Purges” on page 30-1.
- Online Scheduling– Where you add online records to be purged either immediately or on a regular schedule. For details, see “Configuring Online Purge Options” on page 30-3.
- RDW Scheduling – Where you set when records are purged from reporting data warehouses. For details, see “Configuring Reporting Data Warehouse Purge Options” on page 30-5.

Viewing Scheduled Purges

Use the Scheduled Purges form to display the list of scheduled purges for online and warehouse records. You can access the Online and RDW purge settings from this form.

You access the Scheduled Purges form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

NOTE

You can generate reports of all scheduled purges and a history of all purges that have been performed. For details, see *PremierOne Reporting User Guide*.

To view scheduled purge settings:

1. From the navigation panel, select **Purge Operation**, and then select **Scheduled Purges**.

   The Scheduled Purges form appears.

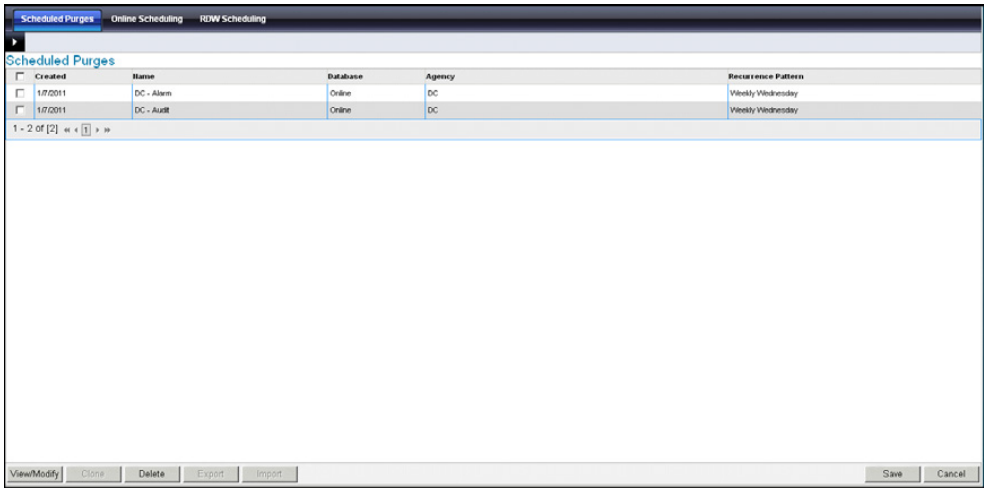


Figure 30-1 Purge Operation – General Tab

2. From the list, select the database for which you want to modify the purge settings.
3. Click **View/Modify**.

   Either the Online Scheduling or the RDW Scheduling tab appears. For more information, see “Configuring Online Purge Options” on page 30-3 or “Configuring Reporting Data Warehouse Purge Options” on page 30-5.

4. Make any necessary changes.
5. Click **Save**.

   A summary of the changed purge operation appears on the Scheduled Purges tab.

Configuring Online Purge Options

Add online database purge settings when you need to add a new set of online records to be purged either immediately or on a regular schedule. Use the Online Scheduling configuration item to set when online records should be purged.

You access the Online Scheduling form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

To add online database purge operations:

1. From the navigation panel, select **Purge Operation**, and then select **Online Scheduling**.

   The Online Scheduling form appears. A list of agencies displays on the left side of the form.

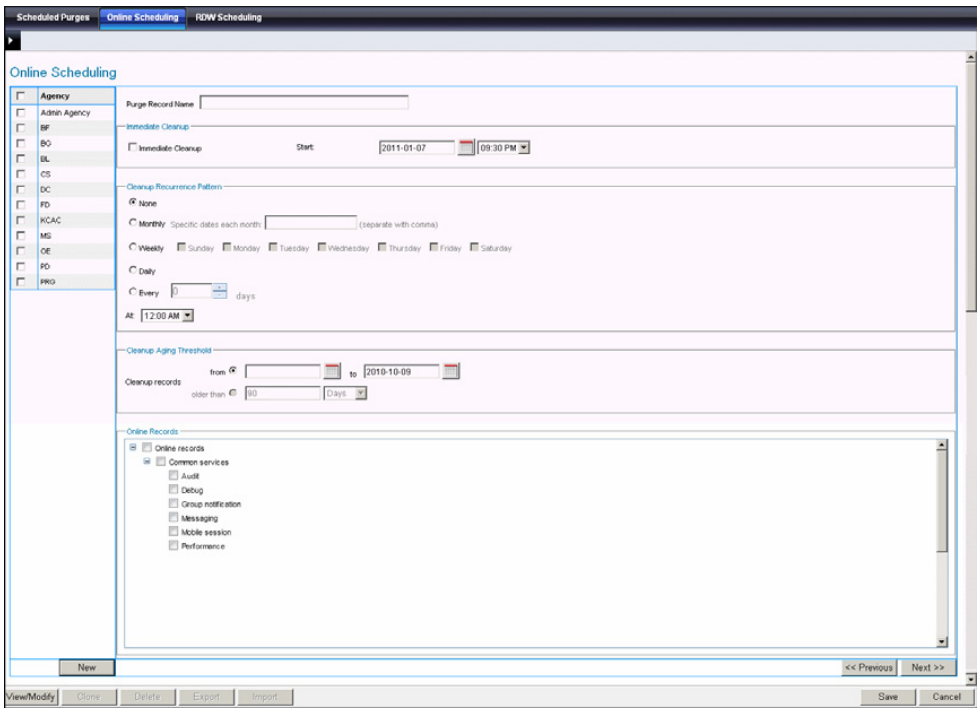


Figure 30-2 Purge Operation – Online Tab

2. At the bottom of the agency list on the left, click the **New** button. You may need to scroll down to see it.

3. In the Purge Record Name field, type a name for this purge operation.

4. Set up the cleanup. Your choices are the following:

   - Immediate Cleanup – Select the **Immediate Cleanup** check box if this purge operation need is immediate. You can select a date range for the immediate cleanup in the Cleanup Aging Threshold section

   - Cleanup Recurrence Pattern – If this purge operation is a routine maintenance operation that recurs on a scheduled basis, select the schedule operations in the Cleanup Recurrence Pattern section. You can select the age of records to be purged in the Cleanup Aging Threshold section.

5. In the Cleanup Aging Threshold section, select the age records must reach before they can be purged.

6. In the Online Records section, select the specific types of records to be purged.

   The online records include the following tables:

CAD (Online)	Mobile/Common Service (Online)
Alarm	(All)
Audit	Audit
DeviceMessage	Bolo
E911	Chat
IncidentManagement	Debug
LoginGroups	GroupNotification
ManualNotification	Messaging
Radio	MobileSession
ReportNumbers	Performance
StatusMonitor	Query
StatusTimer	StateInterface
TDD	UserSession
UserSignOnArea	

7. Click **Save**.

   A summary of the purge operation appears on the Scheduled Purges tab.

NOTE
The New button at the bottom of the page refreshes the page. Use this button if you want to discard your previous input and create a new purge.

Configuring Reporting Data Warehouse Purge Options

Use the RDW Scheduling configuration form to set when records are purged from the data warehouse.

Unit and incident data is copied from the production database to a reporting database warehouse (RDW) in “near to real time.” This information is used to create reports without interfering with the production system. The RDW also maintains a copy of the production data in case something happens to the production database.

You access the RDW Scheduling form from the navigation panel. For details on using the filter display to access the form, see “Using Filters” on page 2-7.

To configure RDW purge settings:

1. From the navigation panel, select **Purge Operation**, and then select **RDW Scheduling**.

   The RDW Scheduling form appears. A list of agencies displays on the left side of the form.

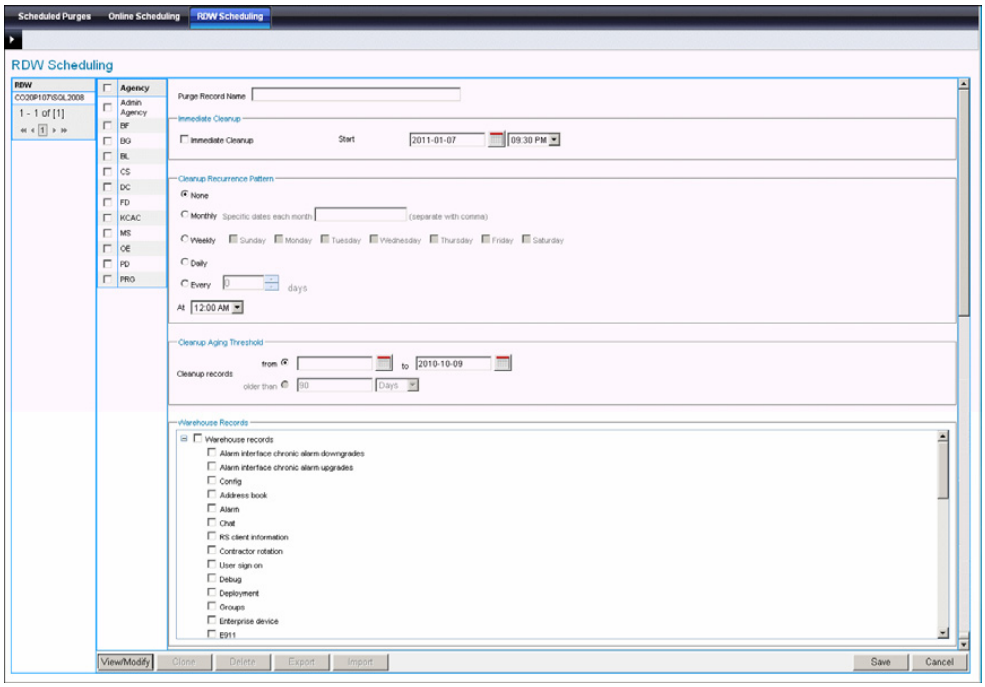


Figure 30-3 Purge Operation – Warehouse Form

2. At the bottom of the agency list on the left, click the **New** button. You may have to scroll down to see it.

3. In the Purge Record Name field, type a name for this purge operation.

4. Set up the cleanup. Your choices are:

   - Immediate Cleanup – Select the **Immediate Cleanup** check box and enter a start date and time if this purge operation need is immediate.

   - Cleanup Recurrence Pattern – If this purge operation is a routine maintenance operation that recurs on a scheduled basis, select the schedule operations in the Cleanup Recurrence Pattern section.

5. In the Cleanup Aging Threshold section, select the age of records before they can be purged.

6. In the Warehouse Records section, select the specific data sets to be purged.

The warehouse records include the following tables:

AddressBook	NGVersion
Alarm	NotificationSubscription
AlarmInterfaceChronicAlarmDowngrades	Performance
AlarmInterfaceChronicAlarmUpgrades	Query
Audit	Radio
Bolo	ReportNumbers
Chat	RSClientInformation
Config	RSEndpointAddress
ConfigAgency	ScheduleRecord
ConfigUdtApplications	Security
ContractorRotation	ServerInformation
Debug	StateInterface
Deployment	StatusMonitor
E911	StatusTimer
EntDevice	SuiteQueue
EntUnit	TDD
ESProvisioning	TestResult
Groups	Toning
IncidentManagement	TPS
License	UM
Login	UnmappedMigrationData
LSM	UR
ManualNotification	User
Messaging	UserSignOn
MobileSession	

7. Click **Save**.

   A summary of the purge operation appears on the General tab.

CHAPTER 31

Configuring Queries

The queries configuration item contains two tabs, for configuring queries at the Suite level and at the Agency level. These two tabs contain the following items:

- Suite Level Setting – Where you configure queries at the PremierOne Suite level.
- Agency Level Setting – Where you configure queries at the agency level.

NOTE
Microsoft Silverlight is a requirement for Query Response Formatting.

Queries Overview

The following diagram shows an overview of the system flow. A query request and subsequent response from a state system goes through different systems. CAD/Mobile sends the request to the query service, which passes it to the Common Services Interface (CSI). CSI is the layer that interfaces to external systems such as CommSys.

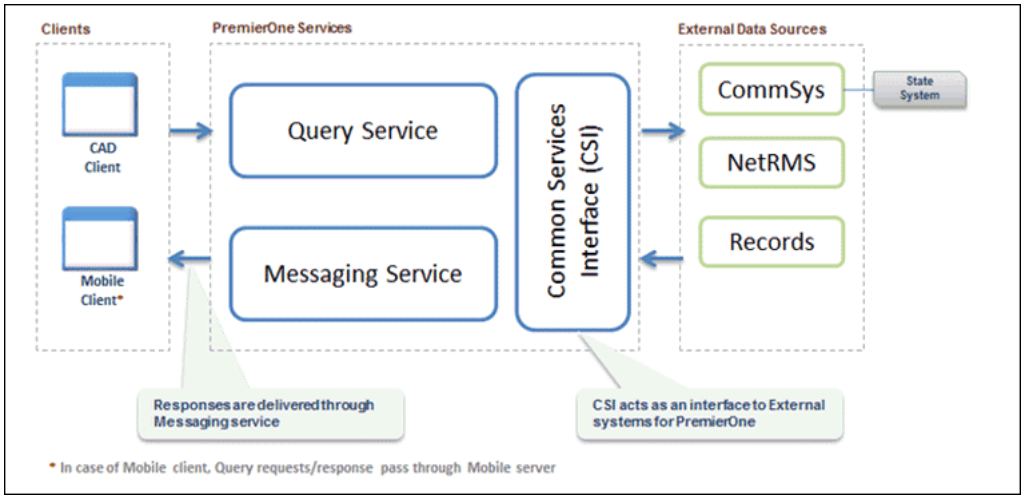


Figure 31-1 Queries System Overview

Importing Metadata

Metadata refers to information related to queries and fields that are imported into the system (such as queries supported by the state, request and response fields available for each query.) Metadata is in the form of an `xml` file which CommSys provides for a particular state.

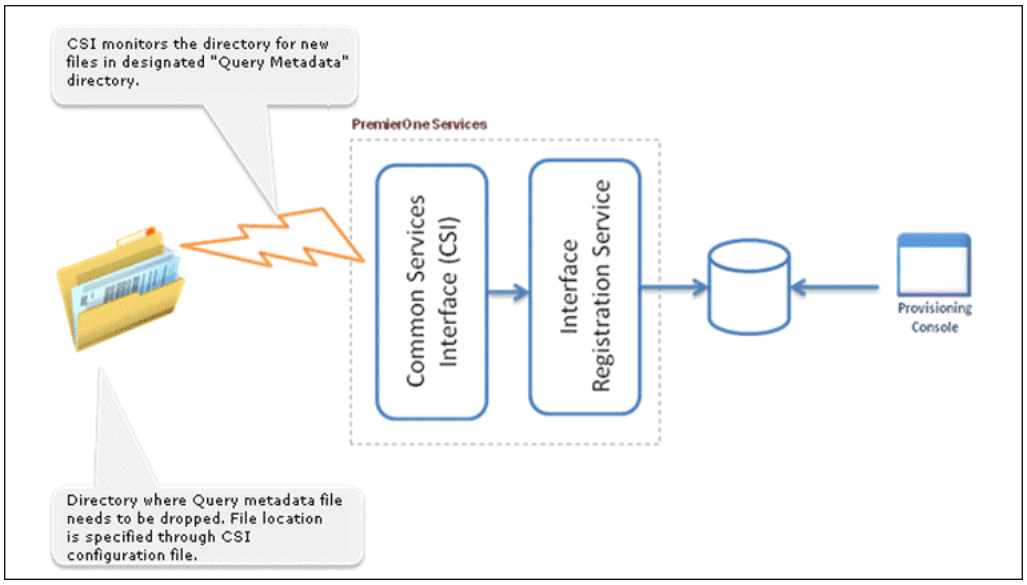


Figure 31-2 Flow of Metadata

NOTE

In the HA environment, CommSys and CSI will be running on multiple servers. In this case, metadata import can be done from any server.

To import metadata:

1. Verify the CSI Configuration

   a. Open the CSI Config tool and verify the connection string.

`ICS Connection` Verify `connectionString`	`/configuration/connectionStrings[1]/add[@name='ICS Connection']`

`InterfaceMetadataEntities` Verify `connectionString`	`/configuration/connectionStrings[1]/add[@name='InterfaceMetadataEntities']`

b. Use the CSI configuration tool to identify the directories used for the metadata import. The tool can be launched by double-clicking `CSIConfigTool.exe` in the Motorola\CSI folder. The directories used are found in the CommSys Metadata section of the tool. The tool may be used to update these directories if necessary.

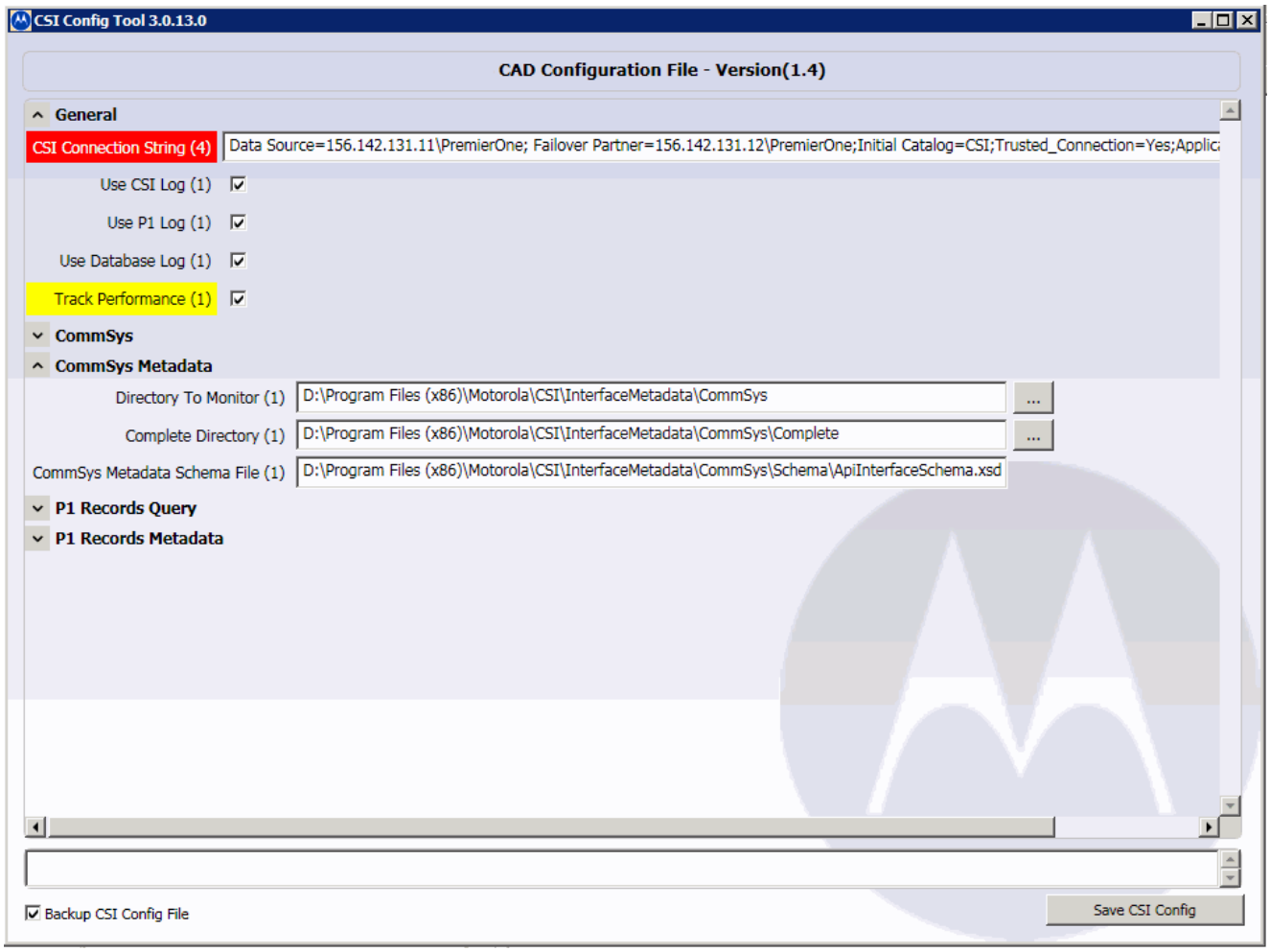


Figure 31-3 CSI Config Tool

c. Open the `CSIMasterService.exe.config` file and set the Commsys Interface state (state for which metadata is imported).

The `CSIMasterService.exe.config` file is located where common services and CSI are installed. The default location is: `C:\Program Files\Motorola\CSI`.

`Searchable string:` `CommSysInterfaceState`	`Change CommSysInterfaceState`	Example if state is Minnesota, set CommSysInterfaceState to 'MN' as shown below

```
  </ComponentGroup>
</Interface>
<!-- CommSys Metadata Components -->
<Interface Name="CommSysQueryMetadataManagementAdapter">
  <ComponentGroup Name="CommSysMetadata">
    <Settings>
      <Setting Name="Enabled_TF" DataType="Bool">True</Setting>
      <Setting Name="InterfaceName">Minnesota</Setting>
      <Setting Name="InterfaceDescription">Minnesota State System</Setting>
      <Setting Name="InterfaceProvider">CSI</Setting>
      <Setting Name="InterfaceEndpointAddress">http://localhost/Interfaces/CommSys</Setting>
    </Settings>
    <Component Name="DirectoryMonitor" ComponentID="MetadataManagement_CommSysDirectoryMonitor">
      <Setting Name="Enabled_TF" DataType="Bool">True</Setting>
      <Setting Name="AssemblyName">CSIFileAdapter</Setting>
      <Setting Name="ClassName">Motorola.PremierOne.CommonServices.Interfaces.DirectoryMonitor</Setting>
      <Setting Name="LoggingLevel" DataType="Int">2</Setting>
      <Setting Name="FileFilter">*.xml</Setting>
      <Setting Name="DirectoryToMonitor">C:\InterfaceMetadata\CommSys\</Setting>
      <Setting Name="ProcessIntervalSeconds" DataType="Int">30</Setting>
```

Figure 31-4 CommSys Metadata Components Showing State Setting

NOTE
The CSI service needs to be restarted if any settings/ location are changed in the config file.

2. Copy the metadata file for import.

   Copy the metadata file provided by CommSys to the `DirectoryToMonitor` location and verify that the file is automatically moved to the `CompleteMoveToDirectory` location (`Complete` folder) in 4-5 minutes.

NOTE
Ensure that the metadata file attribute is *not* "Read Only."

3. Verify successful metadata import in the Provisioning console.

   Open the Provisioning console and navigate to Queries > State Interface. Verify that the Interface drop-down list has the state entry you imported.

Updating Metadata

When metadata is already present, and if CommSys requires updating of the metadata, do the following:

1. Copy the metadata file into the `DirectoryToMonitor` folder as described in "Importing Metadata" on page 31-2.
2. Check for changes in the metadata, for example, if any queries or fields have been removed, make sure those fields/queries are deleted in case they are provisioned.
3. After importing, verify that updated fields/queries are displayed on the Provisioning console.

Metadata Import Errors

If metadata is not imported successfully, check the Application and Motorola CSI log in the Windows Event Viewer (Start > Run > eventvwr).

Common errors and checkpoints:

1. `DirectoryToMonitor` folder does not have write permissions.
2. `CommSysMetadataSchemaFile` is not copied in the specified location.
3. Right version of CSI configuration file is not present for CSI service.

Confirming the State Interface Setup

In the main Provisioning console, select Configuration, and then select `Query_Config xml`. The Agency block should appear and a connection ID should be created.

If the agency information does not appear, copy the existing block.

1. Copy `Agency` block under `Agency` and `ServiceMapping` block under `ServiceMappings`.

   ```
   <Agency>

   <AgencyName>AgencyName</AgencyName>

   <QueryCleanerInterval>15</QueryCleanerInterval>

   <DeletePendingQueryAfter>2</DeletePendingQueryAfter>

   </Agency>


   <ServiceMapping>

   <Connectionid>NameOfInterface(Eg.MICHIGAN)</
   Connectionid>

   <EndpointName>SystemIdentityStateInterfaceLocal</
   EndpointName>

   </ServiceMapping>
   ```

2. Change the `<DefaultReceiver>` in the config file to provisioned user ID.

   ```
   <DefaultReceiver>Alex@DC</DefaultReceiver>
   DefaultReceiver>Provisioned User</DefaultReceiver>
   ```

Configuring PremierOne Records Queries

You can provision queries of the PremierOne Records system just as you do queries of other databases. You can configure query types for querying locations, persons, vehicles, entities (property), and case numbers in PremierOne Records. You must create a unique query type for each type of record, and you must include "Records" as one of the selected interfaces for the query type. For details, see "Configuring Query Types" on page 31-15 and "Configuring Response Formats" on page 31-43.

NOTE

For executing any query against the Records interface, the OwnerID request field must be set to the value **All** in Query – Query Types – Form. If this is not provisioned, Records will not send response.

The OwnerID field must also be mapped in the Query – Agency – IM Settings window to a non-used IM field (for example, Misc). If this mapping is not done, the query will not be submitted.

Configuring Queries at the Suite Level

Use the Suite Level Setting tab to configure queries at the PremierOne suite, or system, level. The Suite Level Setting tab contains the following sub-tabs:

- Interfaces – Where you configure query interfaces at the suite level. For details, see "Configuring Interfaces for Queries at the Suite Level" on page 31-8.
- Query Settings – Where you configure the limits on the query response raw data size. For details, see "Configuring Query Response Settings" on page 31-10.
- Query Types – Where you define the information submitted in queries, such as vehicle, person, or gun query. For details, see "Configuring Query Types" on page 31-15.
- Query Types Mapping – Where you associate query types to agencies. For details, see "Configuring Query Types Mapping" on page 31-34.
- Watch Lists – Where you set the options for watch lists. A watch list is a specific kind of query where you specify one or more query types and fields plus a time frame and the number of occurrences that have to occur before it triggers an alert. For details, see "Configuring Watch Lists" on page 31-37.

- Response Format Designer – Where you configure the formatting for query responses in CAD and Mobile. For details, see “Configuring Response Formats” on page 31-43.
- Response Format Mapping – Where you associate query response formats to agencies. For details, see “Configuring Response Format Mapping” on page 31-49.
- Response Fields Mapping – Where you associate query response fields to the IM Vehicle and Person forms, and designate key fields for importing query responses. For details, see “Configuring Response Fields Mapping” on page 31-52.
- ALPR – Where you select the Query Type to run on an ALPR hit, and map the query to the appropriate query type field. For details, see “Configuring ALPR Automatic Queries” on page 31-54.
- Query 2-Factor Authentication – Where you enable required two-factor authentication for Mobile, Radio, and Handheld devices. For details, see “Configuring Query Two-Factor Authentication” on page 31-56.

Configuring Interfaces for Queries at the Suite Level

Use the Suite-Level Setting Interfaces tab to control whether the interface should cascade, whether to notify users of login failure, identify which users should receive unsolicited messages from the interface, and set the details, such as host name, retry time, queue name, and logon.

To configure interface settings:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then **Interfaces**.

   The Interfaces form appears with the Settings tab in focus. A list of existing interfaces displays on the left side of the form.

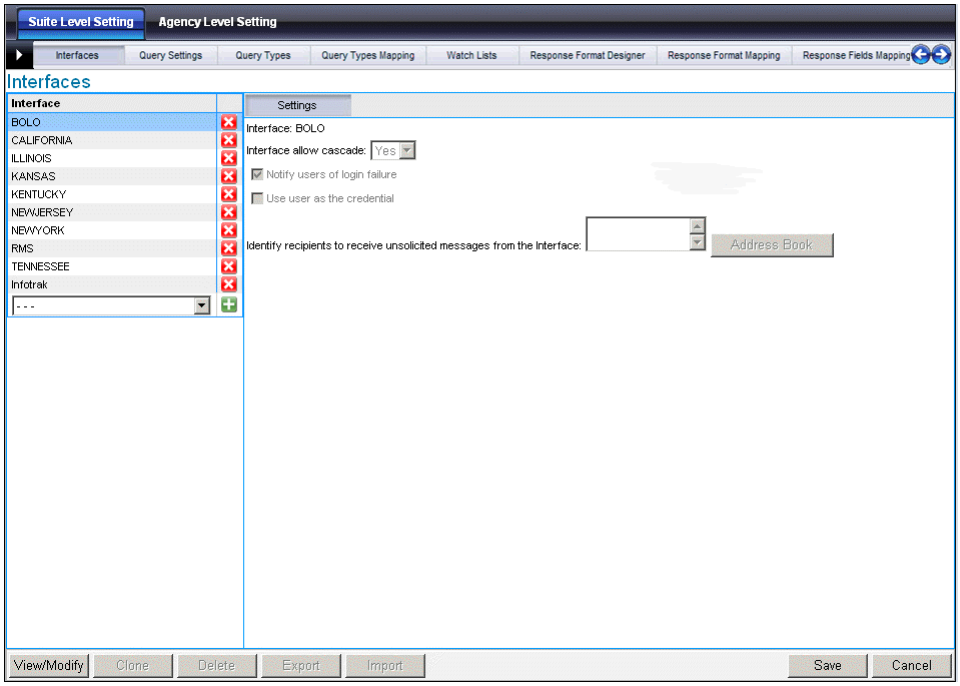


Figure 31-5 Suite Level Setting Form – Interfaces Tab

2. From the Interface list on the left side of the form, select the interface you want to configure settings for.

   If the state you need is not listed, scroll to the bottom of the list, and select the state from the drop-down list of states.

3. Click **View/Modify**.

4. From the Interface Allow Cascade list, select whether to allow cascading queries.

   Cascading queries means that one query can cause another query to be created. For example, if you run a vehicle query and it returns owner information, PremierOne can automatically create a license plate query against the owner information that was received.

5. To notify users when their login to the state database fails, select the Notify Users of login failure check box.

6. To use the PremierOne credentials for login, select the Use user as the credential check box.

7. To have specific recipients receive any unsolicited messages from the interface, click **Address Book** to the right of the Identify recipients to receive unsolicited messages from the interface label and select the users to notify.

   After you click **Save** from the Address Book dialog box, the users you selected appear in the box.

8. Click **Save**.

In Provisioning > Configuration > `Query_Config xml`, the Agency block should appear and a connection ID should be created. If the agency information does not appear, copy the existing block replacing `Agency` and `State` with the appropriate values:

```
<Agency>
<AgencyName>Agency</AgencyName>
<QueryCleanerInterval>15</ QueryCleanerInterval>
<DeletePendingQueryAfter>2</ DeletePendingQueryAfter>
</Agency>
<Connectionid>State</Connectionid>
<EndpointName>SystemIdentityStateInterfaceLocal</
EndpointName>
```

Configuring Query Response Settings

When PremierOne receives a query response from a state database, the raw data includes all the responses, and includes technical parameters such as headers, XML details, and so on. PremierOne parses the query responses so that required fields are clearly visible and identifiable. For example, PremierOne would parse the Person query response to display the Name, City, and License No fields. However, you may want to also see the actual raw data before the parsing mechanism is applied.

Use the Query Settings configuration item to limit the query response raw data size at the agency and device type levels. You can define a maximum raw data size for query responses, above which PremierOne truncates the raw data sent to agency users. You can also set individual limits for MDT and CAD client devices that override the agency limits for raw data response size.

If a query's raw data response size is greater than the provisioned limit, PremierOne truncates the response and displays a message to the CAD user indicating that the query response was truncated.

NOTES

The maximum response limit only applies to the CAD and Mobile client applications. PremierOnecaptures all raw data query responses without any truncation for auditing and reporting purposes.

If a query response includes any attachments, PremierOne truncates only the raw data response based on these settings. If necessary, attachments are truncated according to the values configured for message attachments. For details, see "Configuring General Agency Messaging Settings" on page 26-2.

When you configure query settings, you enter information on following tabs of the Query Settings form:

- Default Settings – Where you can choose to block raw data above a specified maximum query response raw data size, or to indicate that provisioned device type level settings for MDT and CAD clients should be used.
- Mobile Settings – Where you can set a maximum query response raw data size that is specific to MDT devices.
- CAD Settings – Where you can set a maximum query response raw data size that is specific to CAD devices.

Configuring Agency Default Query Settings

Use the Default Settings tab to set a maximum query response raw data size for all agency users, or to indicate that provisioned device type level settings for MDT and CAD clients should be used.

To configure agency default query settings:

1. From the navigation panel, select **Query**, then **Suite Level Setting**, and then **Query Settings**.

The Query Settings form appears with the Default Settings tab in focus.

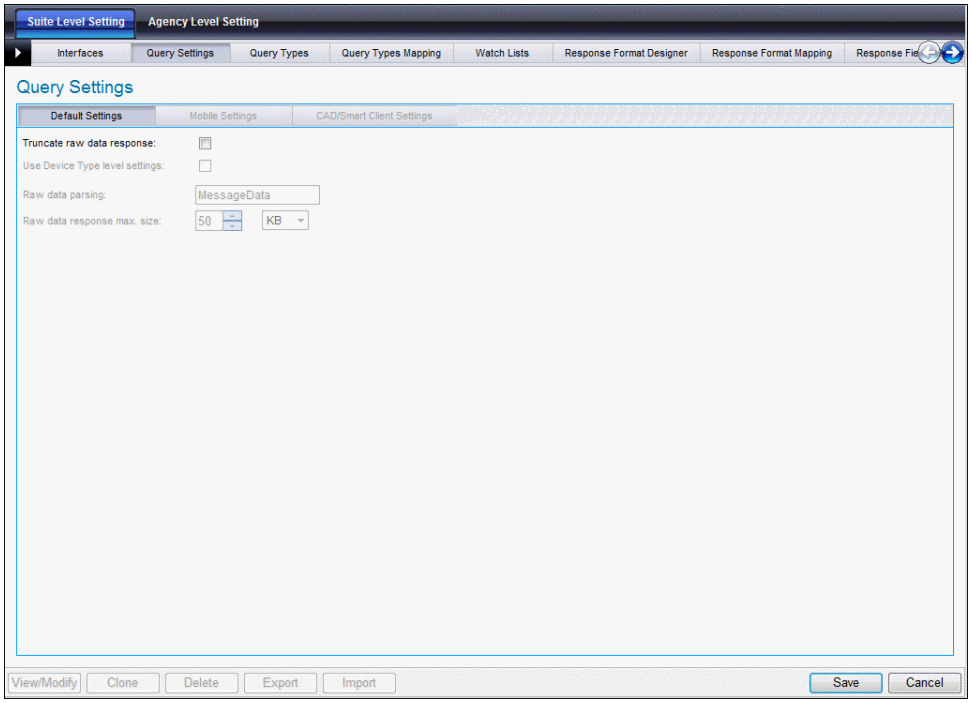


Figure 31-6 Query Settings Tab

2. Click **View/Modify**.

   The Truncate raw data response field becomes editable.

3. Select the **Truncate raw data response** check box.

   The remaining fields on the Default Settings tab become editable.

> **NOTE**
> If you do not select the Truncate raw data response check box, all raw data is sent with query responses.

4. In the Use Device Type level settings field, select the check box to set unique raw data response sizes for Mobile and CAD devices. For details on device type settings, see "Configuring Mobile Query Response Settings" on page 31-12 or "Configuring CAD/Smart Client Query Response Settings" on page 31-13.

   If you do not select this check box, then the agency default settings apply to all devices for the agency.

5. In the Raw data parsing field, type the name (variable) for parsing the raw data response sent from external systems, or leave the default value of `MessageData`.

6. In the Raw data response max. size field, indicate the raw data size limit for query responses by selecting a number and KB (Kilobytes) or MB (Megabytes) in the fields provided.

7. Click **Save**.

Configuring Mobile Query Response Settings

You can set a query response raw data size limit specific to mobile devices. This setting overrides the Default Settings.

To configure Mobile query settings, you must select the Block raw data in Query response and Use Device Type level settings check boxes on the Default Settings tab. For details, see "Configuring Agency Default Query Settings" on page 31-10.

To configure Mobile query settings:

1. Access the form for query settings. For instructions, see "Configuring Agency Default Query Settings" on page 31-10.

   The Query Settings form appears with the Default Settings subtab in focus (see Figure 31-6).

2. Click **View/Modify**.

   The Truncate raw data response check box becomes editable.

3. Select the **Truncate raw data response** check box.

   The remaining fields on the Default Settings tab become editable.

4. Select the **Use Device Type level settings** check box.

   The Mobile Settings and CAD/Smart Client Settings tabs become editable.

5. Select the **Mobile Settings** tab.

The Mobile Settings form appears.

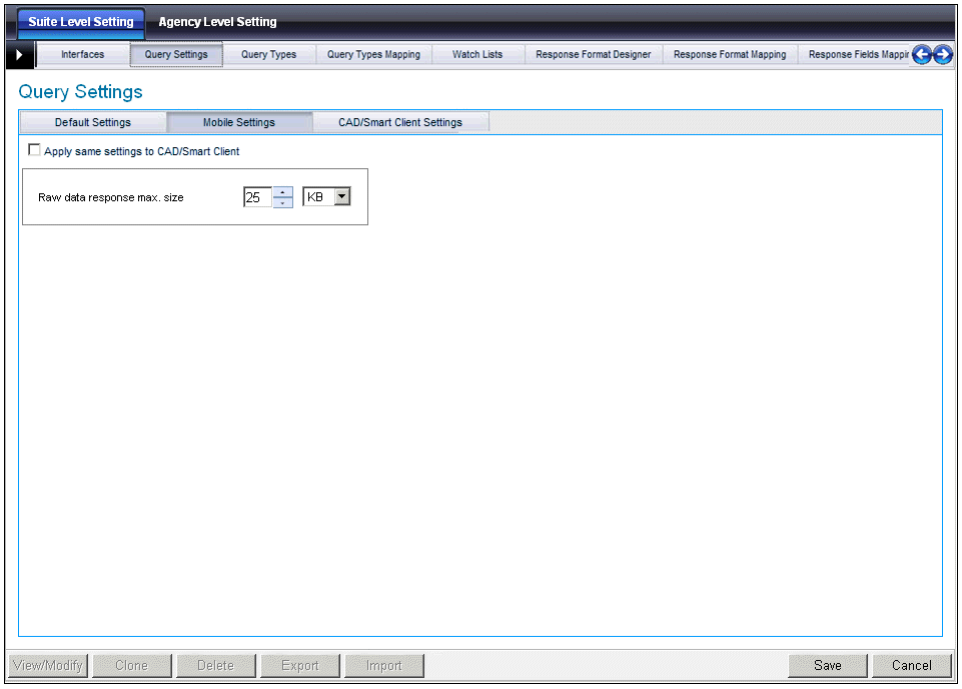


Figure 31-7 Mobile Settings Tab

6. To use the same raw data limit for CAD and Smart Client workstations that you set for Mobile clients, select the **Apply same settings to CAD/Smart Client** check box.

   To set a different limit for CAD and Smart Client workstations, see "Configuring CAD/Smart Client Query Response Settings" on page 31-13.

7. In the Raw data response max. size field, indicate the raw data size limits for query responses by selecting a number and KB (Kilobytes) or MB (Megabytes) in the fields provided.

   Any response information that exceeds this threshold is truncated.

8. Click **Save**.

Configuring CAD/Smart Client Query Response Settings

You can set a query response raw data size limit specific to CAD and Smart Client devices. This setting overrides the Default Settings.

To configure CAD/Smart Client query settings, you must select the **Block raw data in Query response** and **Use Device Type level settings** check boxes on the Default Settings tab. For details, see "Configuring Agency Default Query Settings" on page 31-10.

To configure CAD/Smart Client query settings:

1. Access the form for query settings. For instructions, see "Configuring Agency Default Query Settings" on page 31-10.

   The Query Settings form appears with the Default Settings subtab in focus (see Figure 31-6).

2. Select the CAD/Smart Client Settings tab.

   The CAD/Smart Client Settings tab appears.

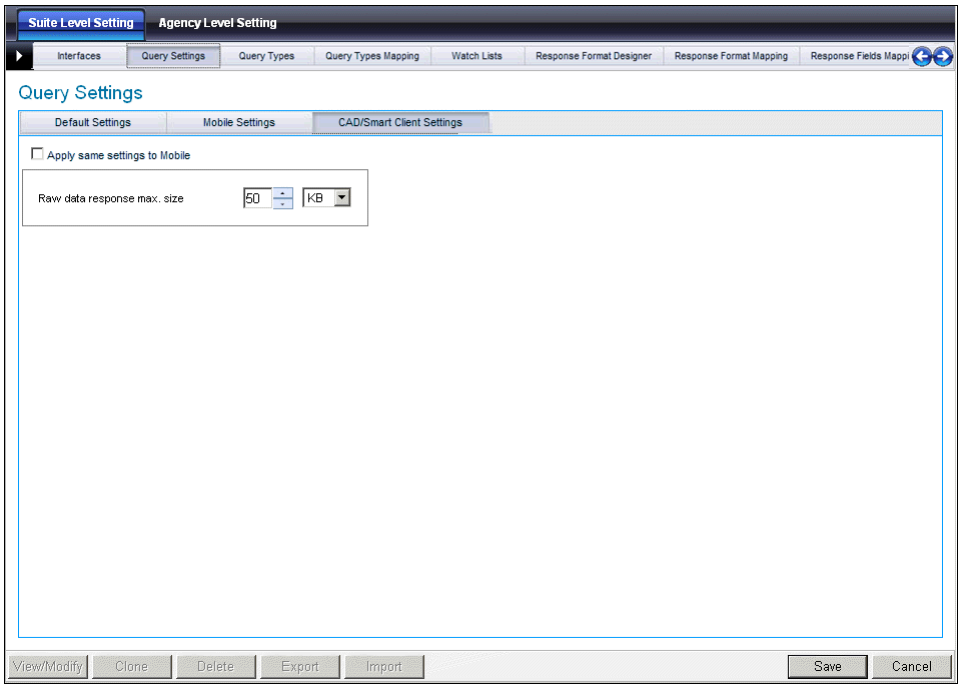


Figure 31-8 CAD Settings Tab

3. To use the same raw data limit for Mobile clients that you set for CAD/Smart Client workstations, select the **Apply same settings to Mobile** check box.

   To set a different limit for Mobile clients, see "Configuring Mobile Query Response Settings" on page 31-12.

4. In the Raw data response max. size field, indicate the raw data size limits for query responses by selecting a number and KB (Kilobytes) or MB (Megabytes) in the fields provided.

   Any response information that exceeds this threshold is truncated.

5. Click **Save**.

Configuring Query Types

Use the Query Types configuration setting to add and manage query types when the existing query types do not meet your needs. Query types define the information collected for submittal, such as vehicle, person, or gun query.

You can add, modify, clone, and delete query types. For details, see "Working With Configuration Items" on page 2-9.

NOTE

You must assign permissions for each query type to roles that you want to access queries. For details on roles, see "Configuring Roles" on page 8-2.

When you add a query type, you enter information on nine tabs of the Query types form:

- Settings – Where you enter the display name, select whether to include the query for Mobile and Handheld, configure the Mobile settings, select whether to consolidate the query responses and configure the consolidation settings, select whether additional user authorization is required, select whether to create an associated command line command, and select whether to notify the user of a successful database entry or update. For details, see "Adding Query Type Settings" on page 31-16.
- Interfaces – Where you identify which interfaces to query. For details, see "Adding Interfaces for Query Types" on page 31-18.
- Interface Fields – Where you identify which fields to include on the query form. For details, see "Adding Interface Fields for Query Types" on page 31-19.
- Form – Where you select whether the form will display in one or two columns, add new form fields, select form fields, and associate form fields with interfaces. For details, see "Adding Form Fields for Query Types" on page 31-20.
- Responses – Where you control the format and content of responses. For details, see "Adding Response Fields for Query Types" on page 31-24.
- Dups. – Where you identify duplicate fields in different interfaces. For details, see "Setting Up Duplicate Fields for Query Types" on page 31-27.
- Hot Hits – Where you define the fields and text in the responses that will trigger a hot hit and configure the processing for hot hits. For details, see "Adding Hot Hits for Query Types" on page 31-28.
- Casc. Queries – Where you configure the field or fields and text that will cause a cascading query, or a new query to be created. For details, see "Adding Cascading Queries for Query Types" on page 31-30.
- Drill Down – Where you select the fields in a query response that a user can click to populate a new query. For details, see "Adding Drill Down Information for Query Types" on page 31-33.

Adding Query Type Settings

Use the Settings tab of the Query Types window to configure the basic settings for the query type, such as the name of the query, whether the query is available to MDT units, and consolidation settings.

To add query type settings:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then **Query Types**.

   The Query Types form appears with the Settings tab in focus. A list of query types displays on the left side of the form.

   If you selected Existing in the filter, then a list of existing records displays. If you entered search criteria in the filter, only the matching records display.

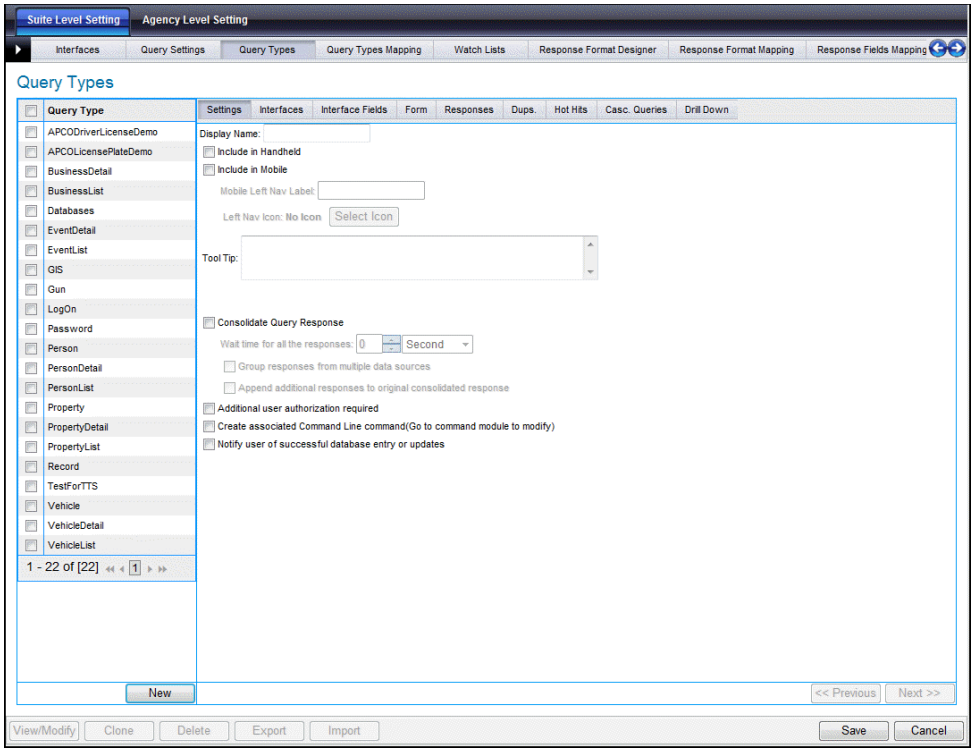


Figure 31-9 Query Types – Settings Tab

2. At the bottom of the Query Type list, click the **New** button.

3. In the Display Name field, type the name for the new query type, such as Vehicle or Person.

NOTE

PremierOne Handheld supports the following query types. You must use these names for Handheld queries to work properly:

– Article by Serial #
– Boat by Hull
– Gun Query
– Person by Drivers License
– Person by Name
– Vehicle by Plate
– Vehicle by VIN

4. To make the query available to handheld units, select the **Include in Handheld** check box.

5. To make the query available to Mobile units, select the **Include in Mobile** check box. If you do include the query type for Mobile, do the following:

   a. In the Mobile Left Nav Label field, type the name you want to appear in the left navigation area in Mobile.

   b. In the Left Nav Icon field, click **Select Icon**, and then navigate to the location where the icon you want to use for this query type is located.

   c. In the Tool Tip field, type the text for the tool tip that appears when a user hovers his or her mouse over the icon.

   d. In the Send copy of mobile responses to field, click **Address Book** to send a copy of query responses to a mobile client.

6. In the Consolidate Query Response field, select whether you want to consolidate all of the responses to the query. If you do consolidate the responses, do the following:

   a. In the Wait time for all the responses field, enter how long to wait and select whether that should be in seconds, minutes, hours, or days.

   b. In the Group responses from multiple data sources field, select whether to group the responses.

   c. In the Append additional responses to original consolidated response field, select whether to add the additional responses to the original response.

7. In the Additional user authorization required field, select whether additional user authorization is required.

8. In the Create associated Command Line command (Go to command module to modify) field, select whether to add a command identifier for this query type. You will need to go to the Command Line configuration item and modify the QY command (use one of the parameter identifiers).

   For details, see “Configuring Commands” on page 21-1.

9. In the Notify user of successful database entry or updates field, select whether to make the notification.

10. Click **Save**.

Adding Interfaces for Query Types

Use the Interface subtab of the Query Types tab to define the interfaces to be queried for the query type.

To add interfaces for a query type:

1. Open the form for Query Types.

   For details, see "Adding Query Type Settings" on page 31-16.

2. Select the Interfaces subtab for the query type.

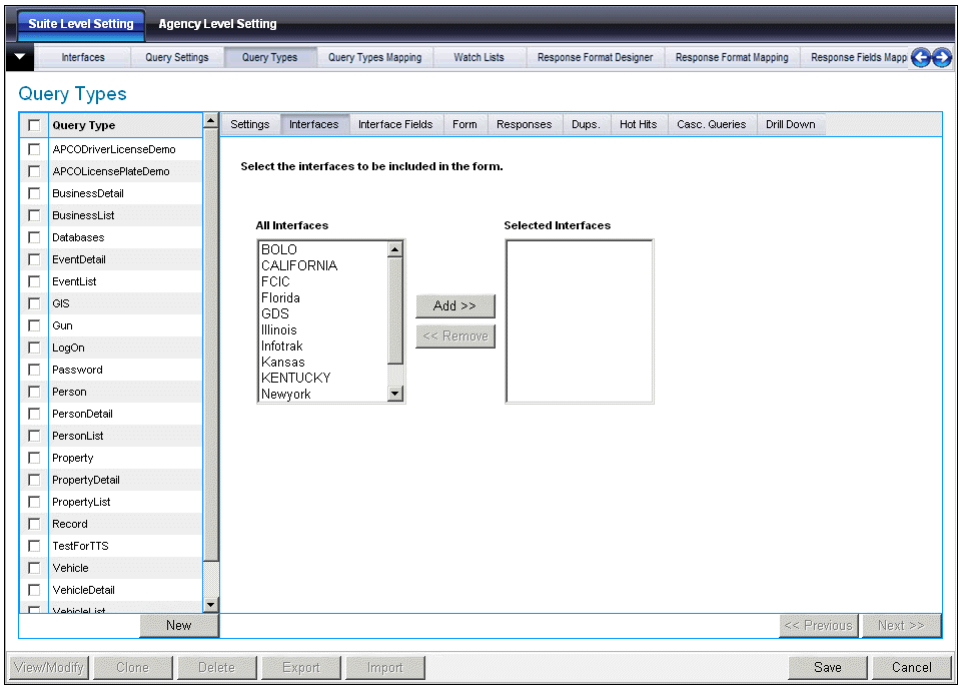


Figure 31-10 Query Types Form – Interfaces Tab

3. In the All Interfaces box, select the interfaces you want to be queried by the query type.

4. Click **Add**.

5. Click **Save**.

Adding Interface Fields for Query Types

Use the Interface Fields subtab of the Query Types tab to add the actual fields that will be used in the query. You can group related fields into query sets, such as vehicle information and person information.

To add interface fields for a query type:

1. Open the form for Query Types.

   For details, see “Adding Query Type Settings” on page 31-16.

2. Select the Interface Fields subtab for the query type.

   The Interfaces you added in the Interface tab appear in the Interface list.

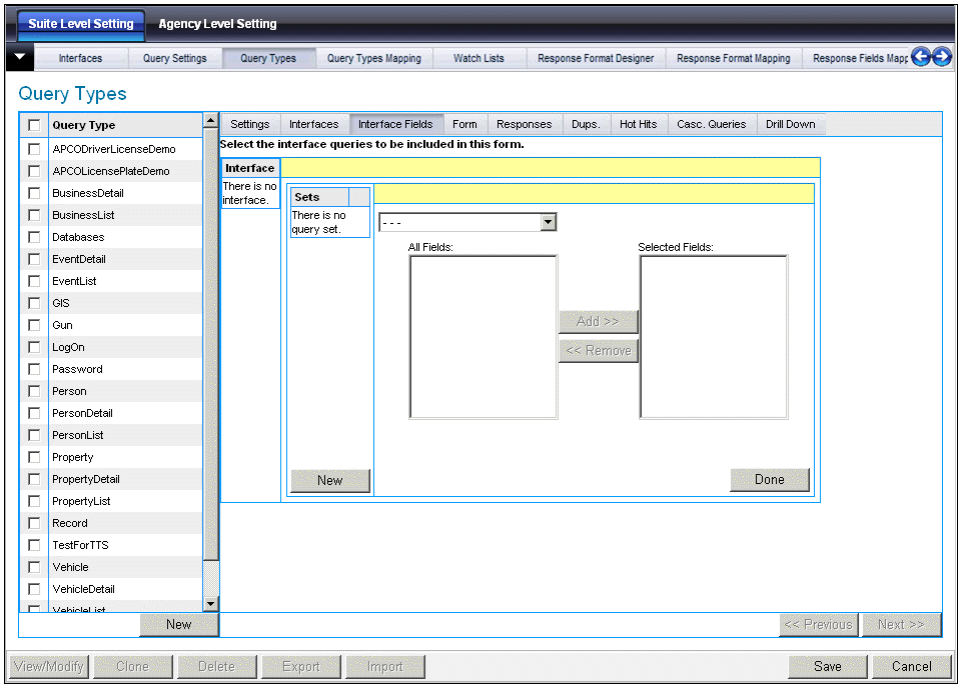


Figure 31-11 Query Types Form – Interface Fields Tab

3. From the Interface list, select the interface for which you want to select interface fields.

The label for the first field changes to the name of the interface you selected.

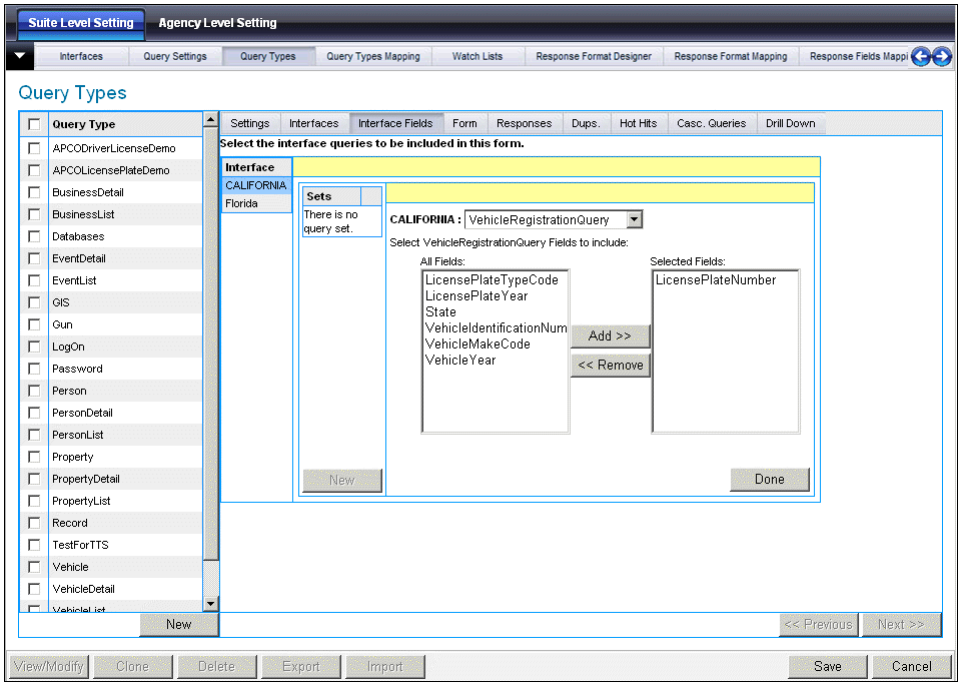


Figure 31-12 Selected Interface

4. In the first field, select a category, such as Vehicle.

   The fields for that category appear in the All Fields box.

5. From the All Fields list, select the fields to include in the query form. You can select more than one field by pressing the **Ctrl** key.

6. Click **Add**.

7. Click **Done**.

   You have now created a set of fields to include on the form that are all related to the category and the interface.

8. Click **Save**.

Adding Form Fields for Query Types

Use the Form subtab of the Query Types tab to add the fields that display on the query form, the fields that are actually submitted to the state interface, the field display label, and whether the fields are required and visible.

NOTE

For executing any query against the Records interface, the OwnerID request field must be set to the value **All**. If this is not provisioned, Records will not send response.

To add form fields for a query type:

1. Open the form for Query Types.

   For details, see “Adding Query Type Settings” on page 31-16.

2. Select the Form subtab for the query type.

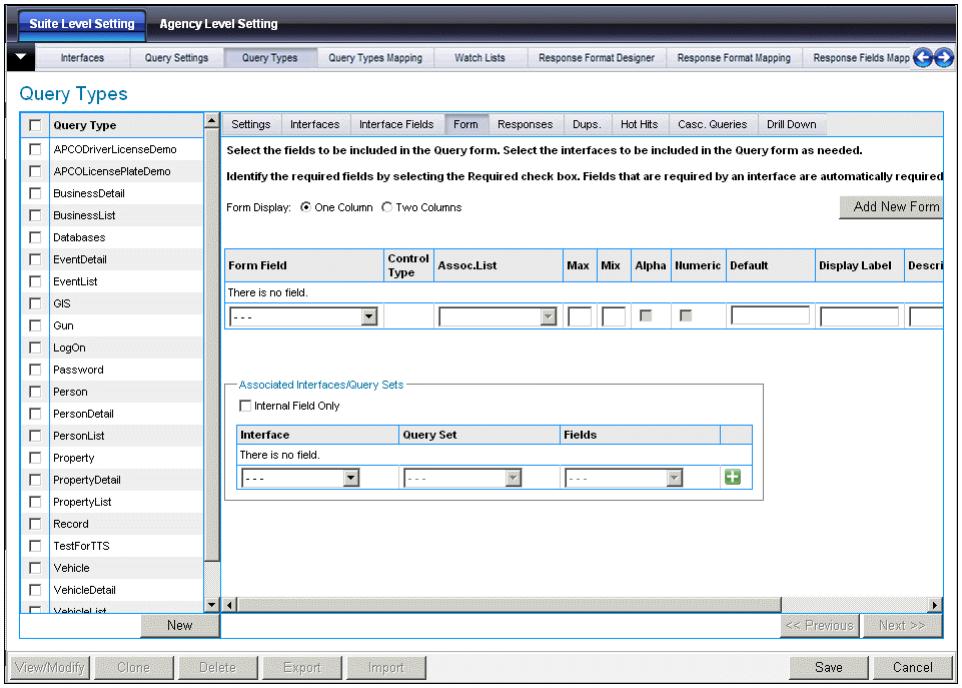


Figure 31-13 Query Types Form – Form Tab

3. Select whether you want the query form to display in one column or two.

4. Click **Add New Form Field(s)** to customize the form. You may want to select the Form Field list to see the available fields first.

The Add New Fields dialog box appears.

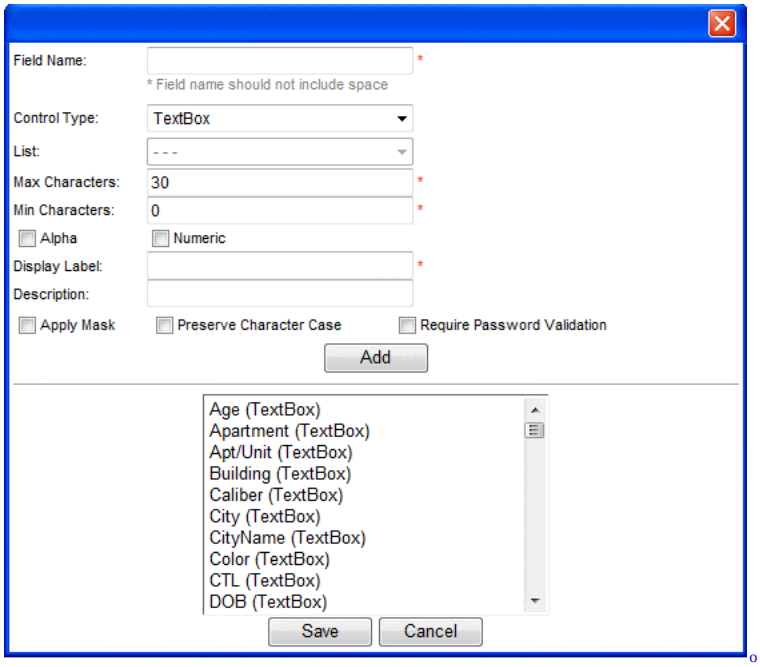


Figure 31-14 Add New Fields Dialog Box

a. n the Field Name field, type a name for the new field.

   Do not include spaces in the name.

b. In the Control Type field, select whether the field should be a TextBox or ListBox field.

   - If you select **TextBox**, the List field is disabled.

     In the Max Characters field, type the number of characters that will be the maximum allowable in the field.

     In the Min Characters field, type the number of characters that will be the minimum allowable in the field.

     To allow letter entries in the field, select the Alpha check box.

     To allow numeric entries in the field, select the Numeric check box.

   - If you select **ListBox**, the List field is enabled, and the Max Characters, Min Characters, Alpha, and Numeric fields are disabled.

     From the List list, select the name of the list from the LSM provisioning item with the values you want to appear in this list box.

c. In the Display Label field, type the field label you want to appear on the screen for the new field.

d. In the Description field, type a description of the purpose of the new field.

e. To hide the characters entered in this field, showing asterisks in their place, select **Apply Mask**.

f. To preserve the case (upper or lower) of the characters as they are entered, select **Preserve Character Case**.

g. To require password validation for the new field, select **Require Password Validation**.

h. Click **Add**.

The new field you added appears in the box at the bottom of the dialog box.

i. Click **Save** to save the new field and close the Add New Form Field(s) dialog box.

5. From the Form Field list, select the first field you want on the form from the drop-down list. The fields in the list are the ones you selected on the Interface Fields tab.

PremierOne automatically populates the Control Type, Validation/Assoc. List, Display Label, and Description fields. You can enter a default value in the Default field.

a. To require that a field be populated before the form can be submitted, select the **Required** check box.

b. To hide a field, clear the **Visible** check box.

The Visible check box determines whether the field displays on the form. Hidden fields could be identifying fields required by the interface, such as the Agency ID. Alternatively, an agency might track information in hidden fields for reporting purposes.

c. Click the plus icon to save the information and to add another row.

CAUTION
If you do not click the plus symbol, PremierOne does not save the form information, even after you click Save.

You can change the order of the fields by selecting a field and clicking **Move Up** or **Move Down**.

6. In the Associated Interfaces/Query Sets section, set up the interfaces to which the query sets are to be submitted.

a. Select the row field in the table at the top of the form by clicking the row.

The Form Field name displays at the top of the Associated Interfaces/Query Sets section.

b. If the field is an internal field only, select the **Internal Field Only** check box.

These fields will not be submitted to the interface and are usually used for internal reporting purposes.

c. From the Interface list, select the interface that the query was created for.

d. From the Query Set list, select the query set that you want submitted. These are created on the Interface Fields tab.

e. From the Fields list, select the field for submittal from that query set.

Click the plus at the end of the row to save the row and add another row.

CAUTION
If you do not click the plus symbol, PremierOne does not save the information in the row, even after you click Save.

7. Click **Save**.

Adding Response Fields for Query Types

Use the Responses subtab of the Query Types tab to configure the fields that you want to use to define rules (Hot Hit, Cascade, Drill Down) for the query type.

To define response fields for a query type:

1. Open the form for Query Types.

   For details, see “Adding Query Type Settings” on page 31-16.

2. Select the Responses subtab for the query type.

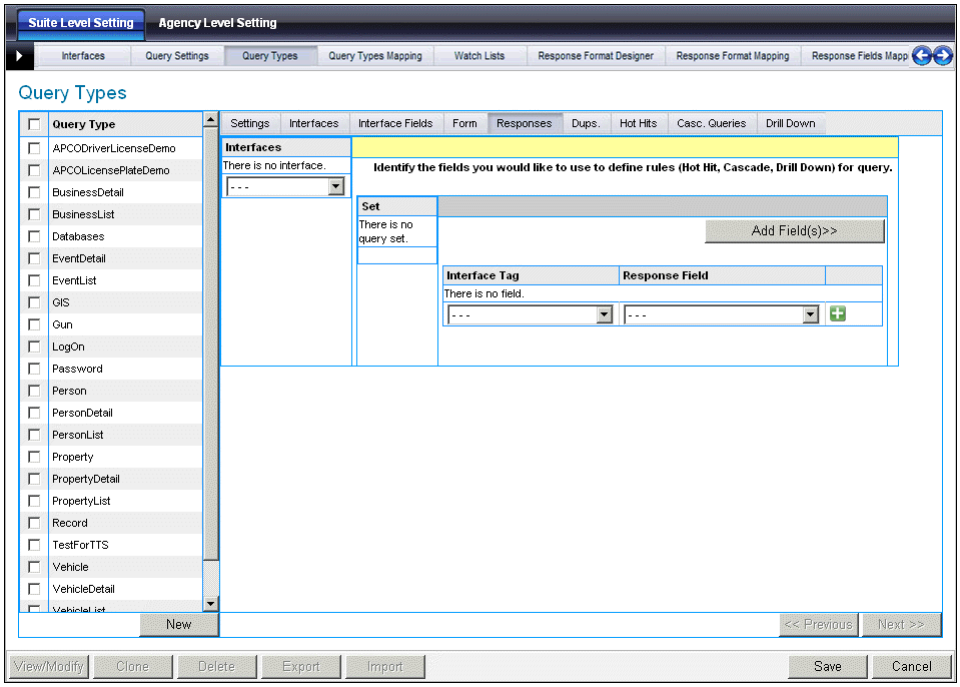


Figure 31-15 Query Types Form – Responses Tab

3. From the Interfaces list, select the interface you want to map first.

   If the interface you need is not shown, click the down arrow in the blank field, and then select the interface from the list.

4. From the Set list, select the set of fields you want to define the query responses for.

   The set fields are defined on the Interface Fields tab. For more information, see “Adding Interface Fields for Query Types” on page 31-19.

5. To customize the form, click **Add Field(s)**. You may want to click the arrow in the Interface Tag field to see the available fields first.

The Add New Responses Fields dialog box appears.

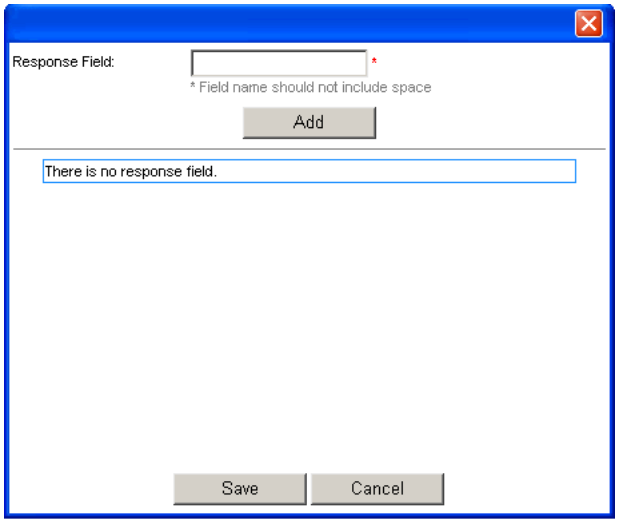


Figure 31-16 Add New Responses Fields Dialog Box

a. Enter information in the Response Field field.

b. Click **Add**.

The field you added appears in the area at the bottom of the dialog box.

c. Click **Save**.

6. Identify the fields you want to display in the response.

a. From the Interface Tag list, select the first field for the response form.

b. In the Display Label field, type the label as you want it to appear on the form.

c. In the Description field, type a description for the field.

d. Select whether you want the field to appear in bold text.

e. Select whether the field is a summary field.

Summary fields display more than one piece of response information.

f. Click the plus symbol at the end of the row to save the information in the row and to add another row.

CAUTION
If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

7. Click **Save**.

Setting Up Duplicate Fields for Query Types

Use the Dups subtab of the Query Types tab to add the fields that may have different names in different interfaces, but return the same information, such as PersonLastName and Last_Name.

To add duplicate fields for a query type:

1. Open the form for Query Types.

   For details, see "Adding Query Type Settings" on page 31-16.

2. Select the Dups. subtab for the query type.

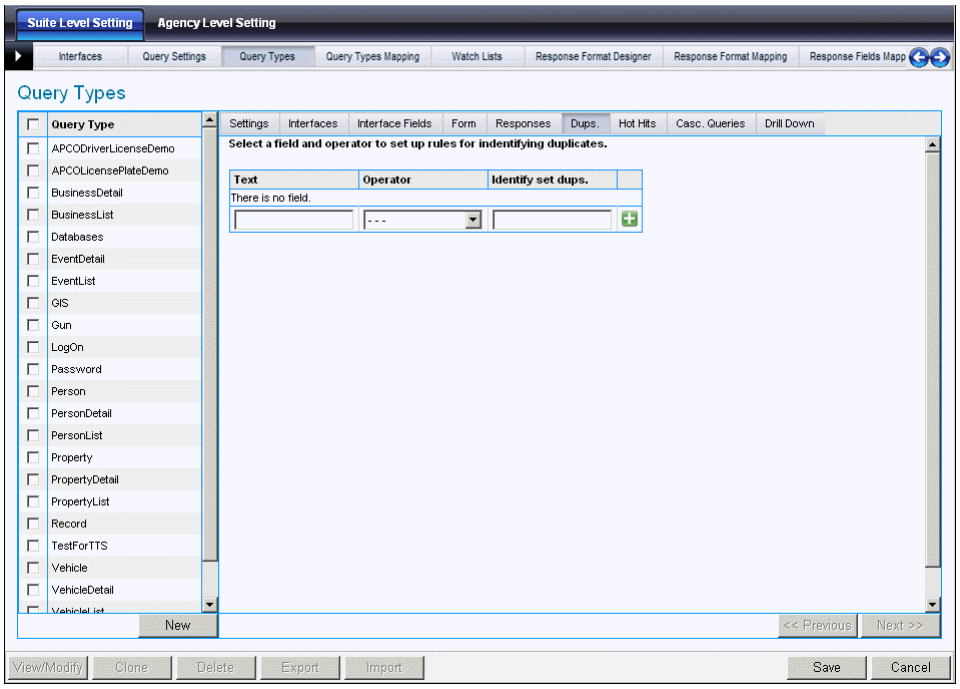


Figure 31-17 Query Types Form – Dups Tab

3. In the Text field, type the name of the first field in the duplicate pair, such as PersonLastName.

4. In the Operator field, select the operator, **And** or **Or**.

5. In the Identify set dups. field, type the name of the second field in the duplicate pair, such as Last_Name.

   Click the plus icon to save the pair and to add another row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the duplicate pair, even after you click Save.

6. Click **Save**.

Adding Hot Hits for Query Types

Use the Hot Hits subtab of the Query Types tab to add hot hits, keywords that occur in a query response, such as WANTED. The hot hit response triggers a notification message and an optional alarm.

Hot hits rules configured for query types override hot hits configured at the interface level. For details, see “Configuring Interface Hot Hit Settings at the Agency Level” on page 31-61. Query type hot hit rules can override or be combined with Interface hot hit rules.

For more information about hot hit rules, see “Hot Hit Examples” on page 31-61.

To add hot hits for a query type:

1. Open the form for Query Types.

   For details, see “Adding Query Type Settings” on page 31-16.

2. Select the Hot Hits subtab for the query type.

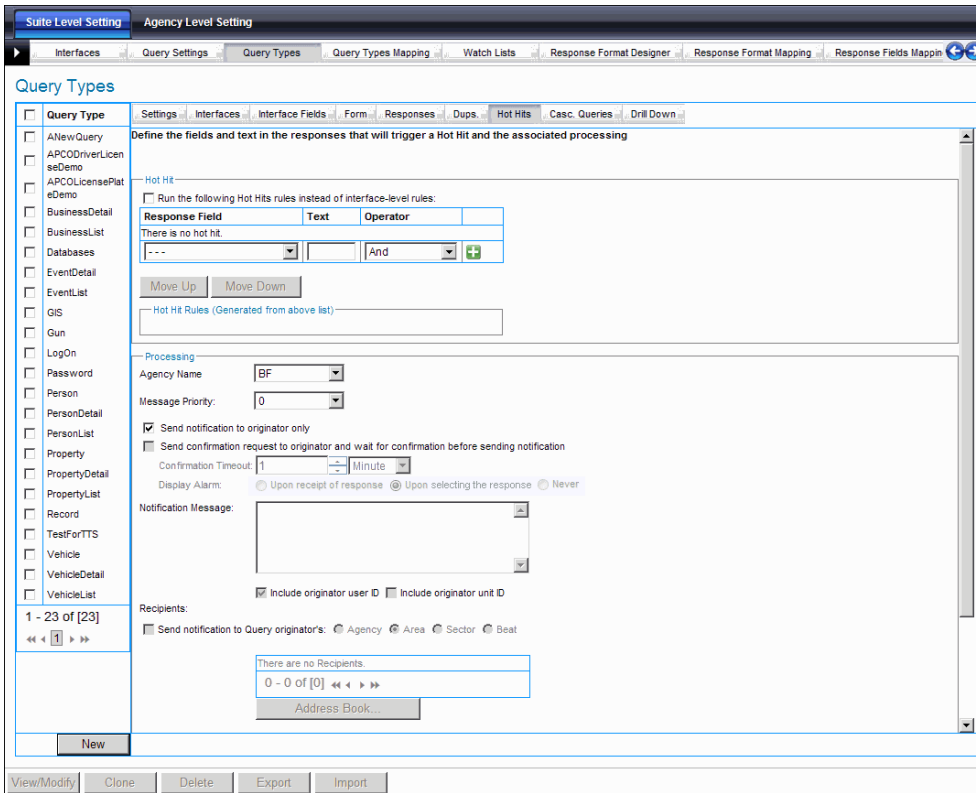


Figure 31-18 Query Types Form – Hot Hits Tab

3. From the Query Type list on the left, select the query type you want to modify, if it is not already selected, and then click **View/Modify**.

4. Select the Run the following Hot Hits rules instead of Interface level rules check box to allow the user to run the Query Type hot hits rules instead of the Interface level settings.

   To run the Query Type hot hits rules combined with the Interface level rules, leave the Run the following Hot Hits rules instead of Interface level rules unchecked.

5. In the Response Field field, select a field with the value to use as the keyword for the hot hit.

6. In the Text field, type the text for the keyword.

   Example:

   If your response field is LIC (license), your keyword in the Text field could be 123ABC, the license number of a vehicle involved in an Amber alert.

7. Click the plus symbol at the end of the row to save the row and add a new row.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the information in the row, even after you click Save.

8. To change the order of the rows, select the row you want to move and then use the **Move Up** and **Move Down** buttons to reposition the selected row.

9. To modify a row, select the row to make its fields editable and then make the desired changes.

10. To delete a rule, select the row and then click the **X** at the end of the row to remove it.

11. In the Hot Hit Rules (Generated from above list) section, the rules you created are summarized.

    Refer to this section to confirm that your Hot Hit rules are set up correctly.

12. In the Processing section, configure how you want to handle the processing for the hot hit.

    a. From the Agency Name list, select the agency to send a message to.

    b. In the Message Priority field, assign a priority to the notification message.

    c. Select one of the following:

    - To only send the notification to the originator, select the **Send notification to originator only** check box.
    - To send a confirmation request to the originator and wait for a confirmation message before sending a notification, select the **Send confirmation request to originator and wait for confirmation before sending notification** check box.

d. In the Confirmation Timeout field, enter the number and the units, such as minutes, hours, or days.

e. In the Display Alarm field, indicate when to display a hot hit notification *for the originator only* by selecting one of the following:

- **Upon receipt of response**: The hot hit confirmation dialog box displays when the query response is received.
- **Upon selecting the response**: The hot hit confirmation dialog box displays when the query response is selected in the Work Assist Area.
- **Never**: The hot hit confirmation dialog box does not automatically display. The user needs to click the Hot Hit button to display the confirmation dialog box.

f. In the Notification Message box, type the message that you want sent when this hot hit is triggered. Then select whether you want to **Include originator user ID** or **Include originator unit ID**.

g. To send notifications only to logged in users from the Provisioned user list, select the **Send notification to logged in users only** check box.

h. To send a notification to the Query originator's Agency, Area, Sector, or Beat select the **Send notification to Query originator's** check box and then select the appropriate option.

i. To select the recipients, click the **Select Destinations to Notify** button and select the users to whom you want the hot hit notification message sent.

13. Click **Save**.

Adding Cascading Queries for Query Types

Use the Casc Queries subtab of the Query Types tab to add cascading queries, queries which are triggered based on the response received from a previous query. For example, if you run a vehicle query against a license plate and the query returns the vehicle owner information, PremierOne then automatically creates a person query against the owner information. Thus, the query cascades from the vehicle query to the owner query.

To add cascading queries for a query type:

1. Open the form for Query Types.

   For details, see "Adding Query Type Settings" on page 31-16.

2. Select the Casc. Queries subtab for the query type.

   The Cascade Queries form appears, with the Cascade Trigger subtab in focus.

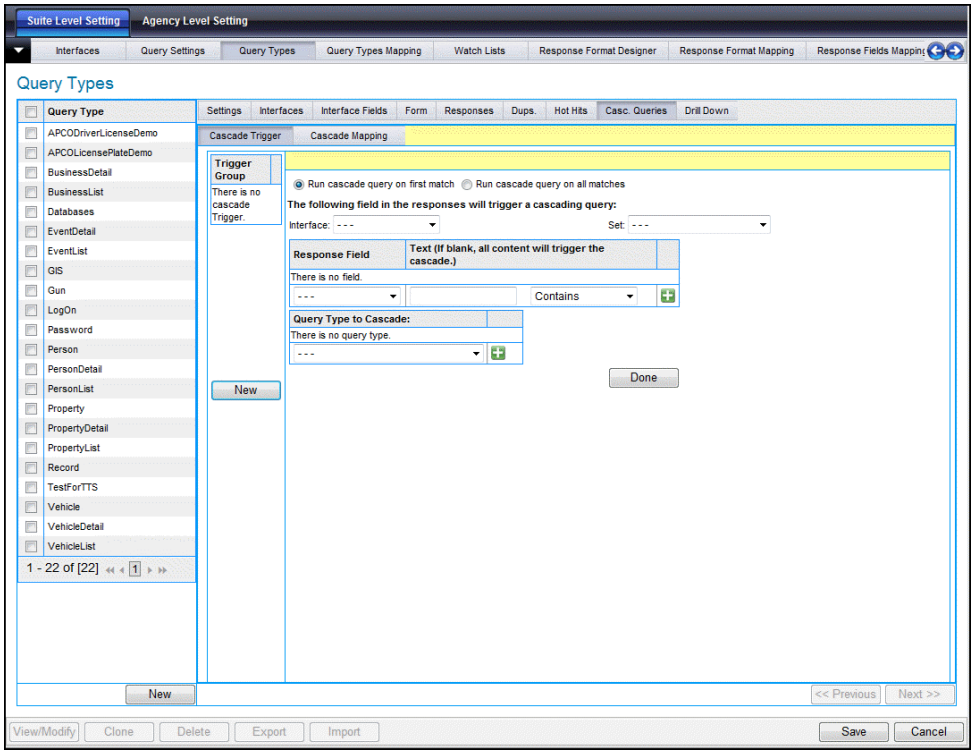


Figure 31-19 Query Types: Casc. Queries Tab

3. To run a query only on the first match of a multiple match response, select **Run cascade query on first match**.

4. To run a query on all matches of a multiple match response, select **Run cascade query on all matches**.

NOTE

Selecting Run cascade query on all matches may result in a large number of cascade queries being triggered for multiple response data, which can cause performance issues for PremierOne. Before enabling the Run cascade query on all matches configuration, Motorola Solutions recommends that you evaluate the quantity of cascade query hits and its impact on performance.

---

5. In the Interface field, select the interface from which you will select a field to trigger the cascading query.

6. In the Set field, select the set from which you will select a field to trigger the cascading query. The sets are defined on the Interface Fields tab. For more information, see “Adding Interface Fields for Query Types” on page 31-19.

7. In the Response Field field, select the field with the value that will trigger the cascading query.

8. In the Text field, type the value that will trigger the cascading query. If you leave the Text field blank, the presence of the field, regardless of value, will trigger the cascading query.

   In the next field, select **Contains** or **Does not contain**.

   Click the plus symbol at the end of the row to save the information in the row and add another row.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

9. In the Query Type to Cascade field, select the query type for the cascading query.

   Click the plus symbol at the end of the row to save the information in the row and add another row.

   CAUTION
   If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

10. Click **Done**.

    A trigger set appears in the Trigger Group list on the left.

11. Click the Cascade Mapping subtab.

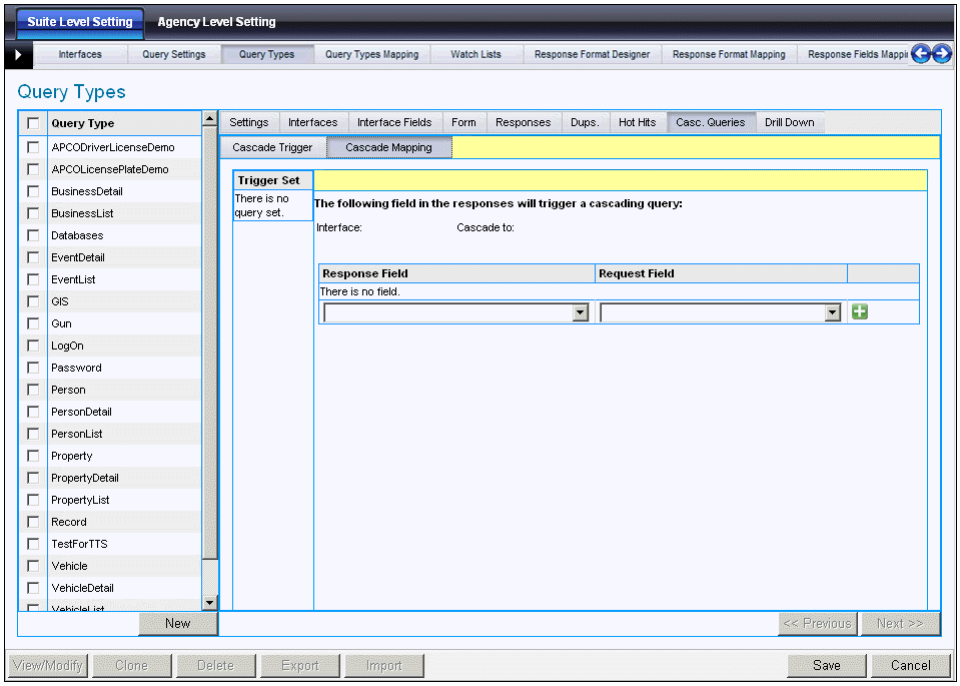


Figure 31-20 Query Types Form – Casc. Queries Cascade Mapping Form

12. From the Trigger Set list, select the set you want to view.

    The form shows the mapping you performed on the Cascade Trigger tab.

13. Click **Save**.

Adding Drill Down Information for Query Types

Use the Drill Down subtab of the Query Types tab to map associated queries for fields that a user can click on to populate a new query.

To add drill down information for a query type:

1. Open the form for Query Types.

   For details, see "Adding Query Type Settings" on page 31-16.

2. Select the Drill Down subtab for the query type.

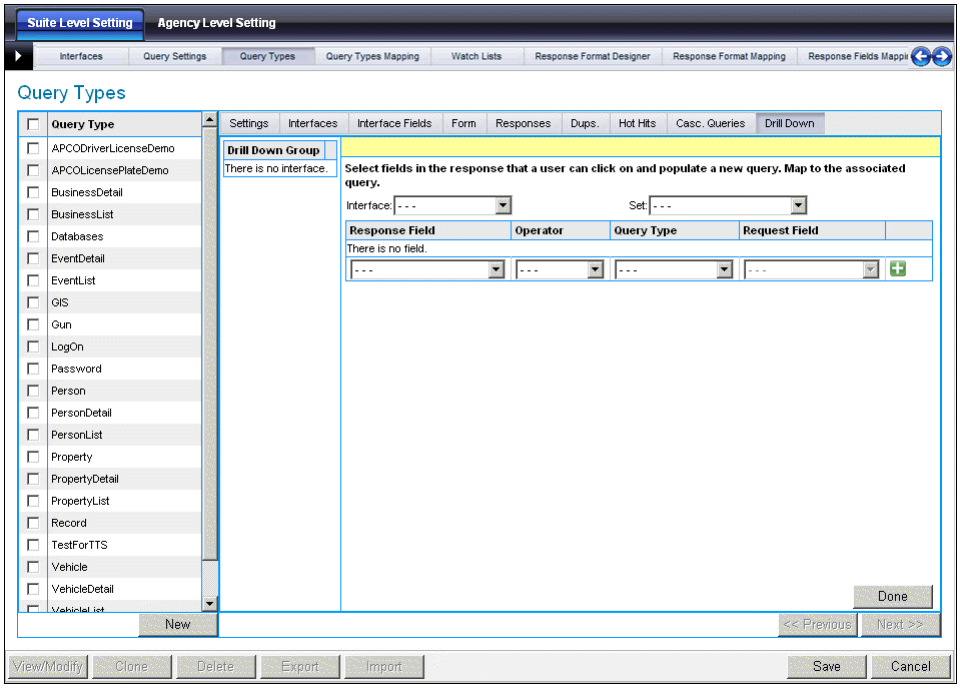


Figure 31-21 Query Types Form – Drill Down Tab

3. From the Query Type list on the left, select the query type you want to modify, if it is not already selected, and then click **View/Modify**.

4. From the Drill Down Group list, select the interface with which you want to work.

5. In the Interface field, select the interface from which you will select a field a user can click to populate a new query.

6. In the Set field, select the set of questions from which you will select a field a user can click to populate a new query.

7. In the Response Field field, select the field a user can click to populate a new query.
8. In the Operator field, select **And** or **Or**.
9. In the Query Type field, select the query type for the new query.
10. In the Request Field field, select the field from the new query type for the new query.
11. Click the plus symbol to the right of the row to save the information in the row and to add a new line.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

12. Click **Done**.
13. Click **Save**.

Configuring Query Types Mapping

Use the Query Types Mapping tab to associate query types to agencies. You can choose to map by query type, or by agency.

To map query types to agencies:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then **Query Types Mapping**.

The Query Types Mapping screen appears.

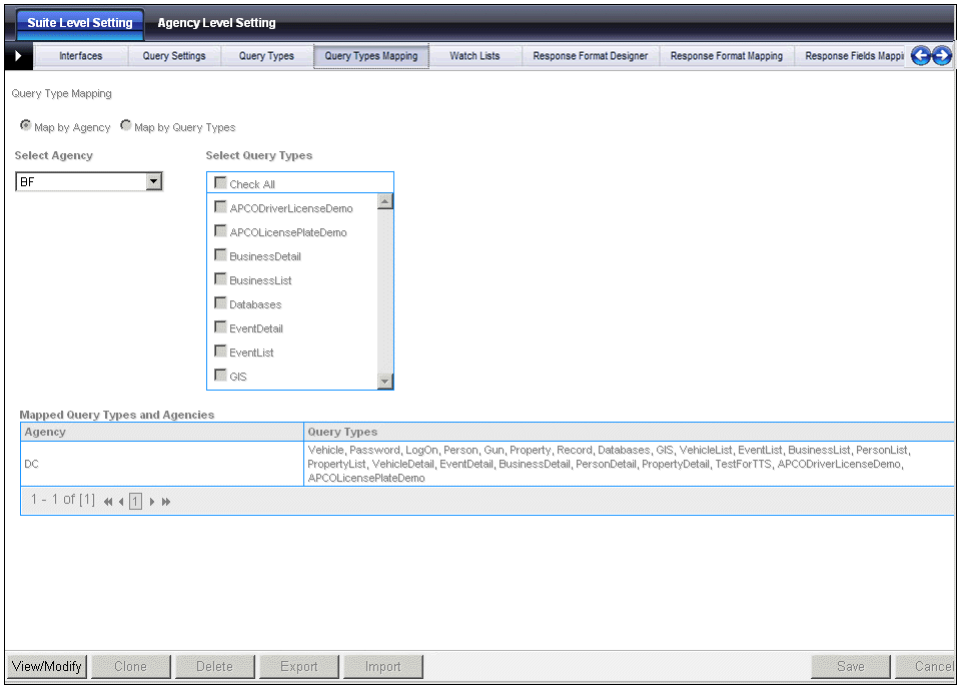


Figure 31-22 Query Types Mapping Tab

2. Click **View/Modify**.

   The Query Types Mapping screen refreshes.

3. Do one of the following:

   a. Select Map by Agency to assign query types to a particular agency.

   b. Select Map by Query Types to assign a particular query type to one or more agencies.

Mapping Query Types by Agency

To map query types by agency:

1. Navigate to the Query Types Mapping screen as described in “Configuring Query Types Mapping” on page 31-34.

2. Select **Map by Agency**.

The Query Type Mapping screen refreshes. Existing mapped query types and agencies appear at the bottom of the screen.

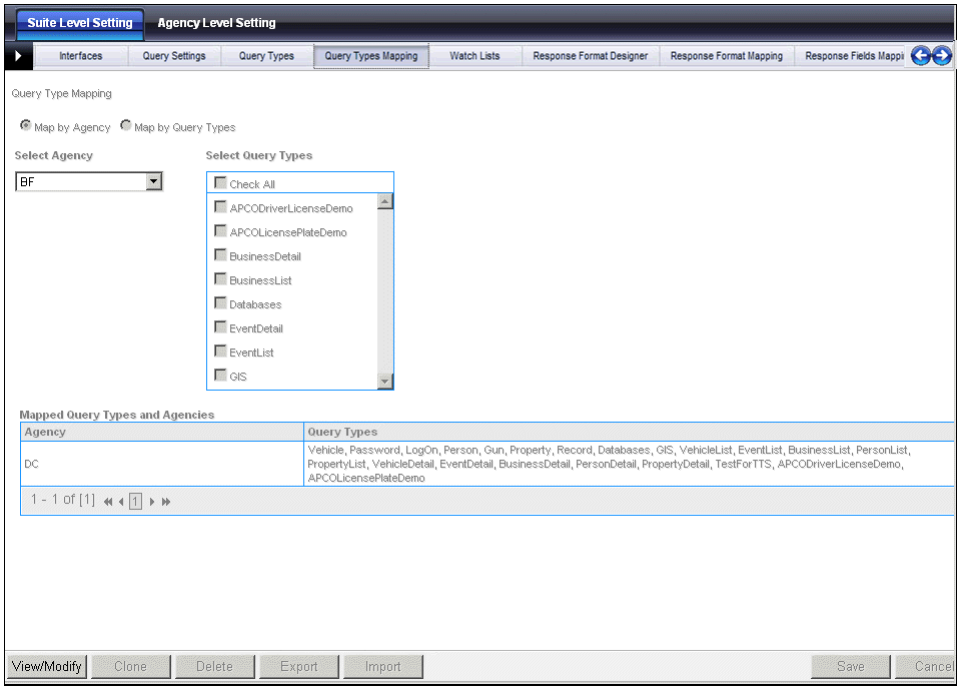


Figure 31-23 Query Type Mapping by Agency Screen

3. From the Select Agency list, select the agency to which you want to map query types.

4. In the Select Query Types list, select the query types that you want to map to the selected agency.

5. Click **Save**.

Mapping Query Types by Query Type

To map query types by query type:

1. Navigate to the Query Types Mapping page as described in "Configuring Query Types Mapping" on page 31-34.

2. Select **Map by Query Types**.

The Query Type Mapping screen refreshes. Existing mapped query types and agencies appear at the bottom of the screen.

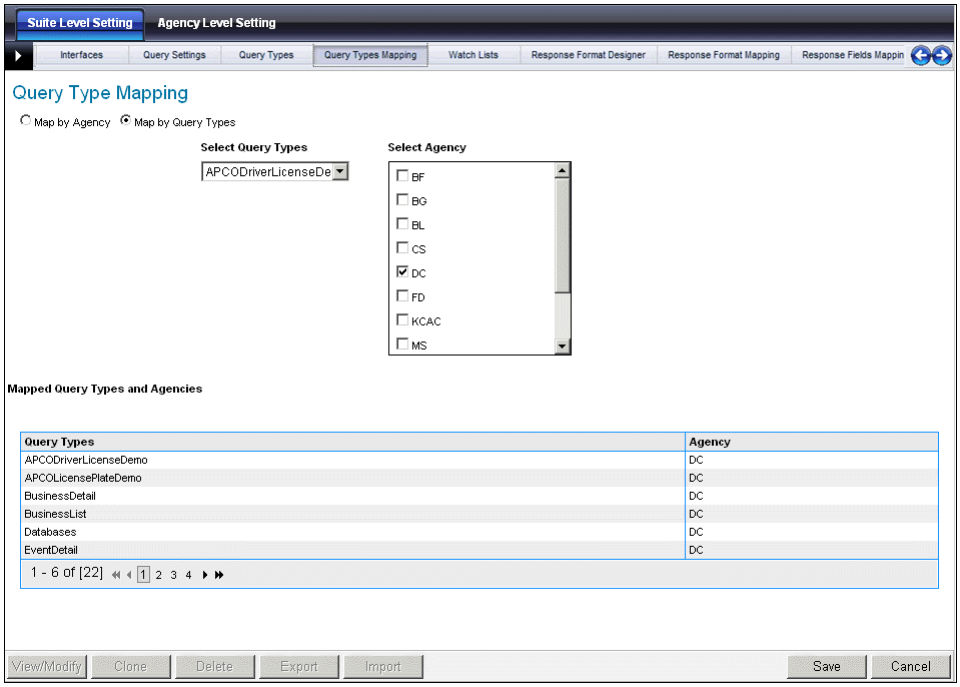


Figure 31-24 Query Types Mapping by Query Type Screen

3. From the Select Query Types list, select the query type you want to map.

4. In the Select Agency list, select the agencies to which you want to map the selected query type, or select **Check All** to select all agencies.

   Repeat for all query types you want to map.

5. Click **Save**.

Configuring Watch Lists

Use the Watch Lists configuration setting to set options for watch lists. A watch list is a specific kind of query where you specify one or more query types and fields plus a time frame and the number of occurrences that the text has to occur before it triggers an alert. You also set an alert priority and create an alert message to be sent to selected recipients.

For example, you could create a license plate query for a specific license plate. If a query on the same plate is run over the defined number of occurrences within a short time period, that could indicate some involvement in criminal activity.

You can add, modify, clone, and delete watch lists. For details on cloning and deleting, see “Working With Configuration Items” on page 2-9.

Adding Watch Lists

Add a watch list when the existing watch lists do not meet your needs. When you add a watch list, you enter information on three tabs of the Query types form:

- Settings – Where your define the watch list name, size limitations, and system generated settings.
- Freq List – Where you determine how often to check for queries (frequency) and over what time period (time frame).
- Exclude List – Where you exclude any entries that you do not want to have monitored for repetitive search activity.

Adding Watch List Settings

Watch list settings include the watch list name, size limitations, and the system-generated watch list settings.

To add watch list settings:

1. From the navigation panel, select **Query**, and then select **Watch Lists**.

   The Watch Lists form appears with the Settings tab in focus. A list of existing watch lists appears on the left side of the form.

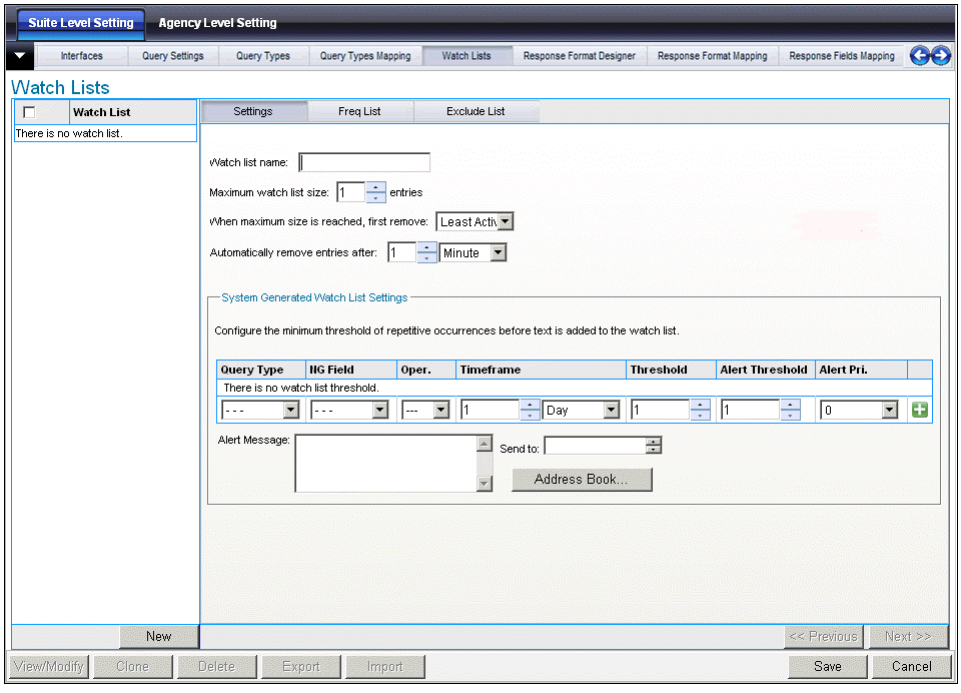


Figure 31-25 Watch Lists Form – Settings Tab

2. At the bottom of the Watch List list, click **New**.
3. In the Watch list name field, type a name for the new watch list.

4. From the Maximum watch list size list, select the maximum number of entries that can be in the watch list.

5. From the When maximum size is reached list, select which entries to remove when the maximum size is reached.

6. From the Automatically Remove Entries list, select when to automatically remove entries.

7. In the System Generated Watch List settings section, configure the settings for system-generated watch lists.

   a. From the Query Type list, select a query type.

   b. From the NG Field list, select a field.

   c. From the Oper. list, select an operator, if needed.

   d. From the Timeframe list, select the time frame.

   e. From the Threshold list, select the minimum number of times the same information must occur in query requests to trigger the watch list.

   f. From the Alert Threshold list, select the number of times the same information must occur in query requests to cause an alert message to be sent.

   g. From the Alert Pri. list, select the priority of the alert message.

      Click the plus symbol at the end of the row to save the information in the row and add another row.

      CAUTION
      If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

   h. In the Alert Message Details field, type the text for the alert message you want to send when the alert threshold is met.

   i. In the Send to field, use the address book to select the recipients of the alert message.

8. Click **Save**.

Adding Frequency Settings for Watch Lists

Add the frequency settings for system generated watch lists on the Settings tab. Add the frequency settings for non-system generated watch lists on the Freq List tab.

To add frequency settings for non-system generated watch lists:

1. Access the form for new watch lists. For instructions, see "Adding Watch List Settings" on page 31-38.

   The Watch Lists form appears with the Settings tab in focus (see Figure 31-25). A list of existing watch lists appears on the left side of the form.

2. Select the Freq List tab.

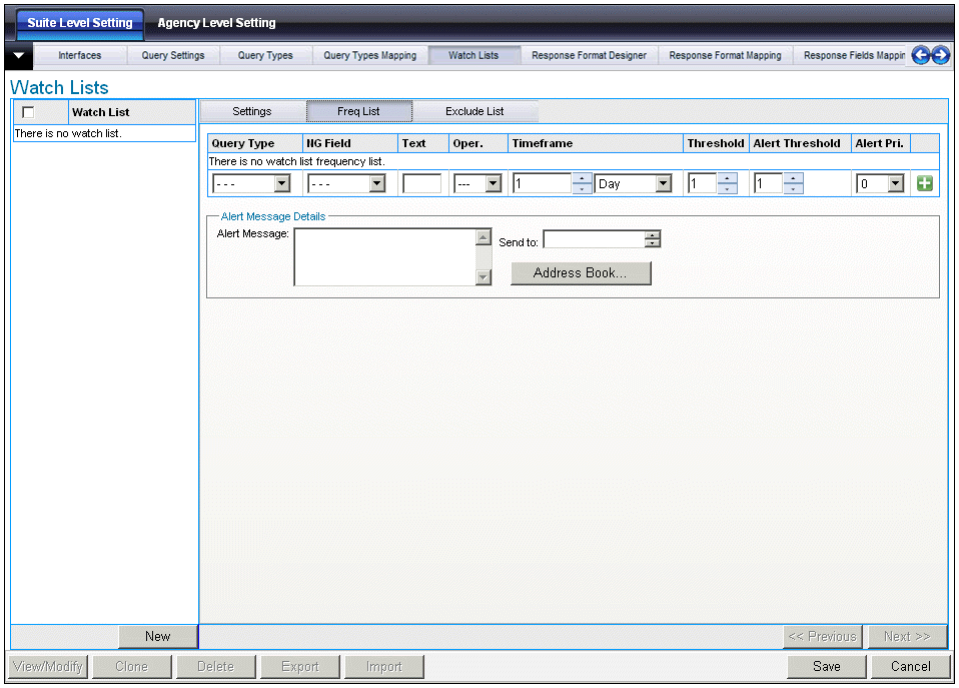


Figure 31-26 Watch Lists Form – Freq List Tab

3. From the Query Type list, select a query type.
4. From the NG Field list, select a field.
5. In the Text field, type the value for the first two fields.

   Example:

   If the first two fields are Vehicle and Make, the Text field value could be **Toyota**.

6. From the Oper. list, select an operator, if needed.
7. From the Timeframe list, select the time frame.
8. From the Threshold list, select the minimum number of times the same information must occur in query requests to trigger the watch list.

9. From the Alert Threshold list, select number of times the same information must occur in query requests to cause an alert message to be sent.

10. From the Alert Pri. list, select the priority of the alert message.

    Click the plus symbol at the end of the row to save the information in the row and add another row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

11. In the Alert Message field, type the text for the alert message you want to send when the alert threshold is met.

12. In the Send to field, use the address book to select the recipients of the alert message.

13. Click **Save**.

Adding Watch List Exclude Settings

Add watch list exclude settings when you want to exclude specific entries from a watch list. For example. you may use license plate ABC123 for training purposes. Therefore, you would want to specify that ABC123 should not be monitored for repetitive search activity.

To add watch list exclude settings:

1. Access the form for new watch lists. For instructions, see “Adding Watch List Settings” on page 31-38.

   The Watch Lists form appears with the Settings tab in focus (see Figure 31-25). A list of existing watch lists appears on the left side of the form.

2. Select the Exclude List tab.

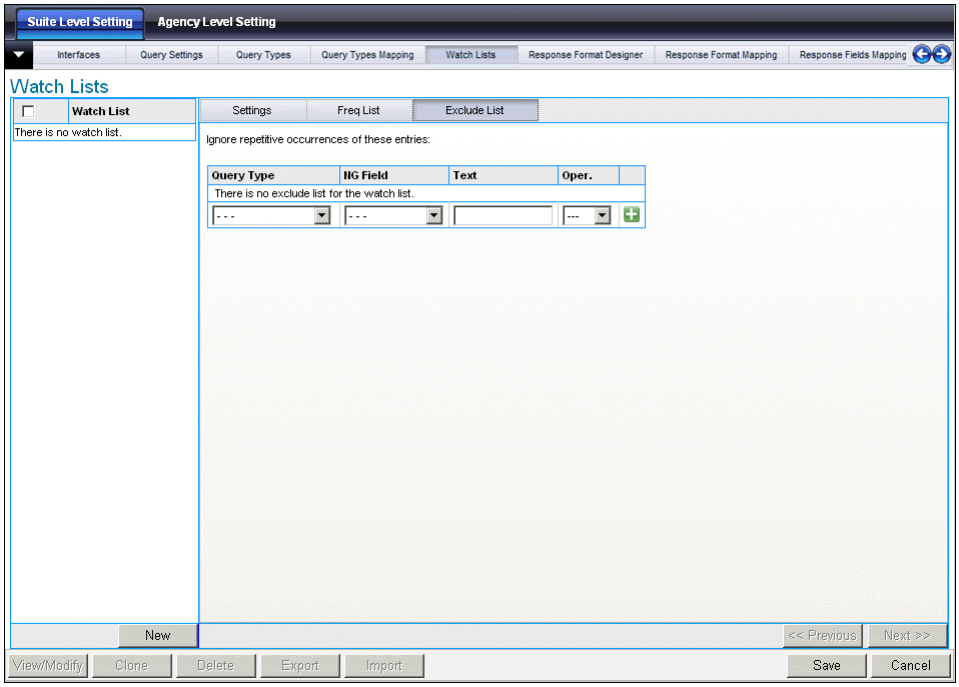


Figure 31-27 Watch Lists Form – Exclude List Tab

3. From the Query Type list, select a query type.

4. From the NG Field list, select a field.

5. In the Text field, type the value for the first two fields.

   Example:

   If the first two fields are Vehicle and Make, the Text field value could be **Toyota**.

6. In the Oper. field, select an operator, if you need to add another field for the same query type.

   Click the plus symbol at the end of the row to save the information in the row and add another row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the information, even after you click Save.

7. Repeat the previous steps to complete the exclude list.

8. Repeat the procedure to add any other watch lists.

   Each unsaved watch list appears in the Watch List list in blue text.

9. Click **Save**.

The new watch lists appear in black text.

Configuring Response Formats

Use the Response Format Designer configuration item to configure the formatting for query responses in CAD and Mobile. The Response Format Designer was developed in Microsoft Silverlight, so you may be prompted to download a Silverlight plug-in.

Formatting controls include font type, size, style, color, tooltips, hypertext, and label text.

To configure response formats:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then select **Response Format Designer**.

   The Response Format Designer form appears.

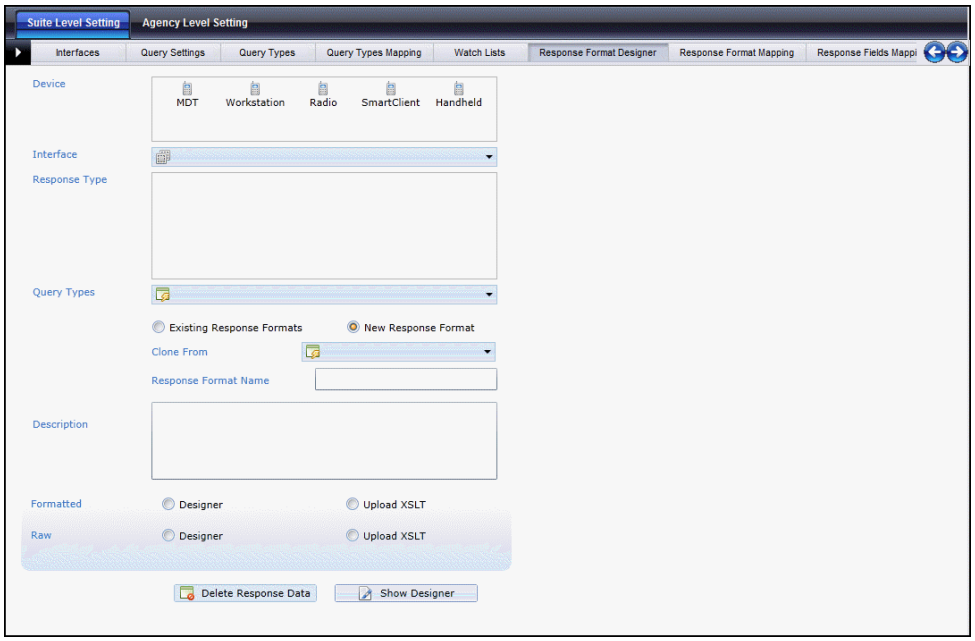


Figure 31-28 Response Format Designer Form

2. In the Device box, select the device you are configuring.

   When you select a device, the Response Type field populates the available response types, such as NCIC.

3. From the Interface list, select the interface.

4. In the Response Type box, select the Response type you are configuring.

   When you select the Response type, then the Query Types list is populated.

5. From the Query Types list, select the Query Type, such as vehicle or gun registration.

6. Do one of the following:

   - If this is an existing response format:

     1) Select **Existing Response Format**.

        A drop-down list of previously saved response formats appears.

     2) Select the appropriate saved response format from the list.

   - If this is a new response format:

     1) Select **New Response Format**.

     2) From the Clone From list, select an existing response format to clone for the new response format. You can clone formats from different device types (for example, from CAD to Mobile).

     3) In the Response Format Name field, type a name for the new response format.

     4) In the Description field, type identifying information for this response format.

7. At the bottom of the window, select one of the following:

   - To configure a Formatted query reply using the Designer tool, select **Designer** in the Formatted row. To configure the reply using your own `.xslt` file, select **Upload XSLT**.

   - To configure a Raw query text reply using the Designer tool, select **Designer in** the Raw row. To configure the reply using your own `.xslt` file, select **Upload XSLT**.

   Proceed with the appropriate procedure, "Configuring a Reply Using the Designer Tool" on page 31-45 or "Configuring a Reply Using XSLT" on page 31-48.

Configuring a Reply Using the Designer Tool

If you selected Designer in the Response Format Designer form, then the window refreshes to display the Format Designer. The left pane contains the fields that can be added to the response. The middle pane is where the formatted fields for the response display. The right pane is where you format the properties of the text.

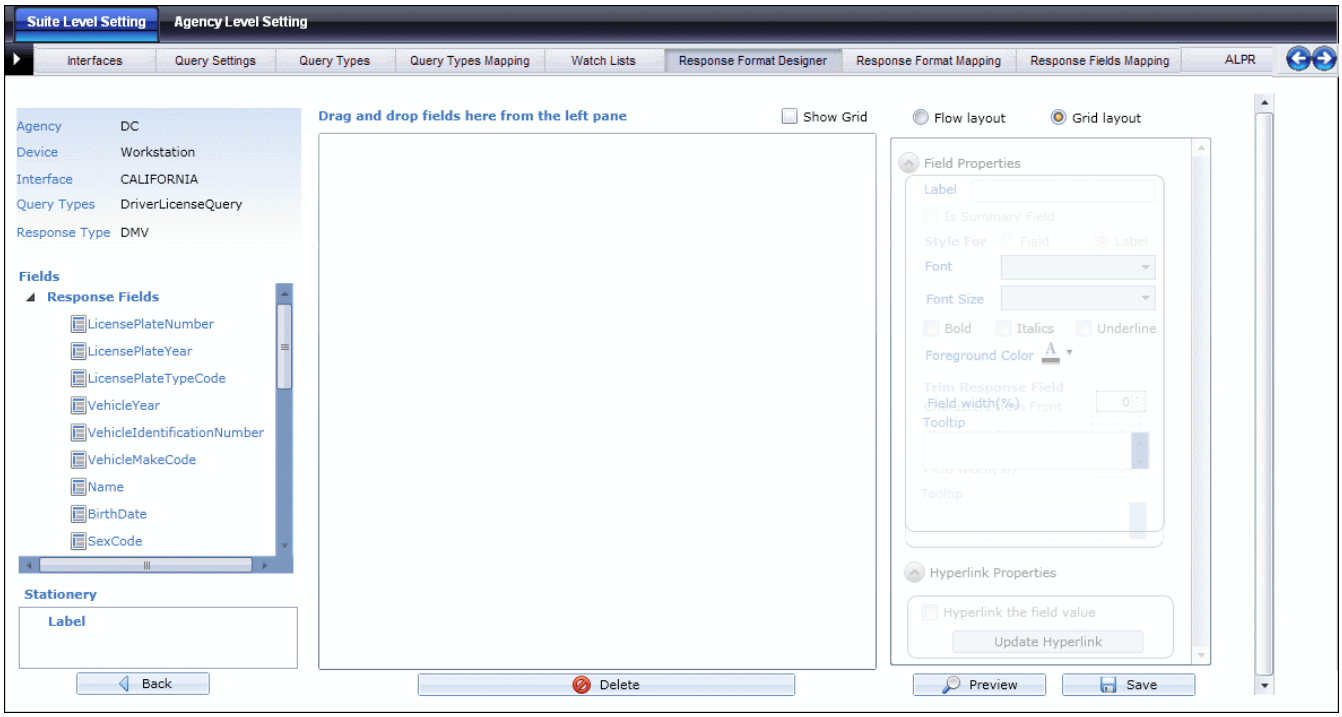


Figure 31-29 Response Format Designer – Designer Window

To format the response text:

1. From the pane on the left, drag-and-drop the fields you want to display into the central pane.

   You can add Response fields, Response headers, Attachment headers, and any defined stationery. You can use the Label stationery as a title or label to separate and group the response data.

2. Select each field and configure the display properties in the Properties pane on the right side of the window. As you make formatting changes, the style updates in the middle window pane.

   You can set the style for both the Label and the actual field value.

3. Do any of the following as needed:

   - To rearrange the display order of the fields, drag the fields to the location where you want them.

   - To display a grid, select the **Show Grid** check box. A grid is useful for viewing alignment of the fields.

- To display the response in “flow” format, select **Flow Layout**. You can set field size percentage using flow layout. For example, in a three column layout, each column is set to 33 percent by default. You can select a column, and then use the Field Width % field to enter the width percentage of the row that the selected column occupies.

Example: Flow Layout

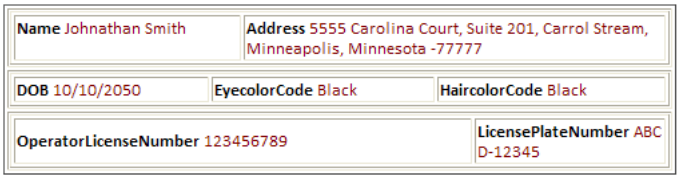


Figure 31-30 Query Response Flow Layout

- To display responses in “grid” format, select **Grid Layout**. All fields are equal widths.

Example: Grid Layout

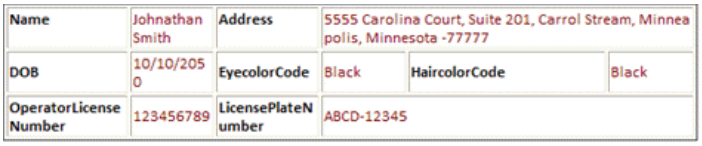


Figure 31-31 Query Response Grid Layout

- To preview the formatted text, select the **Preview** button at the bottom of the right window pane.

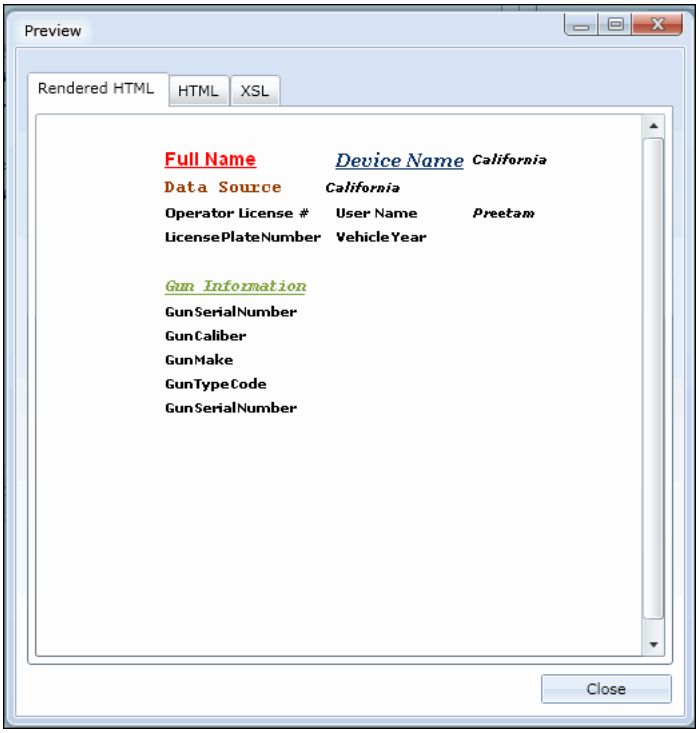


Figure 31-32 Query Preview Window

- To hyperlink a field, select the field and then select the **Hyperlink the field value** check box in the Property pane. In the Field Hyperlink dialog box that appears, click the **Update Hyperlink** button. Enter the URL and hyperlink parameters and click **OK**.

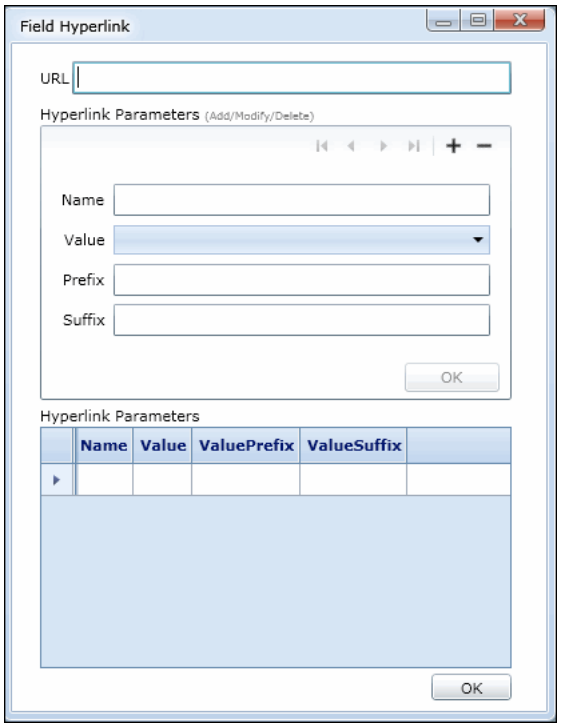


Figure 31-33 Field Hyperlink Dialog Box

4. When finished, select **Save**.

Configuring a Reply Using XSLT

If you selected Upload XSLT in the Response Format Designer form, the Upload form appears.

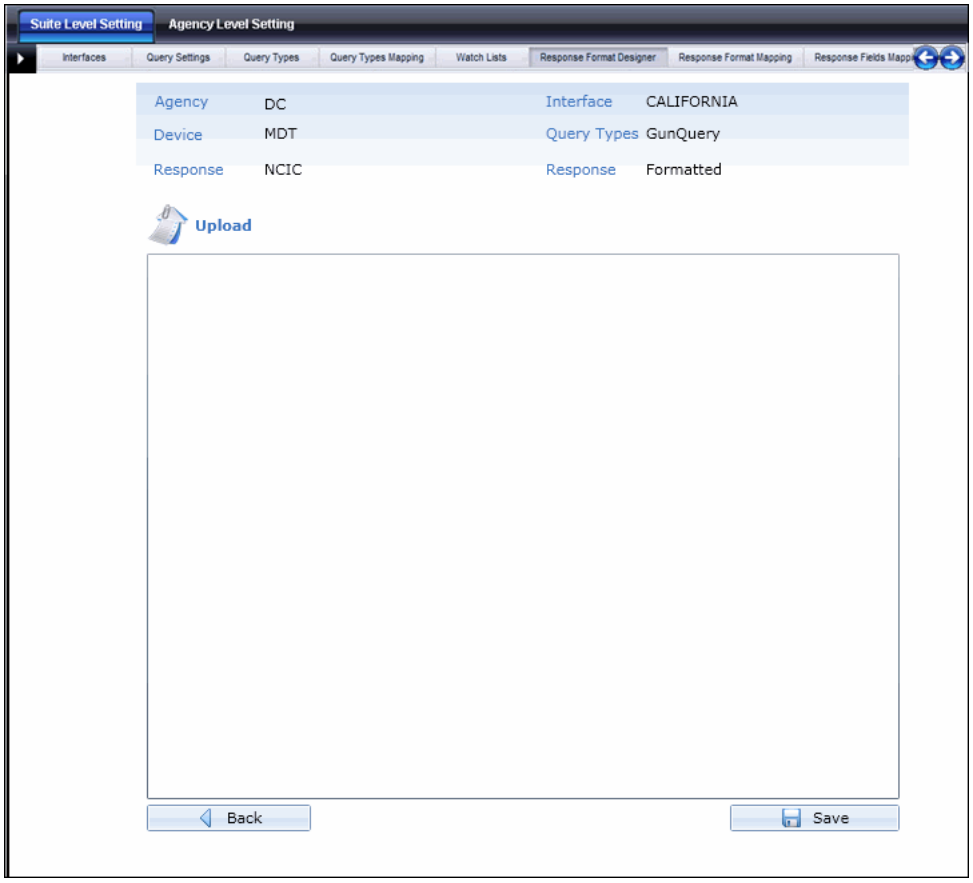


Figure 31-34 XLST Upload Dialog Box

Do the following to format the response text:

1. Copy your XSLT in the text box.
2. Click **Save**.

Configuring Response Format Mapping

Use the Response Format Mapping tab to associate response formats to agencies. You can choose to map by agency, or by response format.

To configure response format mapping:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then **Response Format Mapping**.

   The Response Format Mapping screen appears.

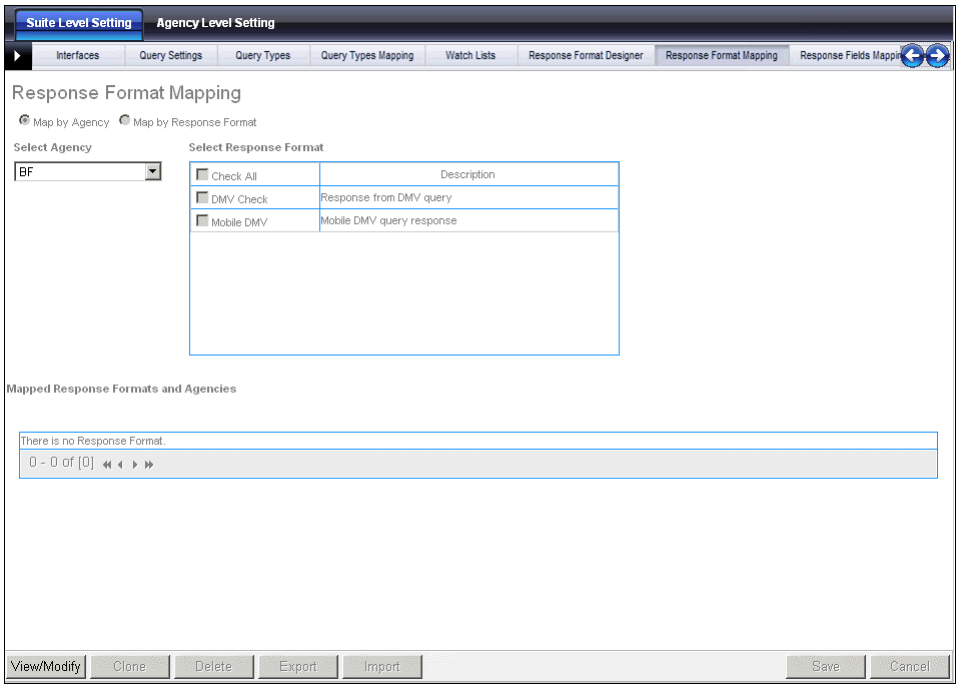


Figure 31-35 Response Format Mapping Tab

2. Click **View/Modify**.

3. Do one of the following:

   a. Select Map by Agency to assign response formats to a particular agency.

   b. Select Map by Response Format to assign a particular response format to one or more agencies.

Mapping Response Formats by Agency

You can map response formats by agency or by response format. For details on mapping response formats by response format, see “Mapping Response Formats by Response Format” on page 31-51.

To map response formats by agency:

1. Navigate to the Response Format Mapping screen as described in “Configuring Response Format Mapping” on page 31-49.

2. Select **Map by Agency**.

   The Response Format Mapping screen refreshes. Existing mapped query types and agencies appear at the bottom of the screen.

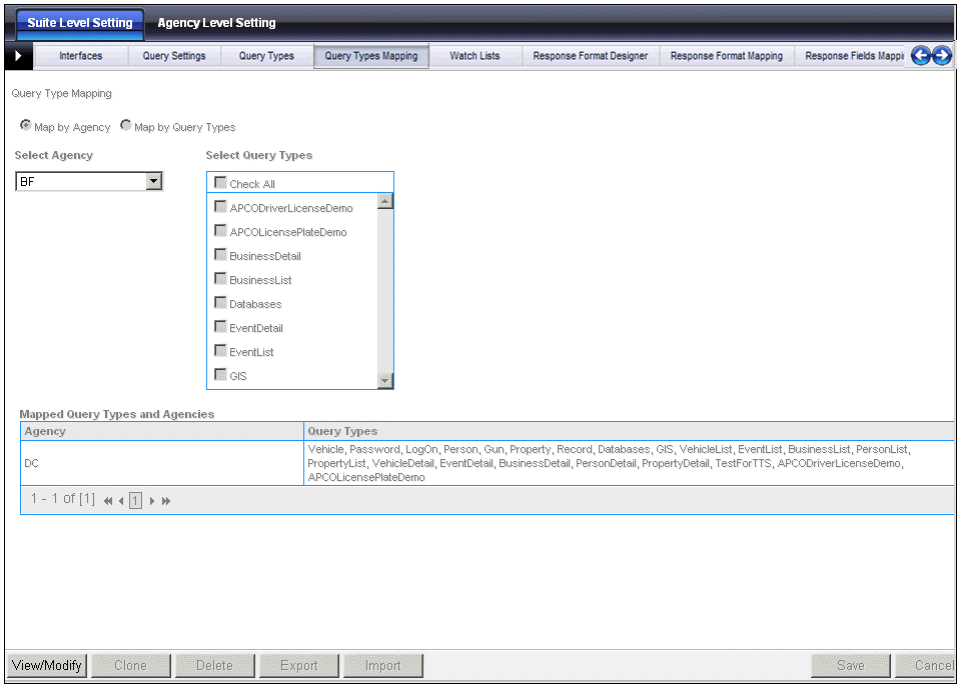


Figure 31-36 Query Types Mapping by Agency Screen

3. From the Select Agency list, select the agency to which you want to map query types.

4. In the Select Query Types list, select the query types that you want to map to the selected agency.

5. Click **Save**.

Mapping Response Formats by Response Format

You can map response formats by agency or by response format. For details on mapping response formats by agency, see “Mapping Response Formats by Agency” on page 31-50.

To map response formats by response format:

1. Navigate to the Response Format Mapping page as described in “Configuring Response Format Mapping” on page 31-49.

2. Select **Map by Response Format**.

   The Response Format Mapping screen refreshes. Existing mapped response formats and agencies appear at the bottom of the screen.

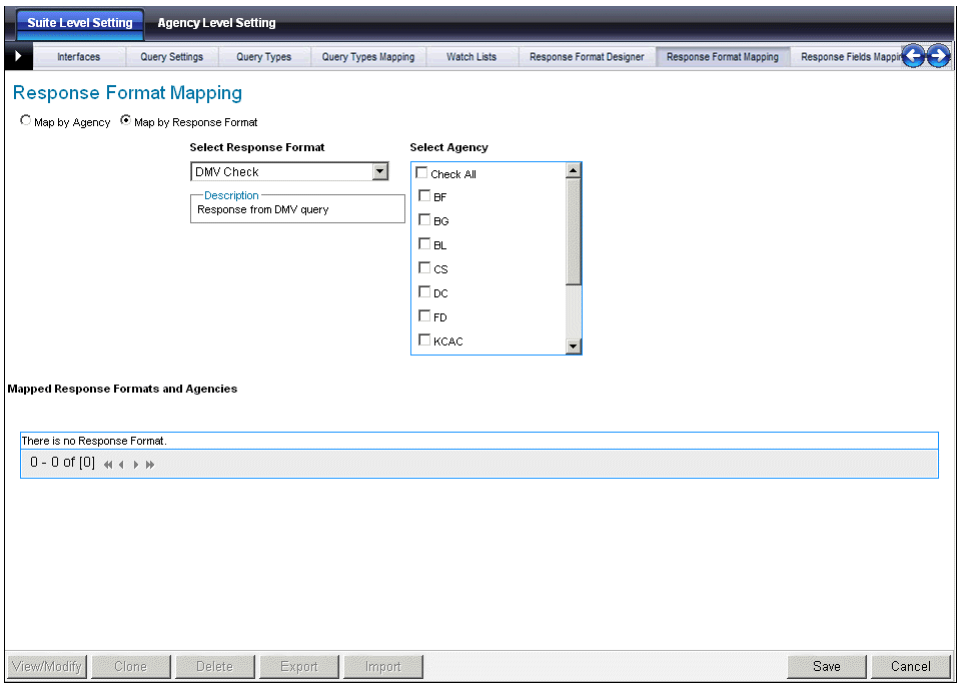


Figure 31-37 Response Format Mapping by Response Format Screen

3. From the Select Response Format list, select the response format you want to map.

4. In the Select Agency list, select the agencies to which you want to map the selected response format.

   Repeat for all response formats you want to map.

5. Click **Save**.

Configuring Response Fields Mapping

Use the Response Fields Mapping tab to map query response fields to the IM Vehicle and Person forms for a response type, and to designate key fields for importing query responses of the specified type to the IM Vehicle and Person forms. Key fields also determine the order in which the mapped fields display on the Add, Update, or Replace dialog box that appears when importing query responses to existing incidents.

To configure response fields mapping:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then **Response Fields Mapping**.

   The Response Fields Mapping screen appears. Any existing response mapping records appear on the left side of the screen.

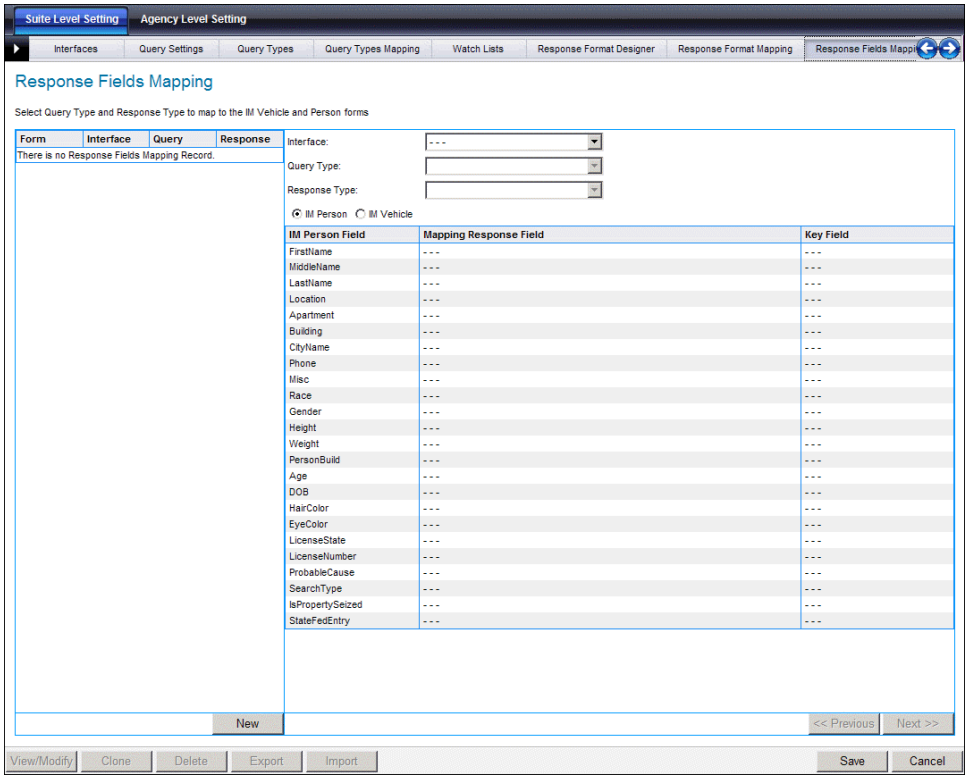


Figure 31-38 Response Fields Mapping Tab

2. Click **View/Modify**.

3. From the Interface list, select the interface you want to map response fields for, for example, California.

4. From the Query Type list, select the query type you want to map response fields for, for example, Vehicle Query.

5. From the Response Type list, select the response type you want to map response fields for, for example, DMV.

6. Select whether you want to map response fields to the IM Person tab or the IM Vehicle tab.

   The mapping table displays the fields for the IM form you select.

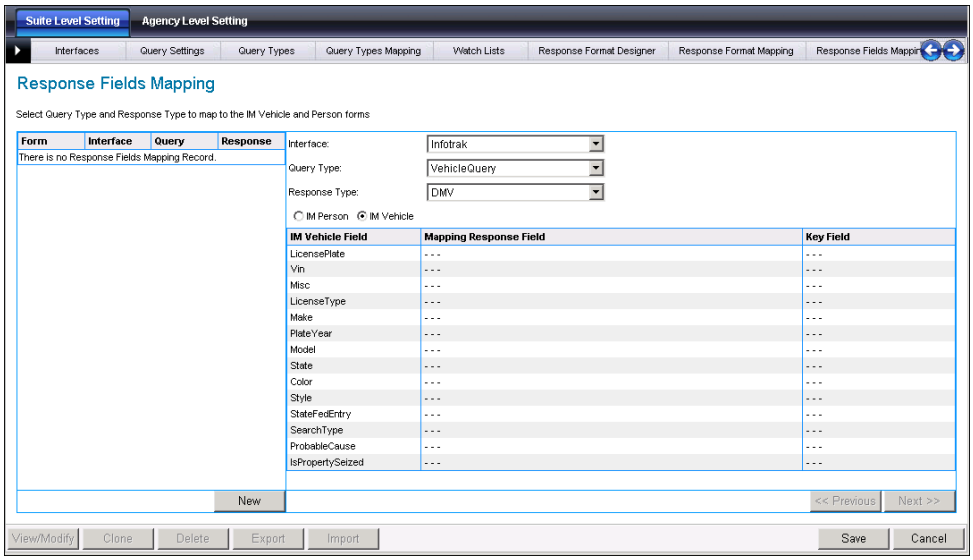


Figure 31-39 Response Fields Mapping Tab – IM Vehicle Form Selected

7. In the IM Person Field or IM Vehicle Field column (whichever you selected to display), click in the row of the field you want to map a response field to, for example, **LicensePlate**.

   The Mapping Response Field and Key Field columns for that row display drop-down lists.

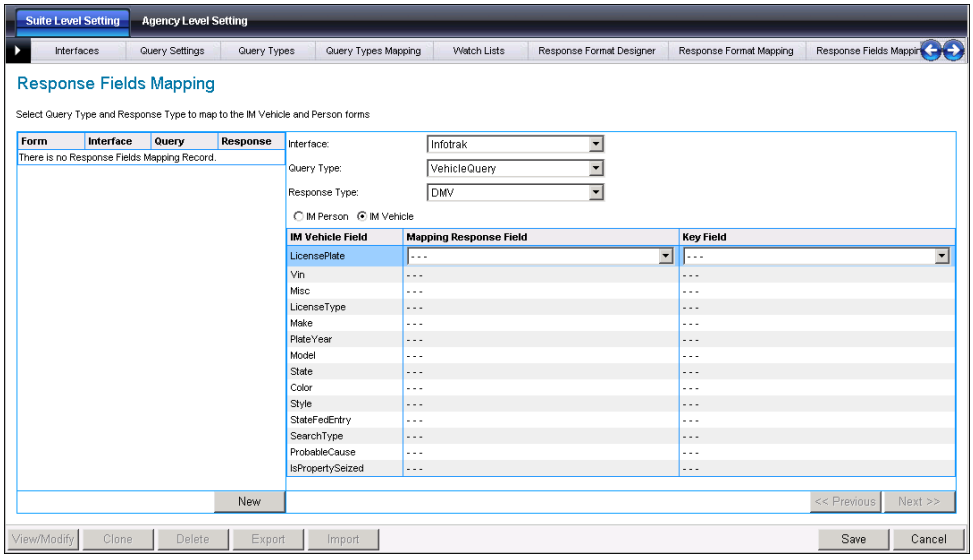


Figure 31-40 Response Fields Mapping Tab – LicensePlate Field Selected

8. From the Mapping Response Field list, select the query response field that you want to map to the IM Vehicle or IM Person form (in this example, the IM Vehicle form).

9. From the Key Field list, select a key field number (1 through 5) for this response field.

   When you import a query response, ALL mapped fields are copied to the IM Person or Vehicle form; it does not matter if they are key fields or not.

   You must assign at least one mapped response field as a key field for this response type to be available for importing to an incident. Responses that do not contain at least one of the configured key fields will not be available for importing.

   You can designate up to five response fields as key fields. The numbers you assign to key fields determines the order in which the fields are displayed on the Add, Update, or Replace dialog box that appears when importing query responses to existing incidents.

10. Continue assigning all the fields you want to map, and select up to five fields to be key fields.

11. Click **Save**.

NOTE

For details on the importing query responses to incidents, see “Importing Query Responses to Incidents” in the *PremierOne CAD User Guide*.

Configuring ALPR Automatic Queries

Use the ALPR tab to configure PremierOne Mobile to automatically run queries on license plate data captured by the ALPR (Automatic License Plate Recognition) system on mobile units.

NOTE

MDT devices must be individually provisioned to enable the ALPR reader to run automatic queries. For details, see “Adding Workstation/MDT/Handheld General Information” on page 11-44.

To configure an ALPR automatic query:

1. From the navigation panel, select **Query**, then **Suite Level Setting**, and then **ALPR**.

   The ALPR screen appears.

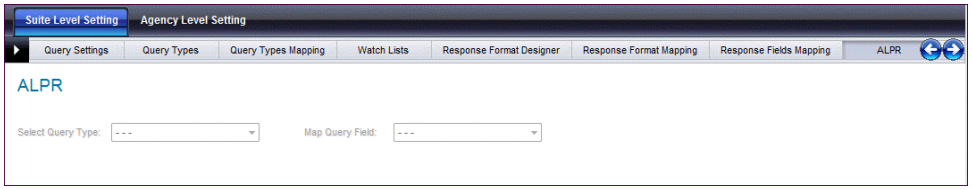


Figure 31-41 ALPR Screen

2. From the Select Query Type list, select the Query Type to automatically run on ALPR hits.

3. From the Map Query Field field, select the field on which to run the query.

Configuring Query Two-Factor Authentication

Use the Query 2-Factor Authentication tab to require two-factor authentication for queries form Mobile, Radio, or Handheld devices.

To configure two-factor authentication:

1. From the navigation panel, select **Query**, then the **Suite Level Setting** tab, and then **Query 2-Factor Authentication.**

   The Two-Factor Authentication screen appears.

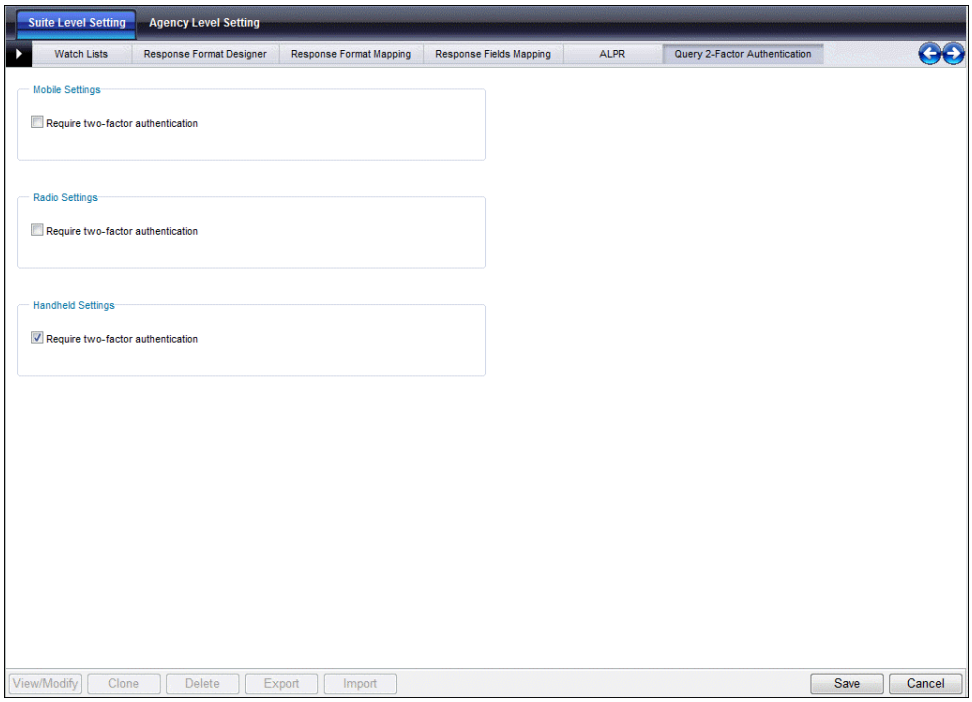


Figure 31-42 Two-Factor Authentication Screen

2. Under the Mobile Settings, Radio Settings, or Handheld Settings sections, select the check box to enable two-factor authentication.

3. Click **Save**.

Configuring Queries at the Agency Level

Use the Agency Level Setting tab to configure queries at the agency level. The Agency Level Setting tab contains the following sub-tabs:

- Interfaces – Where you assign interfaces created at the suite level to agencies.
- IM Query Settings – Where you set query types for person and vehicle searches.

Configuring Interfaces for Queries at the Agency Level

Use the Agency-Level Setting Interfaces configuration setting to enter agency-level configuration information. Configuration information includes fields on the following tabs:

- Mnemonic – Where you define device/role combinations.
- ORI – Where you enter the Originating Agency Identifier number and determine if the ORI should apply to all or to some workstations and to all or to some roles.
- Hot hits – Where you configure hot hits for all query types.

Configuring Interface Mnemonic Settings at the Agency Level

A mnemonic is a unique identifier for a combination of users and devices who can submit and receive query requests and responses to and from the database. For example, a mnemonic could identify that all Supervisors (role) at specifically defined workstations (devices) can submit and receive query requests and responses to the available databases.

The devices (for example, workstations) initiate inquiries to databases such as the department of motor vehicles, NCIC (National Crime Information Center), CLETS (California Law Enforcement Telecommunications System), and NLETS (National Law Enforcement Telecommunications System). Responses are returned to the devices.

Modify the interface mnemonic settings when you need to change the mnemonic or how it is associated with workstations and roles.

To configure an agency-level interface mnemonic:

1. From the navigation panel, select **Query**, then the **Agency Level Setting** tab, and then **Agency Interfaces**.

   The Interfaces form appears with the Mnemonic tab in focus. A list of existing interfaces displays on the left side of the form.

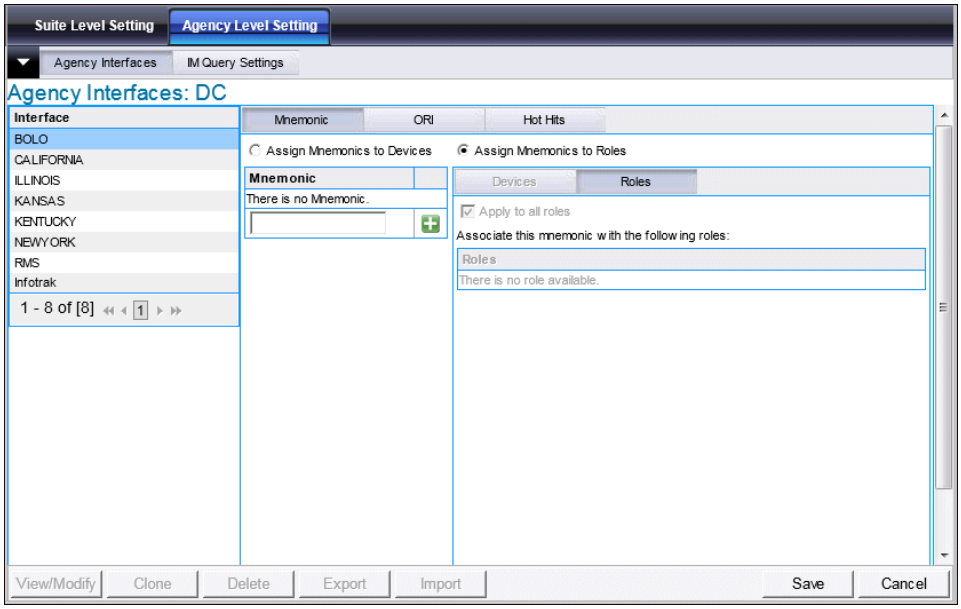


Figure 31-43 Agency Level Interfaces Form – Mnemonic Tab

2. From the Interface list on the left, select the interface for which you want to create a mnemonic.

3. Click **View/Modify**.

4. Do one of the following:

   - To define mnemonics for devices, select the **Assign Mnemonics to Devices** button.

   - To define mnemonics for roles, select the **Assign Mnemonics to Roles** button.

5. In the Mnemonic field, type the mnemonic for the selected interface.

   Click the plus icon at the end of the Mnemonic row to save the mnemonic and add another row.

CAUTION

If you do not click the plus symbol, Provisioning does not save the mnemonic, even after you click Save.

6. For defining mnemonics based on devices, select the mnemonic and then do one of the following on the Devices tab:

   - To have the mnemonic apply to all devices, select the **Apply to all devices** check box.
   - Click **Find** and select the devices.

     If configuring the Smart Client, select the device for the Smart Client (this could be the machine name). The default Smart Client device is **SmartClient_DefaultDevice**.

7. For defining mnemonics based on roles, select the mnemonic and then do one of the following on the Roles subtab:

   - To have the mnemonic apply to all roles, select the **Apply all roles** check box.
   - Click **Find** and select the roles.

     If configuring the Smart client, select **DefaultRole**. The Smart Client uses PremierOne's DefaultRole.

Configuring the Interface ORI Settings at the Agency Level

The ORI (originating agency identifier) is used by the NCIC/Interpol network to uniquely identify law enforcement agencies around the world. The agency's ORI serves as a unique identifier for the agency. An ORI is comprised of the state abbreviation, the county's code, and the jurisdiction within the county.

Configure the interface ORI settings to set how the settings are associated with devices and roles.

To configure the agency-level interface ORI:

1. Access the Query – Agency-Level Setting – Interfaces form. For details, see "Configuring Interfaces for Queries at the Agency Level" on page 31-57.

   The Interfaces form appears with the Mnemonic tab in focus. A list of interfaces displays on the left side of the form.

2. Select the interface for which you want to assign an ORI.

3. Select the ORI tab.

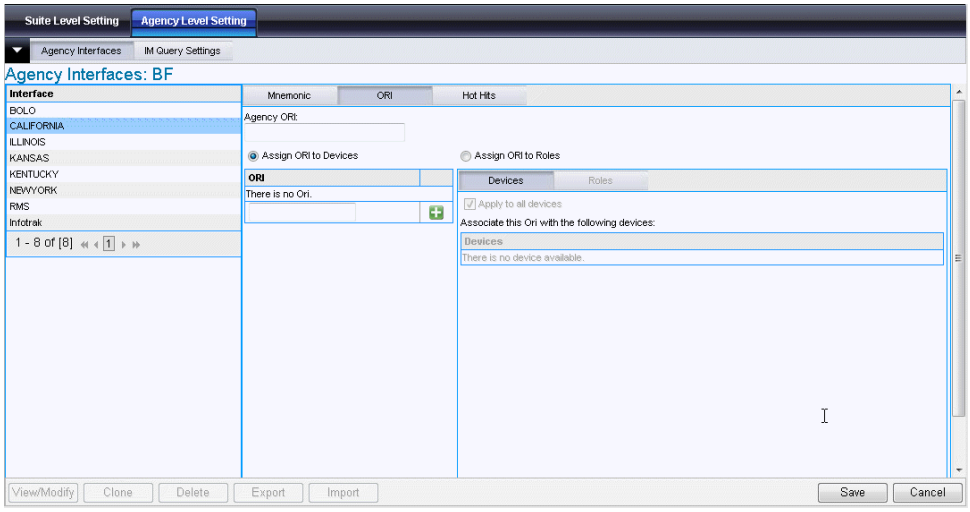


Figure 31-44 Query – Agency Level Settings – Interfaces Form – ORI Tab

4. From the Interface list on the left, select the interface for which you want to create an ORI.

5. Click **View/Modify**.

6. In the Agency ORI field, type the ORI for the agency, using the format of state abbreviation, the county's code, followed by the jurisdiction within the county.

   Click the plus icon at the end of the ORI row to save the ORI and add another row. This also makes the fields on the Devices or Roles subtab editable.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the ORI, even after you click Save.

7. To assign this ORI to devices, select Assign ORI to Devices.

   To assign the ORI to roles, select Assign ORI to Roles.

   Depending on your selection, the Devices or Roles subtab is enabled.

8. On the Devices or Roles subtab, select whether to have the ORI apply to all devices/roles or just to selected devices/roles. This will determine whether all or only specified devices/roles can submit and receive query requests and responses.

   Your selections appear in the Devices table.

9. If you do not choose to apply the ORI to all devices/roles, click **Find** to select the devices/roles to which to apply the ORI.

10. Click **Save**.

Configuring Interface Hot Hit Settings at the Agency Level

Use the Hot Hits tab of the Agency Level Setting interface form to add hot hits for queries at the agency level. Hot hits are keywords that occur in a query response, such as WANTED or a vehicle identification number. The hot hit response triggers a notification message and an optional alarm.

You can also configure hot hit settings for individual query types (see "Adding Hot Hits for Query Types" on page 31-28). The only difference between state and query type is that query type have all the added fields to use in hot hit definition. For interface level hot-hits, only a fixed number of header fields and raw message fields are available. Query type hot hit rules can override or be combined with Interface hot hit rules.

Interface hot hits are evaluated along with Query Type hot hits.

Hot Hit Examples

Hot hit rules can range from a simple keyword search to a combination of complex rules. Following is a list of examples. PremierOne will apply the rules to identify the hot hit response.

- A simple keyword that can be searched in the query response. If PremierOne finds the provisioned keyword, then the response is treated as a hot hit. Example: "STOLEN"
- A combination of more than one keywords. Example: "ARMED" AND "DANGEROUS"
- One *or* more keywords. Example: "OFFICER SAFETY" OR "ESCAPEE" OR "WANTED"
- Keyword search that ignores some strings. Example: "STOLEN" AND NOT "NO NCIC WANT." Here if the response contains "STOLEN" and "NO NCIC WANT," then the response is not treated as a hot hit. If the response contains the "STOLEN" text only, then it is treated as a hot hit.
- Complex expressions. Example: ("FELONY" OR "FUGITIVE") AND ("ARMED" OR "AT RISK"). Example: ("FELONY" OR "FUGITIVE") AND ("ARMED" OR "AT RISK") AND NOT ("NO HITS" OR "NO MISS").

NOTE
The operators in parentheses separate groups of rules. That is, if you have configured two rules using "and" and "or," a third rule using "(and)" is treated as a separate operation from the first "group" of two rules.

To add hot hits for an agency-level interface:

1. Access the Interfaces form. For details, see "Configuring Interfaces for Queries at the Suite Level" on page 31-8.

   The Interfaces form appears with the Settings tab in focus. A list of interfaces displays on the left side of the form.

2. Select the interface.

3. Select the Hot Hits tab.

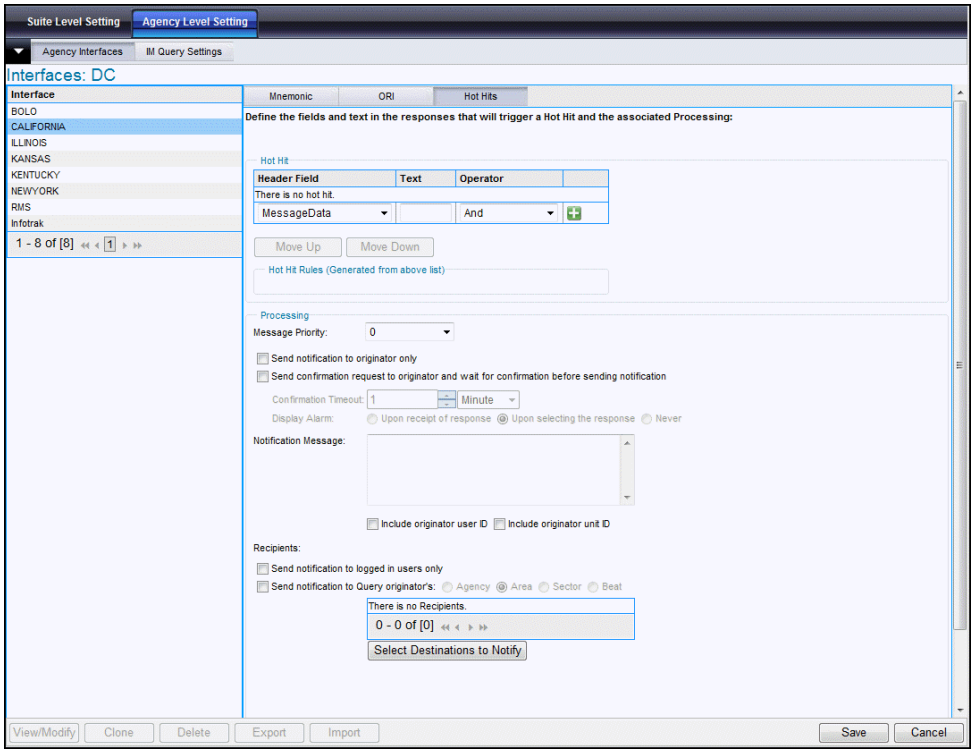


Figure 31-45 Query – Agency Level Settings – Interfaces Form – Hot Hits Tab

4. From the Header Field field list, select a field with the value to use as the keyword for the hot hit.

   For details on using Hot Hit rules, see "Hot Hit Examples" on page 31-61.

5. In the Text field, type the text for the keyword.

   Example:

   If your response field is LIC (license), your keyword in the Text field could be 123ABC, the license number of a vehicle involved in an Amber alert.

6. For multiple statements, select the operator to use from the Operator list.

7. Click the plus symbol at the end of the row to save the row and add a new row.

> **CAUTION**
> If you do not click the plus symbol, PremierOne does not save the information in the row, even after you click Save.

8. To change the order of the rows, select the row you want to move and then use the **Move Up** and **Move Down** buttons to reposition the selected row.

9. In the Hot Hit Rules (Generated from above list) section, the rules you created are summarized.

   Refer to this section to confirm that your Hot Hit rules are set up correctly.

10. In the Processing section, configure how you want to handle the processing for the hot hit.

    a. Select one of the following:

       - To only send the notification to the originator, select the **Send notification to originator only** check box.
       - To send a confirmation request to the originator and wait for a confirmation message before sending a notification, select the **Send confirmation request to originator and wait for confirmation before sending notification** check box.

       Then in the Confirmation Timeout field, enter the time to delay before sending a notification.

    b. In the Display Alarm field, indicate when to display a hot hit notification *for the originator only* by selecting one of the following.

       - **Upon receipt of response**: The hot hit confirmation dialog box displays when the query response is received.
       - **Upon selecting the response**: The hot hit confirmation dialog box displays when the query response is selected in the Work Assist Area.
       - **Never**: The hot hit confirmation dialog box does not automatically display. The user needs to click the Hot Hit button to display the confirmation dialog box.

    c. In the Notification Message box, type the message that you want sent when this hot hit is triggered. Then select whether you want to **Include originator user ID** or **Include originator unit ID**.

NOTE

The notification that is sent to everyone besides the originator is sent as a regular mail message at the configured priority.

---

    d. In the Recipients section, ensure that the **Send notification to logged in users only** check box is selected to send notifications only to logged in users from the Provisioned User List.

    e. To send a notification to the Query originator's Agency, Area, Sector, or Beat select the **Send notification to Query originator's** check box and then select the appropriate option.

f. To select individual recipients, click the **Select Destinations to Notify** button and select the users to whom you want the hot hit notification message sent.

11. Click **Save** on the Hot Hits tab.

Configuring Incident Management Query Settings at the Agency Level

Use the Agency-Level Setting IM Query Settings tab to set the query types for person and vehicle searches.

To configure incident management query settings at the agency level:

1. From the navigation panel, select **Query**, then the **Agency Level Setting** tab, and then **IM Query Settings**.

   The IM Query Settings form appears. The agency you selected is selected in the list on the left side of the form.

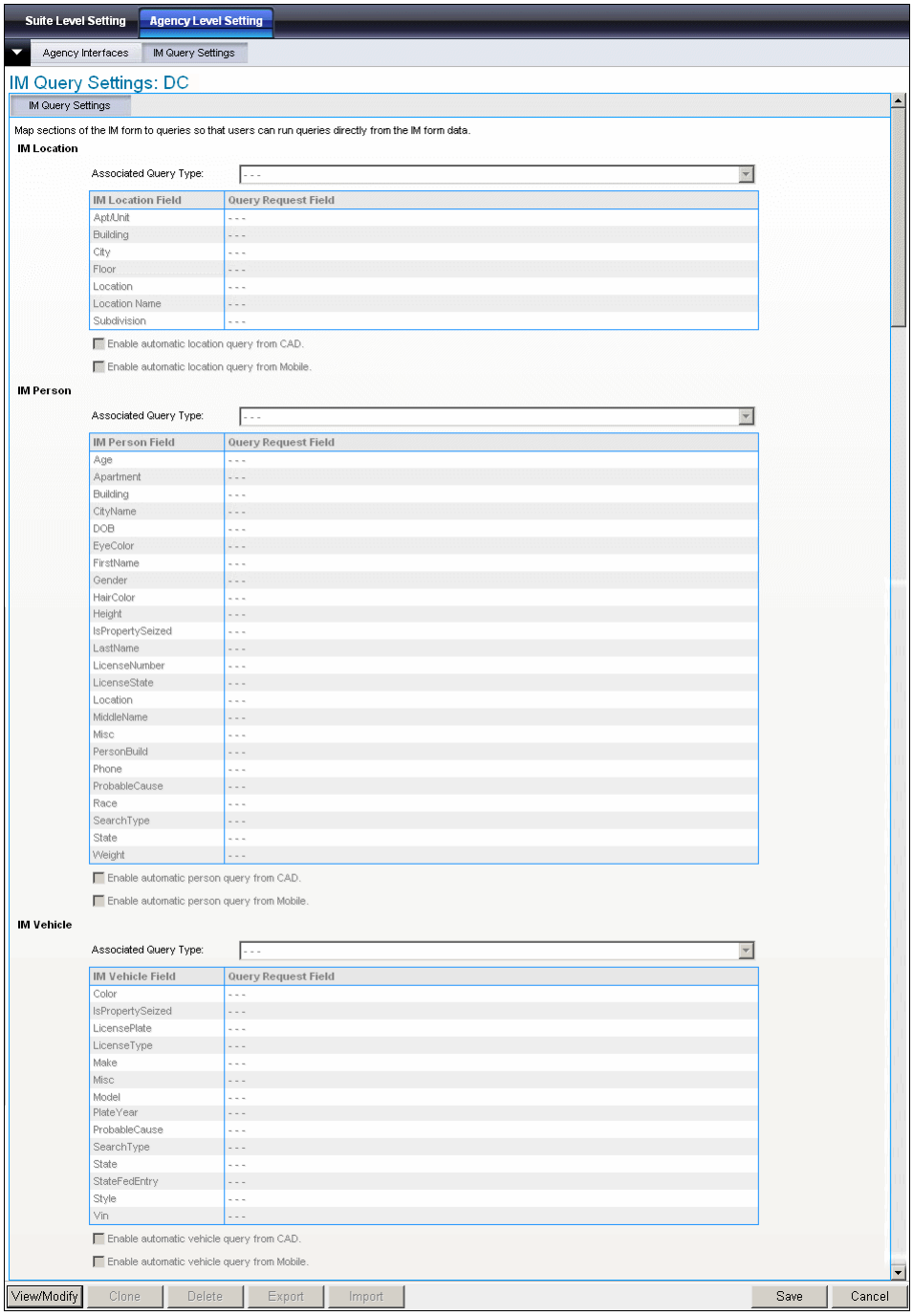


Figure 31-46 IM Query Settings Form

2. Click **View/Modify**.

3. In the IM Location section, select the appropriate query type, and then click the IM Location Field you want to modify and select the field to use for the query.

4. To enable an automatic query of a location following address verification, select Enable automatic location query from CAD, Enable automatic location query from Mobile, or both.

When the automatic location query option is selected, CAD or Mobile automatically initiates a location query upon address verification. If the automatic query option is not selected, CAD or Mobile users can manually run a Location query by pressing the Query button on the Incident Initiation General tab or the Incident Update Summary tab.

5. In the IM Person section, select the appropriate query type, and then click the IM Person Field you want to modify and select the field to use for the query.

6. To enable an automatic query of person records following incident submission, select Enable automatic location query from CAD, Enable automatic location query from Mobile, or both.

   When the automatic person query option is selected, CAD or Mobile automatically initiates a Person query upon incident submission. If the automatic query option is not selected, CAD users can manually run a Person query by pressing the Query button on the Persons tab, if the query type is provisioned. Mobile users can manually run queries using the Qry button on the Persons Details page.

7. In the IM Vehicle section, select the appropriate query type, and then click the IM Vehicle Field you want to modify and select the field to use for the query.

8. To enable an automatic query of vehicle records following incident submission, select Enable automatic location query from CAD, Enable automatic location query from Mobile, or both.

   When the automatic vehicle query option is selected, CAD or Mobile automatically initiates a Vehicle query upon incident submission. If the automatic query option is not selected, CAD users can manually run a Vehicle query by pressing the Query button on the Vehicles tab, if the query type is provisioned. Mobile users can manually run queries using the Qry button on the Vehicle Information page.

9. Click **Save**.

NOTE

If a Records query is mapped, the OwnerID field must be mapped to a non-used IM field (for example, Misc). If this mapping is not done, the query will not be submitted.

CHAPTER 32

Configuring Status Monitors

The Status Monitor configuration item contains the following items:

- Agency Defaults – Where you set defaults for the agency's status monitors such as icons, right-click menu options, unit status colors, incident status colors, and fonts. For details, see "Configuring Agency Defaults for Status Monitors" on page 32-2.
- Displays – Where you add custom status monitor displays. For details, see "Adding Status Monitor Displays" on page 32-26.

You can configure status monitors in three locations in the Status Monitor configuration item: Agency Defaults, Displays (groups of status monitors called Display Sets), or Displays–Windows (individual monitors in a group of monitors).

NOTE
PremierOne uses the settings that you make in the following order: Agency Defaults, Displays, and then Windows. So for example, the font settings made for a Window would override those in Display Sets and Agency Defaults.

NOTE
CAD Status Monitors are currently limited to about 950 items.

Fixed and Varying Areas in Status Monitors

Status Monitors allow users to cover fixed or different areas. CAD provides the following types of monitors:

- Signed On Coverage Areas – These status monitors are primarily for dispatchers who are responsible for units within specific jurisdictional areas. Police agencies commonly split their jurisdiction across several dispatchers to balance the workload. Fire dispatchers usually sign on to cover entire agencies, so this type of monitor is not usually used by fire dispatchers.

- Monitored Areas – These status monitors are a *different* set of status monitor windows that are reserved for quickly displaying areas outside or within the set of signed on coverage areas. For user roles configured to have this type of monitor, the user can issue the MA command for one or more agency/area combinations and see what is happening in that area without affecting their Signed On Coverage Area Status monitor windows.

  Example:

  A police dispatcher who is informed that there is a large fire in FD Station 3 area might issue MA.FD/STN3 to monitor the incidents within that area. The dispatcher can keep police units within that and the surrounding areas informed about the situation, all by watching the Monitored Area status monitor.

- Fixed Areas – These status monitors always display the same areas. Fixed areas are beneficial to remote CAD clients in use by field unit supervisors at different fire, police, and EMS stations. Users can sign on to cover only one area within the larger set of areas of responsibility. As part of the default status monitor display, users can also have Incident and Unit Status monitor windows that display all the areas regardless of how the user signs on. The CC, WT, and DS commands do not function with fixed areas.

- Signed On Coverage Areas and Monitored Areas – These status monitors blend signed on coverage areas with monitored areas in the same window. These are used when there is limited monitor space.

  With this type of status monitor, the MA command can only add to the user's signed on areas; no signed on area will ever be removed, and the user cannot remove it as long as the user is signed on to cover the area.

Configuring Agency Defaults for Status Monitors

Use the Agency Defaults configuration item to set defaults for the agency’s status monitors such as icons, right-click menu options, unit status colors, incident status colors, and fonts.

NOTE
Agency defaults are the settings used for all of the status monitors for a display set, unless you override them by creating new settings for your agency.

When you modify agency defaults, you enter information on three tabs in the Agency Defaults form.

- General Settings – Where you configure unit icons, incident dynamic icons, and capability icons that are used on status monitors, and define the options that are available on the right-click menu.
- CAD – Where you define unit status colors, incident status colors, and fonts for the Incident Status monitors.
- Mobile/Handheld – Where you define unit status colors, incident status colors, and fonts for the agency's Unit Status monitors.

Configuring General Status Monitor Settings– Agency Defaults

Use the Status Monitors General tab to configure icons and right-click options for your agency's default CAD status monitors. The tab has the following subtabs:

- Icons – Where you configure incident and unit icons used on status monitors for special instances.
- Right-Click Menu – Where you configure the default options that are available on right-click menus.

Configuring CAD Status Monitor Icons

The Icons tab is where you configure icons or characters that are used on your agency's default status monitors for special instances, such as Mobile- or AVL- equipped units, priority updates, details to follow, and special unit status.

To configure CAD status monitor icons:

1. From the navigation panel, select **Status Monitors**, and then select **Agency Defaults**.

The General Settings form appears.

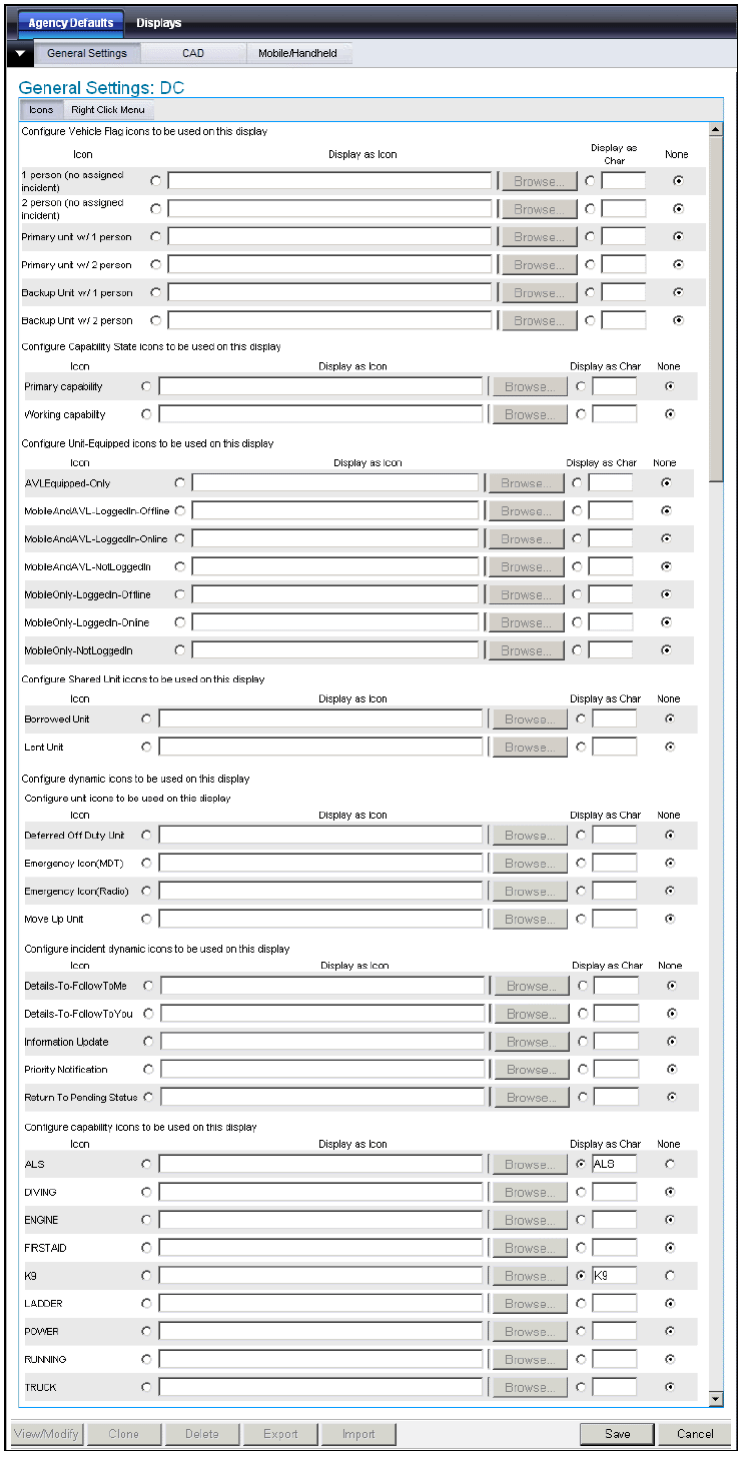


Figure 32-1 General Settings Form

2. Click **View/Modify**.

3. For each option, select whether you want to display an icon or a set of up to four characters on the status monitor to indicate the special circumstance. If you do not want to display an icon or characters, just leave the fields blank.

   - To display an icon, click the **Browse** button for the option, browse to the location of the icon, and then click **OK**. The path to the icon appears in the field. You can use any of the following formats for your icons: `GIF`, `JPG`, `JPEG`, `PNG`, and `BMP`. Because PremierOne resizes the images, there are no minimum or maximum size restrictions.

   - To display characters, select the radio button to the left of the `Display as Char` field, and then enter up to four characters.

Configure Vehicle Flag icons to be used on this display

This section lists the icons used to describe the type of unit and number of officers in the unit.

NOTE

For the icon to display on the status monitor, you must also select the Vehicle Flag (icon) field to display on the status monitor. For details, see "Adding Windows Fields" on page 32-36.

- 1 person (no assigned incident) – The unit is not assigned to an incident and there is only one officer in the vehicle.

- 2 person (no assigned incident) – The unit is not assigned to an incident and there are two officers in the vehicle.

- Primary unit w/1 person – The unit is the primary unit on the incident and there is only one officer in the vehicle.

- Primary unit w 2/person – The unit is the primary unit on the incident and there are two officers in the vehicle.

- Backup unit with 1 person – The unit is the not the primary unit on the incident and there is only one officer in the vehicle.

- Backup unit with 2 person – The unit is not the primary unit on the incident and there are two officers in the vehicle.

Configure Capability State icons to be used on this display

This section lists the icons used to describe the capability of a vehicle. The capability is the primary function or equipment on a vehicle, such as truck or K9 unit.

NOTE

For the icon to display on the status monitor, you must also select the Capability state (icon) field to display on the status monitor. For details, see "Adding Windows Fields" on page 32-36.

- Primary capability – The first capability assigned to a unit (the first capability is the primary capability of a unit).
- Working capability – The capability assigned a to unit that was the reason for the unit to be assigned to an incident. The working capability icon is visible when the unit has been assigned an incident and the unit possesses a capability needed by the incident.

Configure Unit-Equipped icons to be used on this display

This section lists the icons used to indicate whether the unit has Mobile or AVL equipment, and whether the unit is logged in or offline. The icons display automatically and will appear in the left most column.

- AVLEquipped-Only – The unit is equipped only with AVL.
- MobileAndAVL-LoggedIn-Offline – The unit has an Mobile unit and AVL, is logged into the Mobile, but is offline.
- MobileAndAVL-LoggedIn-Online– The unit has an Mobile unit and AVL, is logged into the Mobile, and is online.
- MobileAndAVL-NotLoggedIn – The unit has an Mobile unit and AVL, is not logged into the Mobile, and is offline.
- MobileOnly-LoggedIn-Offline – The unit only has an Mobile unit, is logged into the Mobile, and is offline
- MobileOnly-LoggedIn-Online – The unit only has an Mobile unit, is logged into the Mobile, and is online.
- MobileOnly-NotLoggedIn – The unit only has an Mobile unit and is not logged in.

Configure Shared Unit icons to be used on this display

This section lists the icons used to indicate how the unit is shared between agencies.

NOTE

For the icon to display on the status monitor, you must also select the Shared Unit (icon) field to display on the status monitor. For details, see "Adding Windows Fields" on page 32-36.

- Borrowed Unit – The unit is from outside of the user's signed-on coverage area(s) and has been assigned to an incident within the same user's signed-on coverage area(s).
- Lent Unit – The unit is within the user's signed-on coverage area(s) and has been assigned to an incident outside of the same user's signed-on coverage area(s).

Configure unit icons to be used on this display

This section lists the icons used to indicate the unit is in a special status.

NOTE

For the icon to display on the status monitor, you must also select the Capability (icon) field to display on the status monitor. For details, see "Adding Windows Fields" on page 32-36.

- Deferred Off Duty Unit – The unit is still assigned to an incident, but will be in off duty status once the unit clears from the incident.
- Emergency Icon (MDT) – The unit has pressed the emergency status button in the Mobile. This can only be sent from a Mobile.
- Emergency Icon (Radio) – The unit has pressed the emergency status button on the radio. This can only be sent from a radio.
- Move up unit – The unit is in a move up status (for details on move up status, see "Configuring Move Ups" on page 10-32).

Configure incident dynamic icons to be used on this display

This section lists the icons used to indicate the incident has additional information or has been returned to pending status.

The icons display automatically and will appear in the left most column. The Details-To-Follow, Information Update, and Priority Notification icons display vertically when they are triggered concurrently. This means that the row will expands downward and the new icon appears below the currently displayed dynamic icon.

- Details-To-FollowToMe – The user set the Details-To-Follow flag for an incident. The flag that informs the dispatcher that the call taker is still on the phone with the caller obtaining additional information. When the call taker is finished obtaining information, the call taker can remove the DTF flag, signifying that no further information is available.
- Details-To-FollowToYou – Another user set the Details-To-Follow flag for an incident.
- Information Update – Another user has updated the incident. The icon does not display in the status monitor display of the user issuing the update.
- Priority Notification – Priority updates exist that have not been viewed.
- Return to Pending Status – All units were removed from the incident and the incident was returned to its initial status (pending).

Configure capability icons to be used on this display

This section lists the icons for the provisioned capabilities for the agency.

For details on capabilities, see “Configuring Capabilities/Skills” on page 11-4.

Configure Call Control icons to be used on this display

This section lists the icons for the call control.

- Abandoned – The voice call was hung up before the caller spoke with an operator.
- Active – The call taker is on the line with a text user. This is SMS equivalent to the TALK state for voice calls.
- Busy – The voice call has been answered by another user.
- CAD Logged In/ACD Not Ready – The ACD user is logged into CAD but the console is not connected to the telephony system (ACD only).
- CAD Logged In/ACD Ready – The ACD user is logged into CAD and the console is connected to the telephony system (ACD only).
- CAD Logged In/Telephony Connected – The user is logged into CAD but the console is not connected to the telephony system.
- CAD Logged In/Telephony Not Connected – The user is logged into CAD and the console is not connected to the telephony system.
- CAD Logged out – The workstation is not logged in or is powered off.
- Finished – The voice call is finished and has been released.
- Hold – Another user placed the voice call on hold.

- iHold – The call taker placed the voice call on hold.
- iHold-C– A voice conference call the call taker has on hold.
- Park– The voice call has been parked by you or another user. (VIPER only).
- Presented – An incoming SMS is ringing and has not been answered.
- Redialed – Another call taker is making an outgoing call to a voice caller who just hung up (an abandoned call).
- iRedialed – The call taker was making an outgoing call to a voice caller who just hung up (an abandoned call).
- Ring – An incoming voice call is ringing and has not been answered.
- Talk – The call taker is on the line with a voice caller.
- Talk-C – Status of a voice conference the call taker is part of.
- Terminated – An SMS call was ended by the call taker.
- Updated – A SMS text has an update the call taker has not viewed yet.

Configuring Right-Click Menu Options

Right-click menu options provide direct access to CAD commands in status monitors. These options display when the user right-clicks an incident or unit any of the status monitors. When the user right-clicks an incident, unit, call, or position on any of the status monitors and selects the command from the menu, the command executes immediately or the appropriate work area appears.

The Right Click Menu tab is where you define the right-click menu options for your agency's default status monitors. These options display in all of the status monitors. To define right-click options for individual status monitors, see "Adding Windows Right-Click Menu Options" on page 32-47.

To use the right-click settings configured for the agency, make sure the **Use Agency Level Settings** check box is selected in the Window settings (see "Adding Windows Right-Click Menu Options" on page 32-47). This check box should be selected by default.

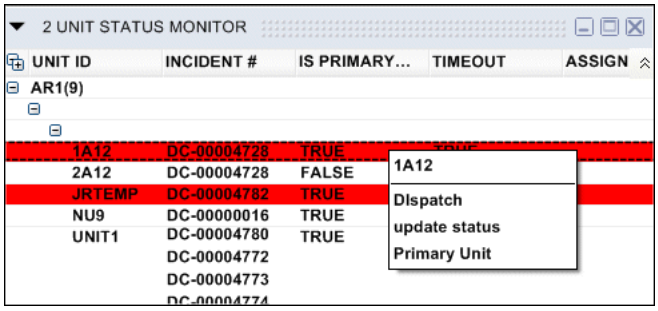


Figure 32-2 Example of Right-Click Menu Options in Unit Status Monitor

To configure the right-click menu options:

1. Access the form for agency defaults. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

   The General Settings form appears.

2. Select the Right Click Menu tab.

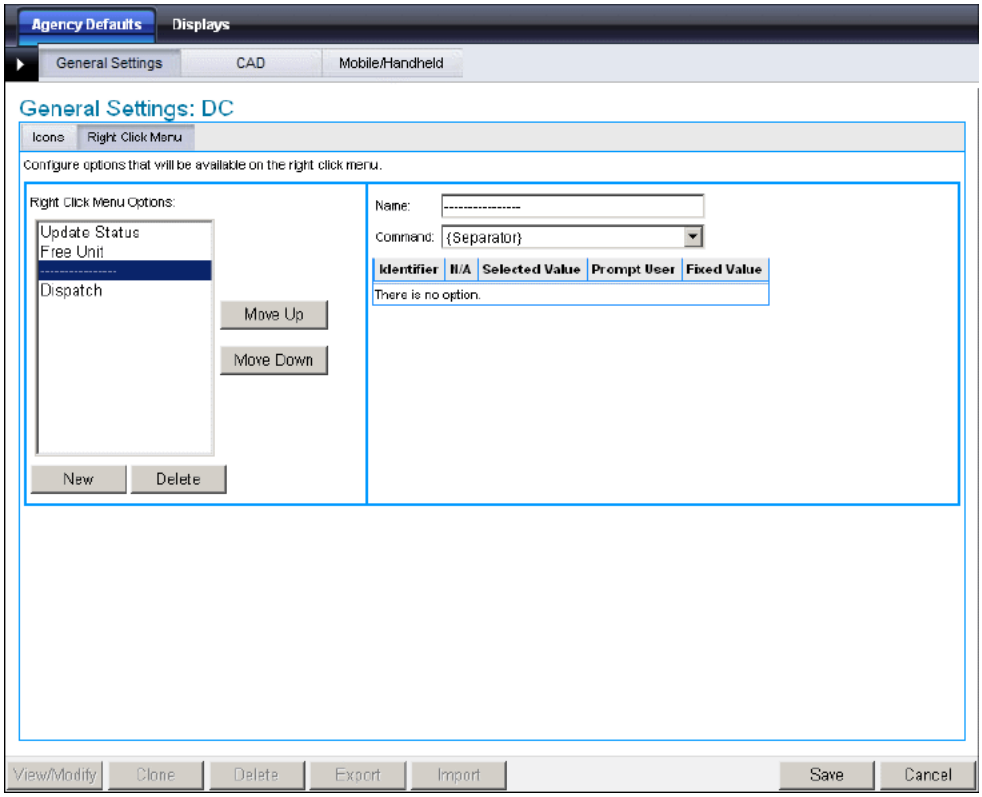


Figure 32-3 General Settings Form – Right Click Menu Tab

3. Click **View/Modify**.

4. At the bottom of the Right Click Menu Option box, click the **New** button.

   The menu option New Option is added.

5. In the Name field, type a name for the command you want to add.

6. From the Command list, select the PremierOne command you want to add to the agency's right-click menu.

(CC) is used to indicate Call Control window commands. For NG, the command identifiers for Action, Line Number, and Phone number are included. For all other call control actions, there are no identifiers.

NOTE

If a context menu is provisioned with actions that cannot be performed due to the status of the call or position, the actions will be disabled.

The table below the Command field changes to list the appropriate identifiers for the command.

For each identifier, select one of the following options:

- N/A – The identifier is not required.
- Selected Value – Use the value for the identifier that is in the row for the incident or unit in the status monitor.
- Prompt User – Prompt the user for a value for the identifier, such as the incident ID for associate incident.
- Fixed Value – Use the value you enter, such as the unit status EN for enroute.

7. Click **Save**.
8. Repeat to add any other commands.

   You can add a separator between commands by selecting the {Separator} value.

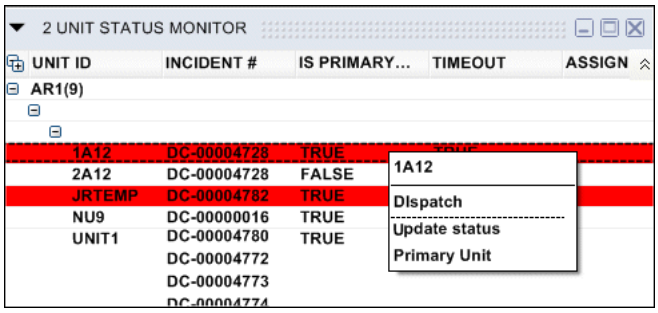


Figure 32-4 Example of Separator for Right-Click Menu Options

The following table provides additional information for configuring right-click options for Call Control.

Table 32-1 Right-Click Options Voice Call Control

Action	Description
Activate TDD Action	Activates TDD while the call taker is handling a currently active voice call (a call in TALK status). While TDD is automatically sensed and activated when necessary, the call taker still has control to activate TDD in case of TDD communication anomaly. (Must be in TALK state).
Terminate TDD Action	Terminates TDD while the call taker is handling a currently active voice call (a call in TALK status). While TDD terminates automatically when a call is released, the call taker still has control of TDD if the call taker wants to terminate the TDD session during a call to enable verbal conversation.
Add Note Action	Displays a dialog box where the call taker can add notes to any voice call or SMS text. (Call/SMS may be in any state).
Barge In Action	Allows the call taker to “Barge In” on another position to converse with the other position’s user and current caller. (Must be in TALK state).
Conference (no-hold) Action	Allows the call taker to initiate a no-hold conference with the currently active voice call. (Must be in TALK state).
Conference (standard) Action	Allows the call taker to initiate a standard (caller placed on hold) conference with the currently active voice call. (Must be in TALK state).
Dial Position Action	Allows the call taker to call another position. This function dials the other position’s intercom lines. The call taker must not be in TALK state).
Join Action	Allows the call taker to join another position and converse with the other position’s user and caller. This function is normally reserved for supervisors. (The other position must be in a TALK state and the call taker must not be in TALK state).
Listen Action	Allows the call taker to listen to another position and hear (but not talk) with the other position’s user and caller. This function is normally reserved for supervisors. (The other position must be in a TALK state). (Must not be in TALK state).
Disconnect List & Join Action	Allows a call taker that has initiated a Listen and/or Join action to terminate the Listen or Join function. (Call may be in any state).
Make Abandoned Action	Allows a call taker to return an Abandoned Call Notification to the ABANDONED state. Call may be in any state).
Clear Action	Allows a call taker to clear an Abandoned Call Notification from the Abandoned Calls list. (Call may be in any state).
Playback Action	Allows the call taker to select a voice call from a status monitor and initiate the playback of the audio recording of that voice call. (Must not be in TALK state).
Start Incident Action	Allows the call taker to initiate an incident in CAD where the voice call/SMS that is selected is automatically associated to the incident being created. (Call may be in any state).

Table 32-1 Right-Click Options Voice Call Control

Action	Description
NG Call Control Command	The actions available when creating a right click menu option using the NG Call Control Command are: • Answer (voice call) • Release (voice call) • Mute • Callback (voice call) • Dial (outgoing voice call) • Hold (and Unhold) (voice call) • Park (voice call) • ACD State Change (toggle ready/not ready) • Rebid (voice call) • Transfer (voice call)

Configuring CAD Status Monitor Settings – Agency Defaults

Use the CAD tab to define incident and unit status colors, fonts, and background colors for your Agency Default settings for CAD status monitors. The tab contains the following subtabs:

- Unit Status Colors – Where you set the colors for the text that displays for normal and timeout situations in the CAD Unit Status monitor.
- Incident Status Colors – Where you set the colors in which each incident status will appear on the status monitor in normal and timeout situations.
- Call Control Colors – Where you set the colors for call status and position state for Call Control windows in normal and timeout situations.
- Fonts – Where you define values for font, font style, and font size for CAD status monitors.
- Monitor background color – Where you define the background color for CAD status monitors.

Configuring CAD Unit Status Colors

Use the Unit Status Colors tab to set the colors for the text that displays for normal and timeout situations in the CAD Unit Status monitor. You can set the colors for the fonts and the background.

Unit status timeouts are defined in Unit Management – Unit Status Codes. For details, see “Configuring Unit Status Codes” on page 10-11.

NOTE

Labels for icons on the CAD and Mobile/Handheld maps use the same colors as defined for status monitors.

To configure CAD unit status colors:

1. Access the form for Agency Defaults. For instructions, see “Configuring General Status Monitor Settings– Agency Defaults” on page 32-3.
2. Click the CAD tab.

   The CAD form appears.
3. Click **View/Modify**.

   The Unit Status Colors form refreshes, and the fields are now editable.

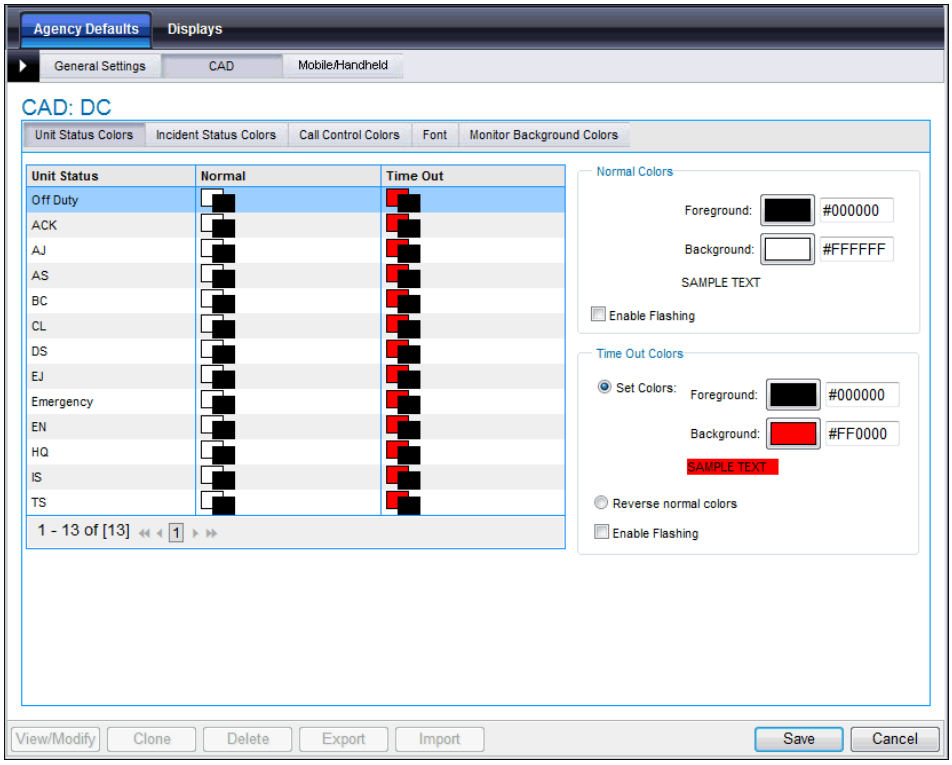


Figure 32-5 CAD Form — Unit Status Colors Tab

4. Select a unit status whose colors you want to change.
5. Set the Normal Colors and Timeout Colors as follows:

   a. Click the colored square next to the Foreground or Background label.

   b. When the color palette appears, click the color you want, and then click **OK**.

The colored square and the sample text display the selected foreground and background colors.

c. To enable flashing for a specific unit status, such as an emergency status, select the **Enable Flashing** check box.

d. To reverse the normal colors for your timeout colors, select the **Reverse normal colors** check box in the Time Out Colors box.

e. Ensure that your text can be easily read by reading the sample text in the box.

6. Click **Save**.

Configuring CAD Incident Status Colors

The Incident Status Colors tab is where you set the colors in which each incident status will appear on the status monitor in normal and timeout situations. You can set the colors for the fonts and the background.

Incident status timeouts are defined in Incident Management – Service Settings – Timeouts. For details, see "Configuring Incident Timeouts" on page 13-26.

NOTE

Labels for icons on the CAD and Mobile/Handheld maps use the colors as defined for status monitors.

To configure CAD incident status colors:

1. Access the CAD agency defaults form. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

2. Click the CAD tab.

   The CAD form appears.

3. Click the Incident Status Colors tab.

   The Incident Status Colors form appears.

4. Click **View/Modify**.

The Incident Status Colors form refreshes, and the fields are now editable.

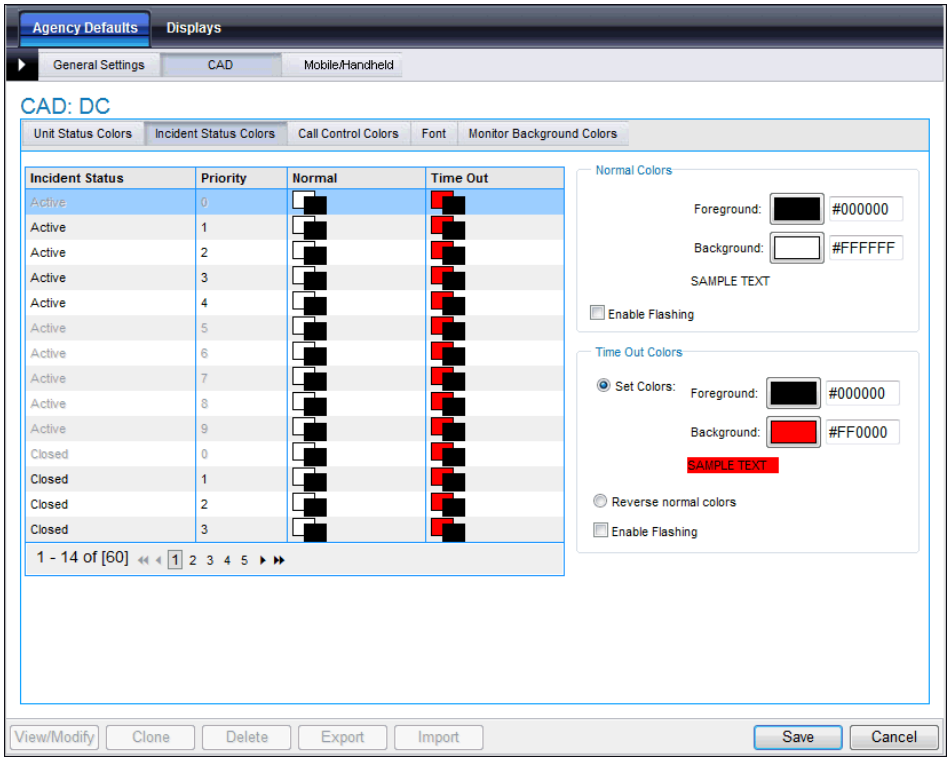


Figure 32-6 Agency Defaults Form – Incident Status Colors Tab

5. Select an incident status and priority combination with the colors you want to change.

6. Set the Normal Colors and Timeout Colors as follows:

   a. Click the colored square next to the Foreground or Background label.

   b. When the color palette appears click the color you want, and then click **OK**.

      The colored square and the sample text display the selected foreground and background colors.

   c. To enable flashing for a specific unit status, such as an emergency status, select the **Enable Flashing** check box.

   d. To reverse the normal colors for your timeout colors, select the **Reverse normal colors** check box in the Time Out Colors box.

   e. Ensure that your text can be easily read by reading the sample text in the box.

7. Click **Save**.

Configuring Call Control Colors

The Call Control Colors tab is where you set the colors for calls in a specific status or state in a Call or Position Call Control window. You can set the colors for the fonts and the background. Colors provisioned are applied to Call and Position windows that are provisioned to display as status monitor windows only. Windows that are provisioned to display as lists in the List region ignore these settings.

Timeout settings are only available for the Hold, iHold, iHold-C ("Held to long" limit), and Active and Updated ("Idle to Long" limit) statuses.

To configure CAD Call Control colors:

1. Access the CAD agency defaults form. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

2. Click the CAD tab.

   The CAD form appears.

3. Click the Call Control Colors tab.

   The Call Control Colors form appears.

4. Click **View/Modify**.

   The Call Control Colors form refreshes, and the fields are now editable.

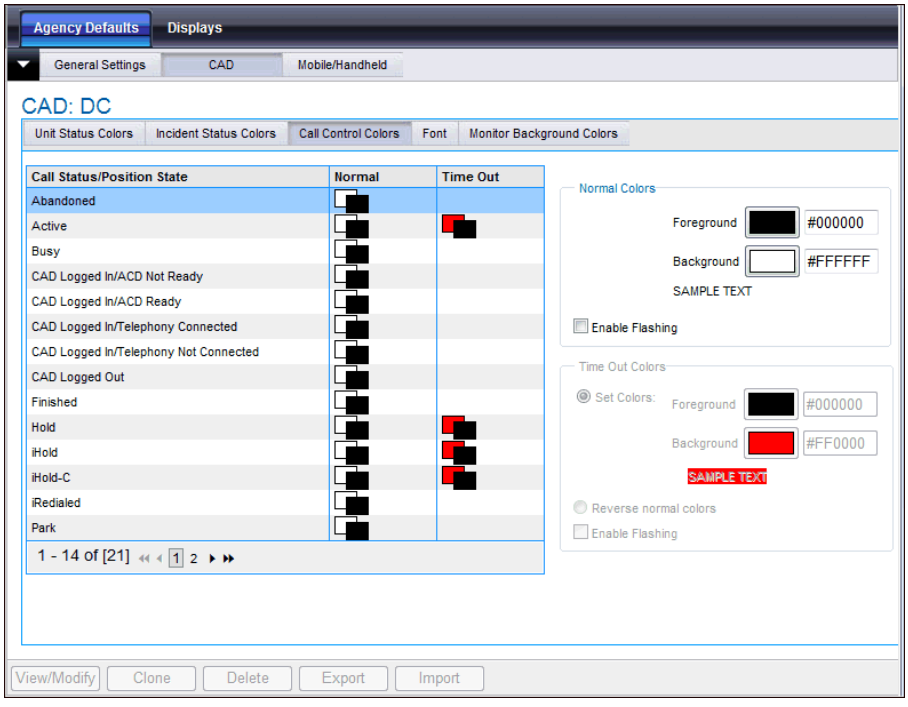


Figure 32-7 Agency Defaults Form – Call Control Colors Tab

5. Select a call status/position state with the colors you want to change.

6. Set the Normal Colors and Timeout Colors as follows:

   a. Click the colored square next to the Foreground or Background label.

   b. When the color palette appears click the color you want, and then click **OK**.

      The colored square and the sample text display the selected foreground and background colors.

   c. To enable flashing for a specific status, select the **Enable Flashing** check box.

      You cannot configure text to flash on a status monitor for voice calls in FINISHED state and SMS texts in TERMINATES status is also not allowed. These states can still have any color set to them but they cannot flash.

   d. To reverse the normal colors for your timeout colors, select the **Reverse normal colors** check box in the Time Out Colors box.

   e. Ensure that your text can be easily read by reading the sample text in the box.

7. Click **Save**.

Configuring Status Monitor Fonts for the Default CAD Display

Use the Font tab on the CAD form to define values for font, font style, and font size for CAD status monitors. These fonts are used in status monitors unless you choose to create overrides in either of the following locations.

- Individual monitors in Display Sets (groups of monitors). For details, see “Configuring Status Monitor Fonts for Display Sets” on page 32-53.
- Monitors in Display Sets. For details, see “Configuring Status Monitor Fonts for Individual CAD Monitors” on page 32-54.

To configure CAD status monitor fonts:

1. Access the form for Agency Defaults. For instructions, see “Configuring General Status Monitor Settings– Agency Defaults” on page 32-3.
2. Click the CAD tab.

   The CAD form appears.

3. Click the Font tab.

   The Fonts form appears.

4. At the bottom of the Fonts form, click **View/Modify**.

The Fonts form refreshes, and the fields are now editable.

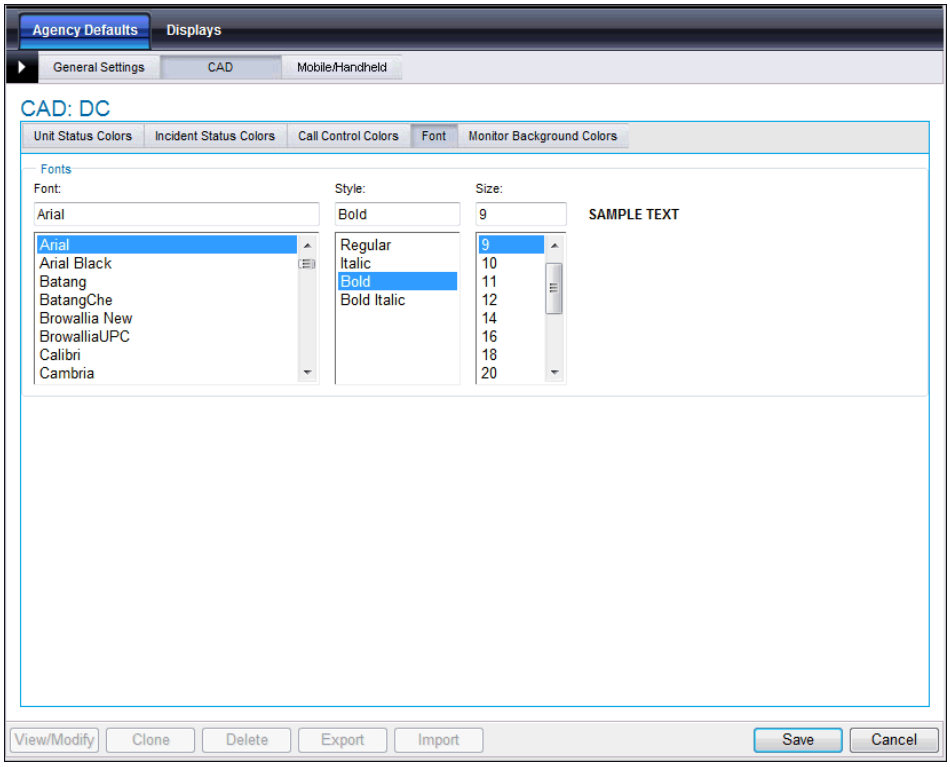


Figure 32-8 CAD Form — Font Tab

5. Select the font, style, and size of text you want to use as the defaults.

   The sample text on the right side of the form displays an example of the selections.

6. Click **Save**.

Configuring the Monitor Background Color

Use the Monitor Background Colors tab on the CAD form to set the background colors for CAD monitors.

To configure CAD monitor background colors:

1. Access the CAD Agency Defaults form. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

2. Click the **CAD** tab.

   The CAD form appears.

3. Click the Monitor Background Colors tab.

   The Monitor Background Colors tab appears.

4. Click **View/Modify**.

The form refreshes, and the fields are now editable.

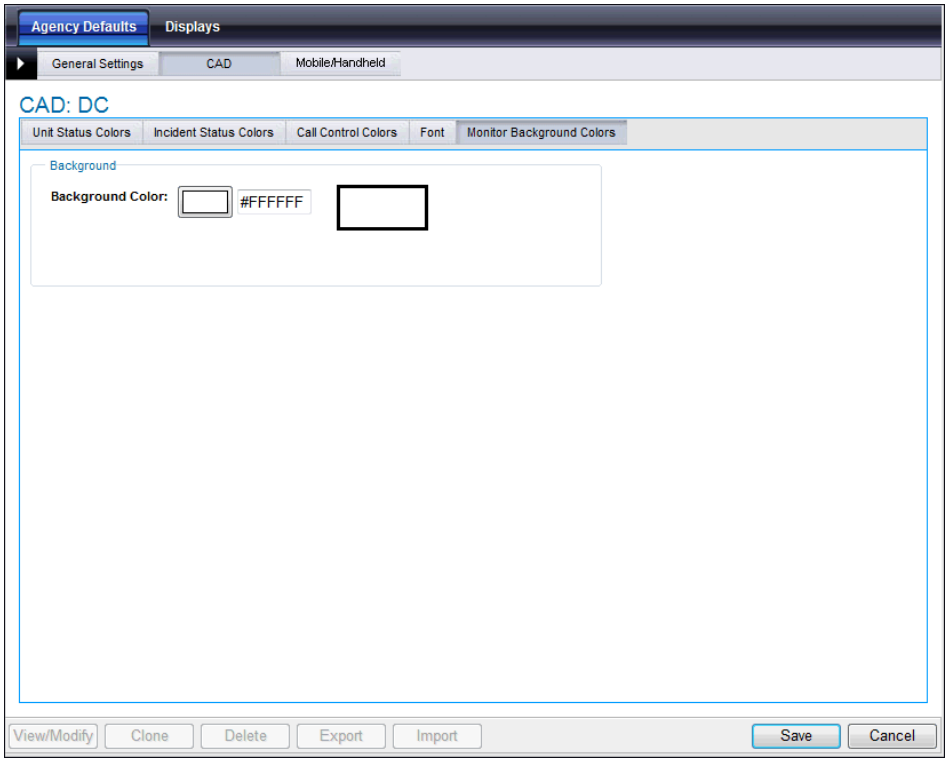


Figure 32-9 CAD Form — Monitor Background Colors Tab

5. In the text field, enter the HTML code for the color. You can alternatively click in the Background Color box and a Color dialog box will display where you can select the color.

   The color you enter displays in the Background Color box. The larger box to the right shows how the background color of the monitor will appear.

6. Click **Save**.

Configuring Mobile/Handheld Status Monitor Settings – Agency Defaults

Use the Status Monitors Mobile/Handheld tab to define incident and unit status colors and fonts for your agency's mobile and handheld units. Use the Status Monitors CAD tab to define incident and unit status colors and fonts for CAD status monitors. The tabs contains the following subtabs:

- Unit Status Colors – Where you set the colors for the text that displays for normal and timeout situations in the CAD Unit Status monitor.
- Incident Status Colors – Where you set the colors in which each incident status will appear on the status monitor in normal and timeout situations.

- Font – Where you define values for font, font style, and font size for CAD status monitors.
- Mobile/Handheld Defaults – Where you specify whether to display closed incidents and how long closed incidents are displayed.

Configuring Mobile/Handheld Unit Status Colors

Use the Unit Status Colors tab to set the colors for the text that displays for normal and timeout situations in the Mobile/Handheld Unit Status monitor.

NOTE

Labels for icons on the CAD and Mobile/Handheld maps use the colors as defined for status monitors.

To configure Mobile/Handheld unit status colors:

1. Access the form for agency defaults. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.
2. Click the **Mobile/Handheld** tab.

   The Mobile/Handheld form appears.
3. Click **View/Modify**.

   The Unit Status Colors form refreshes, and the fields are now editable.

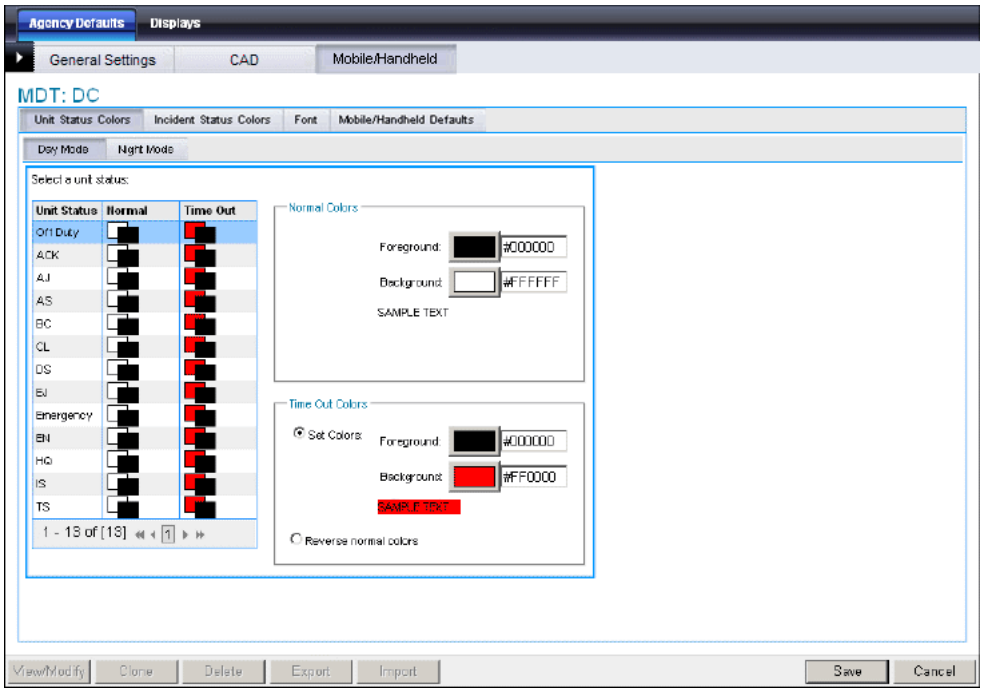


Figure 32-10 Mobile/Handheld Form — Unit Status Colors Tab

4. Select a unit status with the colors you want to change.
5. Set the Normal Colors and Timeout Colors as follows:
   a. Click the colored square next to the Foreground or Background label.
   b. When the color palette appears, select the color you want, and then click **OK**.
   c. To enable flashing for a specific unit status, such as an emergency status, select the **Enable Flashing** check box.
   d. To reverse the normal colors for your timeout colors, select the **Reverse normal colors** check box in the Time Out Colors box.
   e. Ensure that your text can be easily read by reading the sample text in the box.
6. Click **Save**.

Configuring Mobile/Handheld Incident Status Colors

Use the Incident Status Colors tab to set the colors for the text that displays for normal and timeout situations in the CAD Unit Status monitor.

NOTE
Labels for icons on the CAD and Mobile/Handheld maps use the colors as defined for status monitors.

To configure Mobile/Handheld incident status colors:

1. Access the form for agency defaults. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

   The Agency Defaults form appears (see Figure 32-1).

2. Select the Incident Status Colors tab.

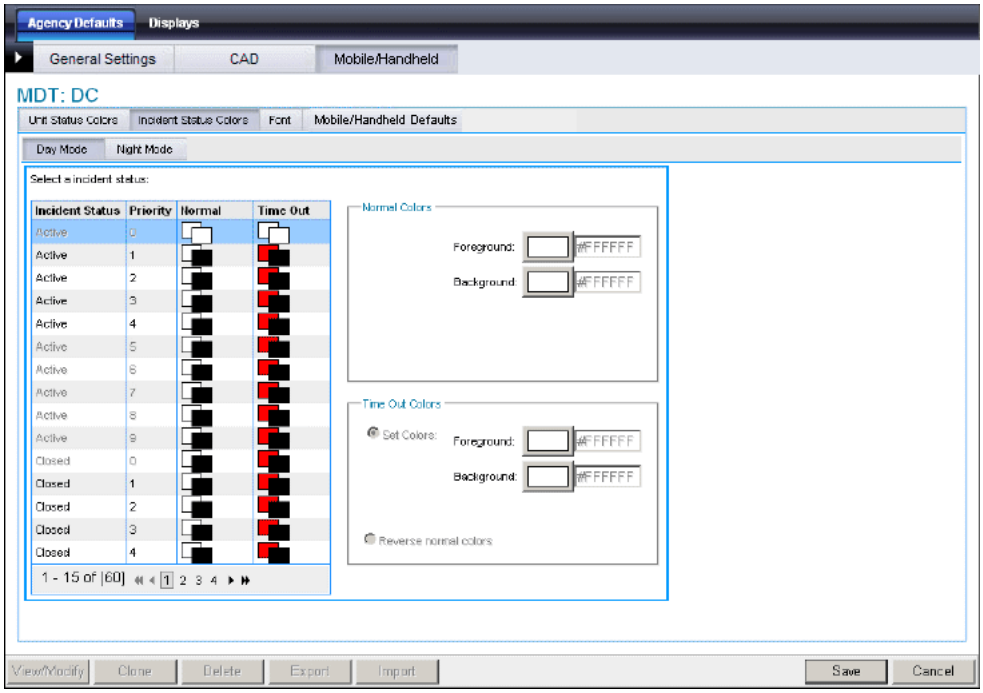


Figure 32-11 Mobile/Handheld Form – Incident Status Colors Tab

3. Click **View/Modify**.

4. Select an incident status and priority combination with the colors you want to change.

5. Set the Normal Colors and Timeout Colors as follows:

   a. Click the colored square next to the Foreground or Background label.

      When the color palette appears, select the color you want, and then click **OK**.

   b. To enable flashing for a specific unit status, such as an emergency status, select the **Enable Flashing** check box.

   c. To reverse the normal colors for your timeout colors, select the **Reverse normal colors** check box in the Time Out Colors box.

   d. Ensure that your text can be easily read by reading the sample text in the box.

6. Click **Save**.

Configuring Mobile/Handheld Status Monitor Fonts

Use the Font tab to define default values for font, font style, and font size for Mobile/ Handheld status monitors.

To configure Mobile/Handheld status monitor fonts:

1. Access the form for Agency Defaults. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

2. Click the Mobile/Handheld tab.

   The Mobile/Handheld form appears.

3. Click the **Font** tab.

   The Fonts form appears.

4. At the bottom of the Fonts form, click **View/Modify**.

   The Fonts form refreshes, and the fields are now editable.

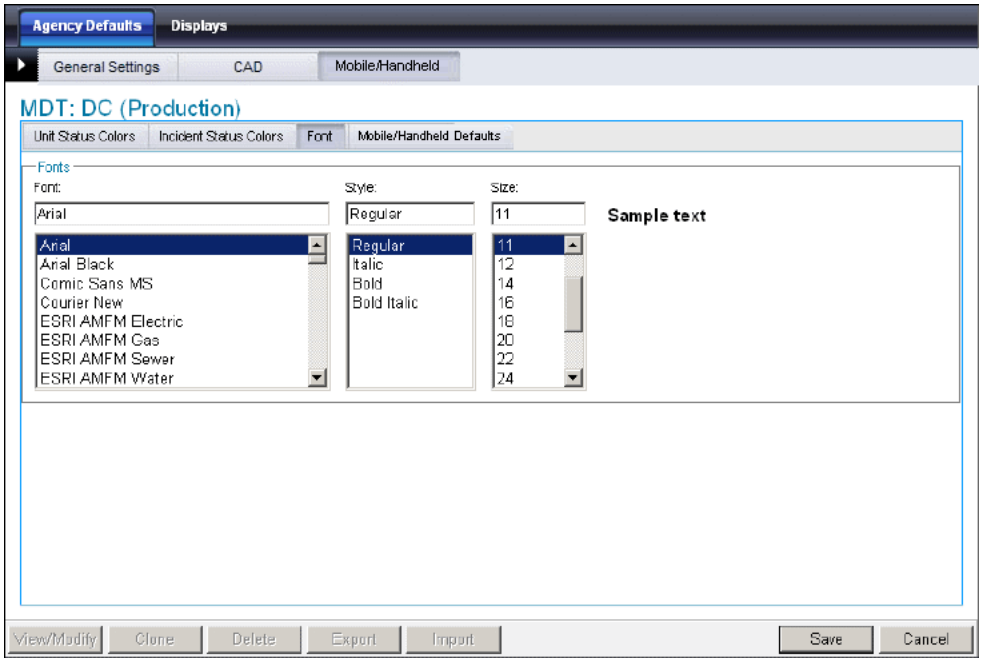


Figure 32-12 Mobile/Handheld Form – Font Tab

5. Select the font, style, and size from the lists, and then click **Save**.

   The sample text on the right side of the form displays the selected font.

6. Click **Save**.

Configuring Closed Incidents for Mobile/Handheld Status Monitors

Use the Mobile/Handheld Defaults tab to specify whether to display closed incidents and how long closed incidents are displayed.

To configure closed incidents for Mobile/Handheld status monitors:

1. Access the form for Agency Defaults. For instructions, see "Configuring General Status Monitor Settings– Agency Defaults" on page 32-3.

2. Click the Mobile/Handheld tab.

   The Mobile/Handheld form appears.

3. Click the Mobile/Handheld Defaults tab.

   The Mobile/Handheld Defaults form appears.

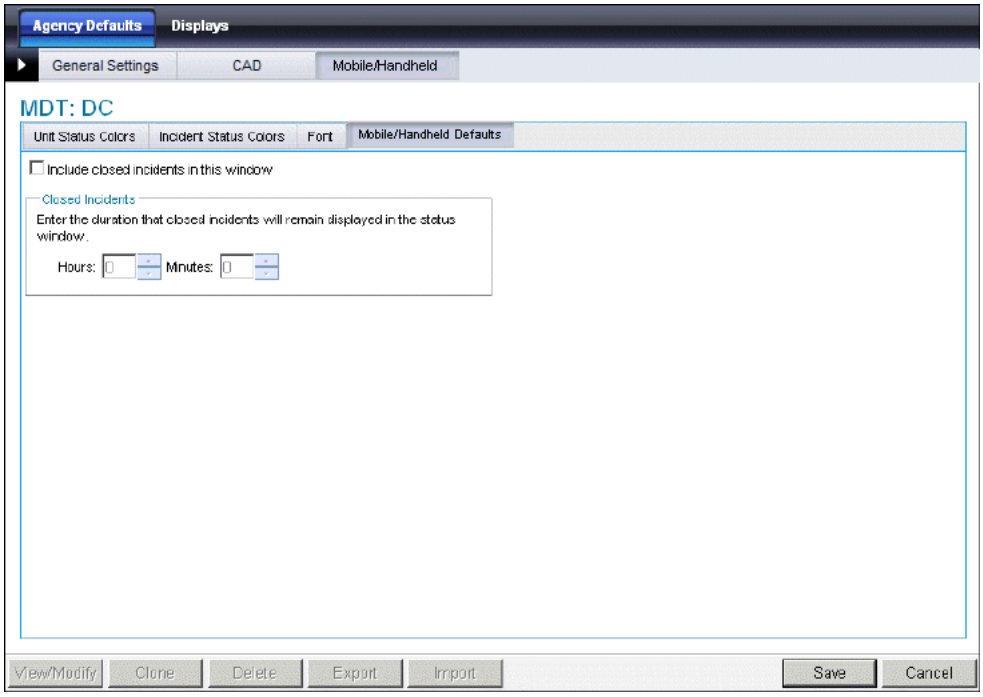


Figure 32-13 Mobile/Handheld Form – Mobile/Handheld Defaults Tab

4. At the bottom of the form, click **View/Modify**.

   The form refreshes, and the fields are now editable.

5. To include closed incidents in the status monitor window, selected the **Include closed incidents in this window** check box.

6. Enter the duration the closed incidents will remain in the status window.

7. Click **Save**.

Adding Status Monitor Displays

Use the Displays configuration item to add custom status monitor displays for a specific group, such as call takers and dispatchers, or for a specific purpose, such as training.

Adding CAD Status Monitor Displays

Add CAD status monitor displays when you need a custom display for a specific group, such as call takers, or for a specific purpose, such as training. When you add status monitor displays, you enter information on three tabs and view monitor displays on a fourth tab.

- General – Where you enter the display name, select who the display is available to, select where the display is accessible from, and select a refresh point for the display's data.
- Windows – Where you set each status monitor type, its fields, sorting, filtering, grouping, window position, alerts, right-click menu options, and colors.
- Font – Where you set the font for the Display Set of status monitors.

You can add, modify, clone, and delete status monitor displays. For details on cloning and deleting, see "Working With Configuration Items" on page 2-9.

NOTE

Users can have access to more than one status monitor configuration. In this case, the first configuration you create is the status monitor that displays by default when the user first logs on. The user can select a different configuration from the CAD client by selecting **Status Monitors** from the Utilities menu.

Adding CAD Status Monitor General Information

Status monitor general information includes the status monitor display name, for whom the display is available, from where the display is accessible, and the refresh point for the display's data.

To add status monitor general information:

1. From the Navigation panel, select **Status Monitor**, and then select **Displays**.

   The Displays form appears. A list of existing records displays on the left side of the form.

If you selected Existing in the filter, then a list of existing records displays. If you entered search criteria in the filter, only the matching records display.

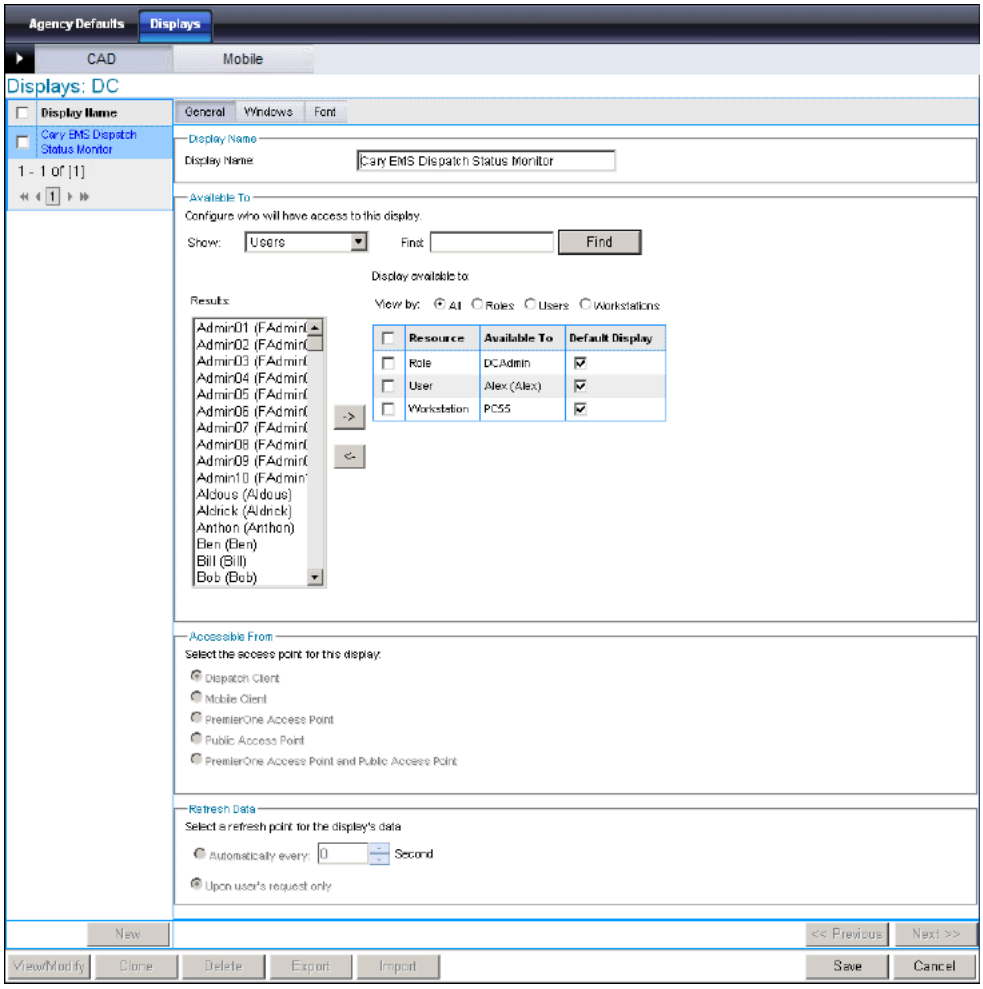


Figure 32-14 Displays Form – General Tab

2. Select the CAD tab.

3. In the Display Name field, type a name for your new display. This is the *group* name for all the status monitor windows for this specific group of people.

4. In the Available to section, specify to whom this group of status monitor windows is available.

   a. From the Show list, select **Users**, **Roles**, or **Workstations**.

      A list of users, roles, or workstations appears in the Results box.

   b. Select the users, roles, or workstations who will have access from the list.

      You can select more than one category, such as roles *and* users.

Your selections display in the table to the right.

c. If you selected more than one category, be sure to select **View by All**.

5. In the Accessible From section, select the access point for the status monitor.

   - To access the status monitor only from CAD, select **Dispatch client**.
   - To access the status monitor only from Mobile, select **Mobile client**.
   - To access the status monitor from Provisioning, select **PremierOne Access Point**.
   - To access the status monitor from a public workstation, select **Public Access Point**.
   - To access the status monitor from Provisioning and from a public workstation, select **PremierOne Access Point** and **Public Access Point**.

6. In the Refresh Data section, select how often to refresh the display's data in seconds.

7. Click **Save**.

Adding CAD Status Monitor Window Information

Status monitor window information includes the following topics, each of which is configured on its own tab: General, Fields, Sorting, Filtering, Grouping, Position, Alerts, Right Click Menu, Font, and Color.

Adding Windows General Information

Use the General tab to select the name of the status monitor type, the display record counter, the data display options, and options for closed incidents, displaying multiple values, and specific status monitor options.

To add windows general information:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add windows information.

3. Select the Windows tab.

   The General subtab appears.

4. Click **View/Modify**.

The fields become editable.

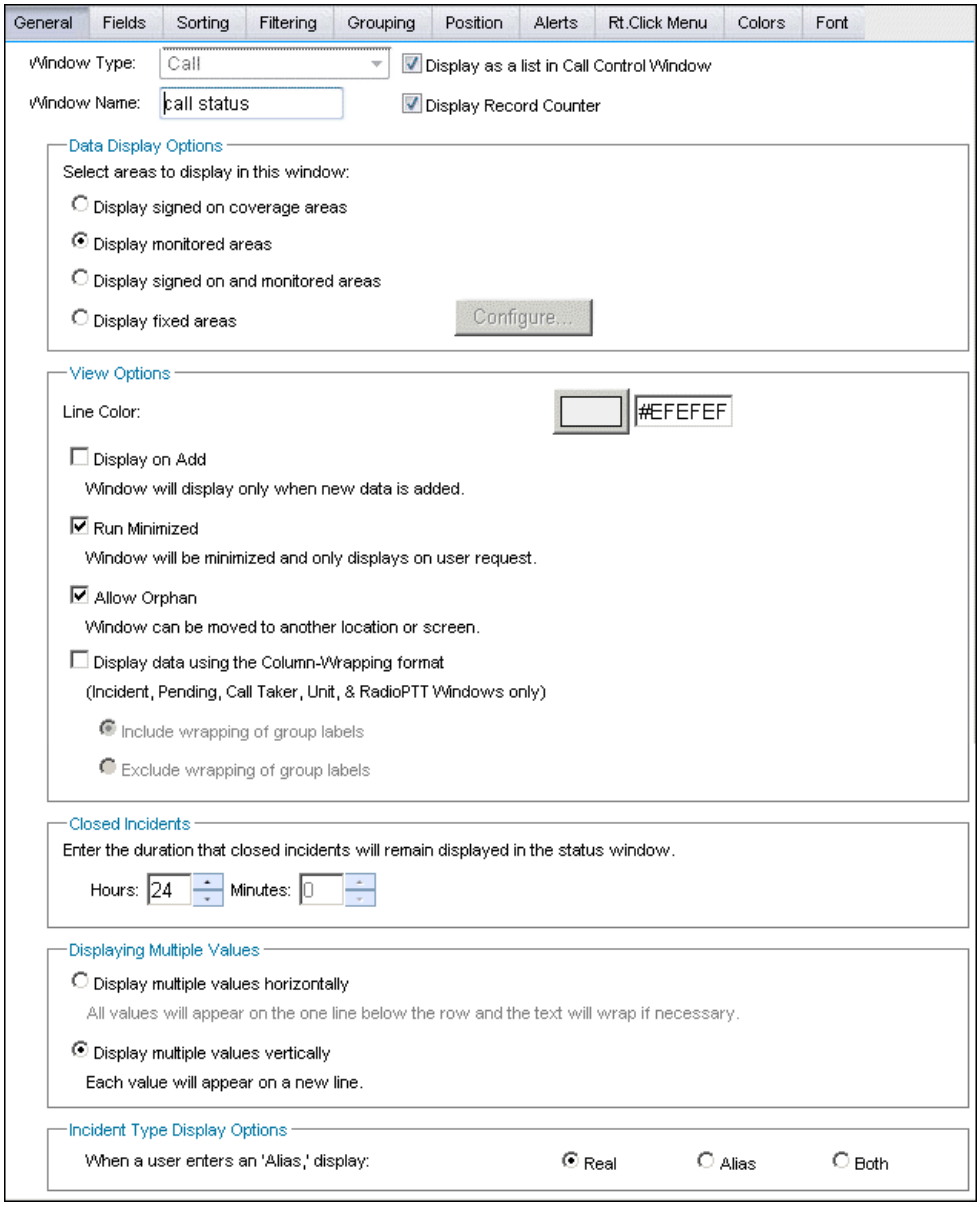


Figure 32-15 Displays Form – Windows Tab, General Subtab - Top

5. From the Window Type list in the General subtab, select the type of status monitor. Options include the following:

   - Call – Displays NG9-1-1 call-related information.

     A call is defined as voice call (includes TDD), an SMS Text conversation, or an abandoned call's associated abandoned call notification.

     When you select this option, the **Display as a list in Call Control window** check box displays. If you want the fields to display as a list in the List region of the Call Control window, and not as a standard status monitor, select this check box.

- Call Taker – By default, displays incidents in all statuses: active, pending (or initial), open, stacked, and closed.

  You can configure how long closed incidents remain in the display in the Closed Incidents section on this tab. You can filter any statuses you don't want to display using the Incident Status field on the Filters tab.

- Incident – By default, displays active and open incidents.

  You can configure whether pending (or initial) and closed incidents display in the Incident Status Monitor Options section on this tab. You can filter out any statuses that are displayed but you cannot add a status that is not active, open, pending, or closed.

- Interface – Displays the current status of interfaces being used with CAD.

  NOTE
  The Interface status monitor supports only server-side devices. Client-side devices such as two-tone alert systems running on the Gold Elite radio system are not supported on the Interface status monitor. Instead, its status is shown on the Console CAD Proxy.

- Pending Incident– By default, displays pending (initial) incidents.

  You can configure whether active incidents display in the Pending Incident Status Monitor section on this tab. There is no way to configure more than pending (initial), and active incidents to display in this window.

- Position – Displays NG9-1-1 position-related information for workstations.

  A position is defined as a PremierOne workstation that is also identified by a 9-1-1 position ID and is associated to the Call Control service.

  When you select this option, the **Display as a list in Call Control window** check box displays. If you want the fields to display as a list in the List region of the Call Control window, and not as a standard status monitor, select this check box.

- Radio PTT – Displays information regarding push-to-talk radio transmissions.

- Supervisor – Displays the activities in the call center by area (all of the supervisor windows have the same fields available for display): number of pending incidents, number of non-pending incidents, total number of available units; the incident numbers of pending incidents that are overdue and awaiting arrival; and number of incidents assigned to each dispatcher by area.

- SupervisorOnDispatcher – Displays information for a supervisor acting as a dispatcher.

  NOTE
  Do not use this status monitor at this time.

- SupervisorOnIncident – Displays information for a supervisor acting as a call taker.

> **NOTE**
> Do not use this status monitor at this time.

- Toning System – Displays information about your toning system.

  When you check the Enable Toning System Status Monitor field (in the Toning System Status Monitor Options section), you must also check at least one display option (station or RTU). You can display both.

- Unit – Displays unit status and unit information.

- Workload Transfer – Displays the incidents transferred to or from a console using workload transfer transactions.

6. In the Window Name field, type a descriptive name for the status monitor.

7. Select whether you want this window to display a counter of the total number of records.

8. In the Data Display Options section, select the areas to display in this window.

   - Display signed on coverage areas – This type of monitor displays only the areas that are in the user's Coverage Group.

   - Display Monitored areas – This type of monitor can display areas other than those to which the user is assigned. Users can issue the MA command to display those areas.

   - Display signed on and monitored areas – This type of monitor displays signed on coverage areas and monitored areas.

   - Display fixed areas – This type of monitor shows only a fixed set of areas and is most commonly used for remote people who are responsible for covering set areas. For a monitor with a fixed display, you cannot change the coverage display of the monitor with any of the CAD commands.

   If you select **Display fixed areas**, click **Configure** to select the areas.

9. In the View Options section, select the view options.

   - Line Color – Click the color box and select a line color for grid rows and columns. The HTML code displays to the right of the box. If you display data in a column format, this color will also be used to shade the background of the labels.

   - Display on Add – Select this option to only display the status monitor when new information is added. In this case the status monitor will automatically maximize.

- Run Minimized – Select this option to start the status monitor in a minimized state when CAD is started. After CAD is started, the window can be displayed, minimized, or maximized. The user can manually minimize a status monitor window that is configured to Display on Add after the window has been displayed.

- Allow Orphan – Select this option if you want the user to be able to move the status monitor to any location on the workstation display.

- Display data using the Column-Wrapping format – Select this option to display items from top to bottom, and then horizontally across the width of the window. This displays the data in continuous columns or rows across the window so that you do not have to scroll through the window to see all the information.

  When you select this option, the Include the wrapping of group labels and the Exclude the wrapping of group labels fields are enabled.

  - To display groups column across the window, select **Include the wrapping of group labels**. This is the default.

Example:

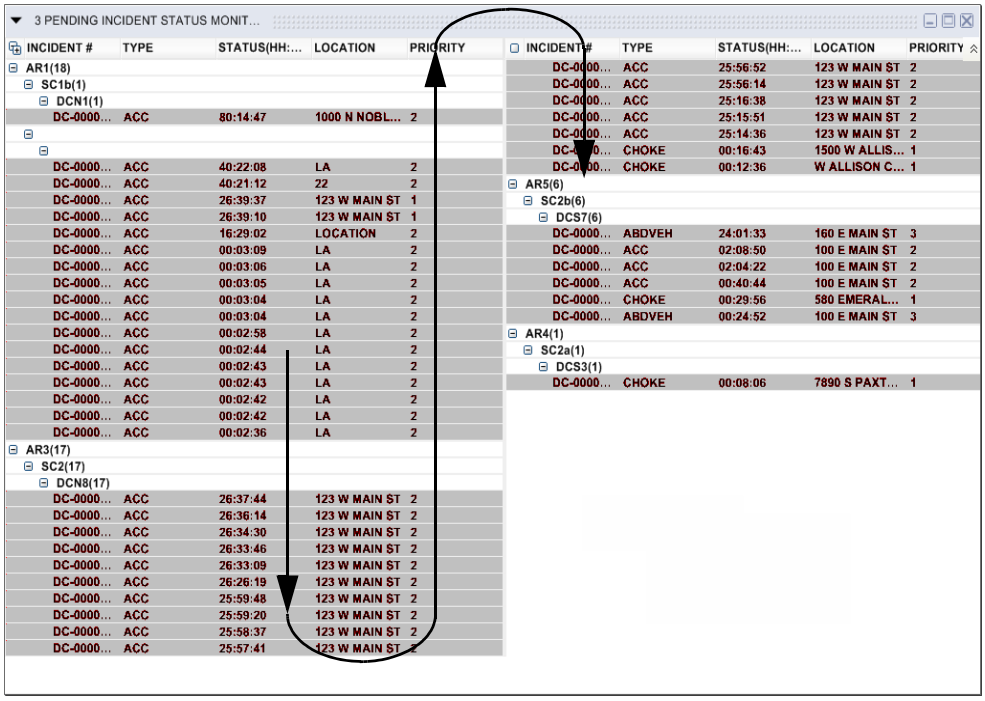


Figure 32-16 Status Monitor With Column Wrapping Included

- To display groups in a single row across the width of the window, select **Exclude the wrapping of group labels**.

Example:

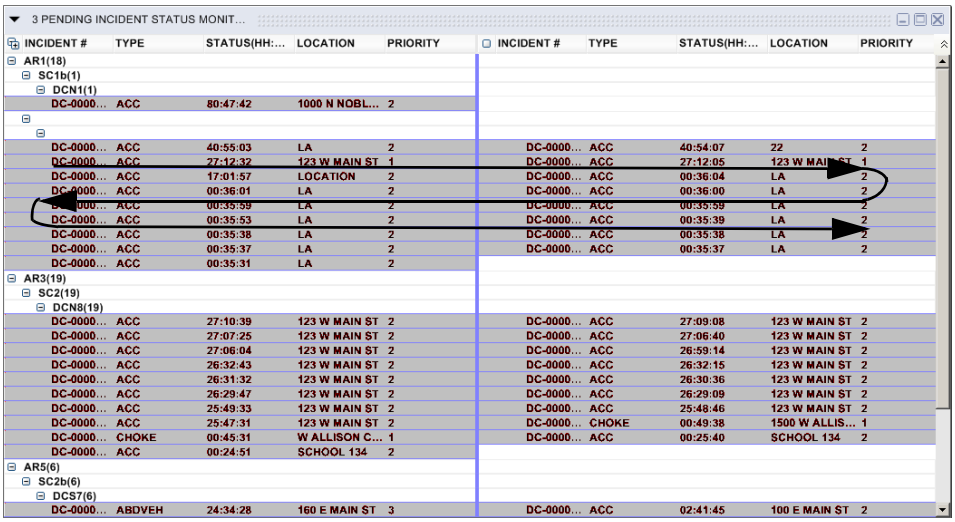


Figure 32-17 Status Monitor With Column Wrapping Excluded

Column-wrapping settings are available for the following status monitors:

- CallTaker
- Incident
- Pending Incident
- Radio PTT
- Unit

10. In the Closed Incidents section, enter the duration that closed incidents remain displayed in the status window.

11. In the Displaying Multiple Values section, select how multiple values are displayed on the status monitor.

    - For all values to appear on the line below the row, select the Display multiple values horizontally check box. When necessary, the text wraps to additional lines.

    - For each value to appear on a new line, select the Display multiple values vertically check box.

12. In the Incident Type Display Options section, do one of the following:

- To only display the real incident type in the status monitor, select **Real**.
- To only display the alias incident type in the status monitor, select **Alias**.
- To display both the real and alias incident type, select **Both**.

  The display will be in the format real incident type - alias incident type, such as `trafficaccident - tra`.

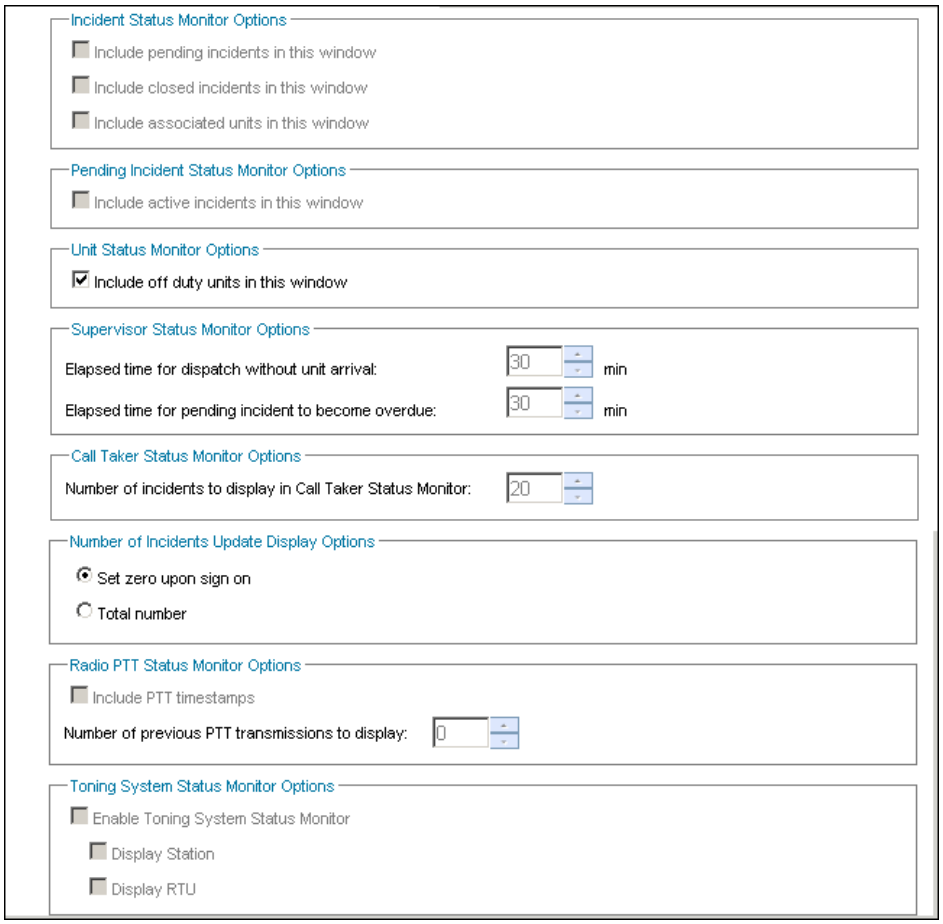


Figure 32-18 Displays Form – Windows Tab, General Subtab - Bottom

13. For Incident Status Monitor Options, do any of the following:

- To display pending incidents in the status monitor, select the Include pending incidents in this window check box.
- To display closed incidents in the status monitor, select Include closed incidents check box.
- To display units on associated incidents in the status monitor, select include associated units in this window check box.

14. To include active incidents in the Pending status monitor, select Include active incidents in this window check box. Otherwise only pending incidents display.

15. To display off duty units in the Unit Status monitor, select the Include off duty units in this window check box.

16. For Supervisor Status Monitor Options, do any of the following:

    - Enter the number of minutes that can pass before a dispatched unit is considered overdue.

    - Enter the number of minutes that can pass before a pending incident is considered overdue.

    The supervisor status monitor displays a manual count of each of these items.

17. For Call Taker status monitor Options, enter the number of incidents to display at a time in the Call Taker status monitor.

18. If you are provisioning the Incident Update Count field to display on the status monitor, select one of the following in the Number of Incidents Update Display Options section:

    - To reset the updates for an incident to zero when a new user signs on, select Set zero upon sign on.

    - To keep a count of the incident updates, select Total number.

19. For Station Alert Status Monitor Options, enter the toning interface response time.

    The Station Alert status monitor displays the stage information for fire stations that are in an alert status; for example, stations that are currently being toned to respond to incidents.

20. For Radio PTT Status Monitor Options, do any of the following:

    - To display PTT time of transmissions in the status monitor, select the **Include PTT timestamps** check box. The check box is selected by default.

    - To display previous PTT transmissions, enter the number of previous transmissions you want to display. The value 20 is the default.

      All the provisioned fields for PTT monitor display in the order they are provisioned. The maximum number of radio transactions that are displayed is 30. The most recent radio transactions display on top of the list. If the number of transactions reaches more than 30, then the older transactions drop off the monitor.

      Attributes display using the following hierarchy: unit ID, vehicle ID, personnel ID, RIN or EID; for example, if the unit ID is available and the radio is associated with the officer ON DUTY then the unit ID is displayed.

If the emergency is keyed up by a unit, the emergency status is indicated on the PTT status monitor. The text color changes from to Red and Bold, and a red asterisk (*) is added in front of the ID field.

21. For Toning System Status Monitor Options, do any of the following:

    - To enable the toning system status monitor, select the **Enable Toning System Status Monitor** check box.
    - To display the station, select the **Display Station** check box.
    - To display the remote terminal unit (toning device ID), select the **Display RTU** check box.

      The ID can be a number or a name.

22. Click **Save**.

23. Repeat the previous steps for each status monitor you want to configure.

Adding Windows Fields

Use the Fields tab to select the fields that display for each window you chose on the General tab.

Before adding Windows fields, you must complete the steps in “Adding Windows General Information” on page 32-28.

To add windows fields:

1. Access the form for a new display. For instructions, see “Adding CAD Status Monitor General Information” on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add windows fields.

3. Select the Windows tab.

4. Select the Fields tab.

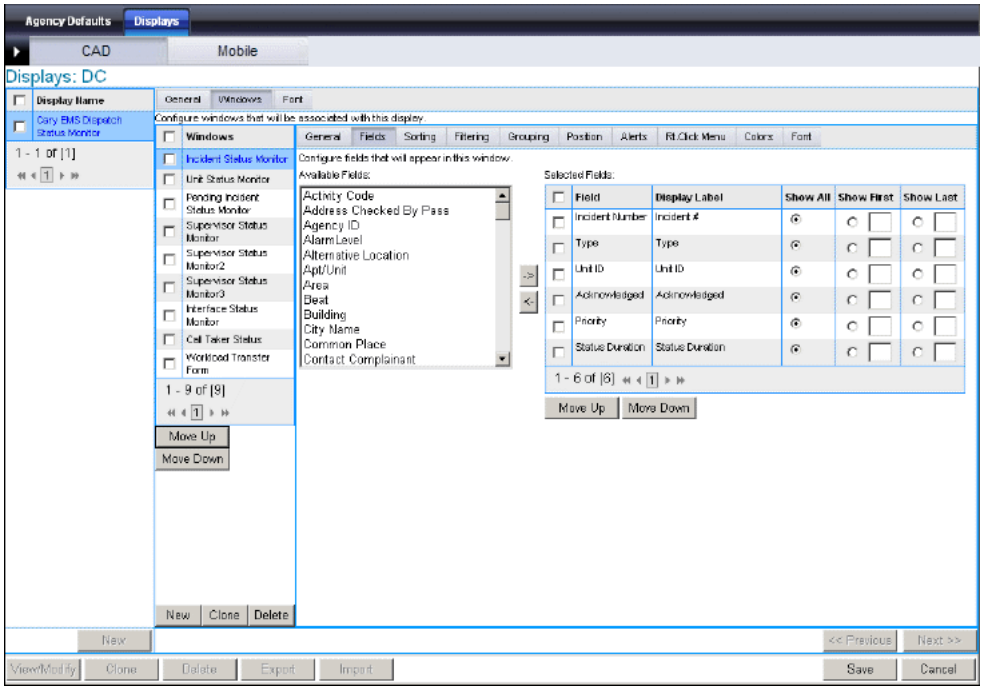


Figure 32-19 Displays Form – Windows Tab, Fields Subtab

5. From the Windows list on the left, select the window with the fields you want to configure.

6. From the Available Fields list, select the fields you want to appear on the status monitor.

   Each field appears in the Selected Fields table.

   For PTT status monitors, the PTT Source and Timestamp fields are added by default; you cannot remove the PTT Source field. To remove the Timestamp field, clear the Timestamp check box for PTT monitors on the General tab.

   For Unit Status monitors:

   - The Status Duration Timer tracks the amount of time a unit has been in a specific status. It only resets to zero when a user changes the unit status code, either by specifying a different unit status code than the unit's current status on the command line or the US form, or by specifying the same unit status code (as the unit's current status) on the command line.

   - The Updated Duration Timer tracks the duration since the unit was last updated by a user. It does not reset to zero when the unit times out. This timer is reset to zero when a user: 1) changes the unit's status (to the same or different unit status code); 2) submits the UO command; 3) submits a US command with changes to any other current activity data, such as Unit's Location, Dispositions, or

Working Capability; 4) changes any of the assignment data (such as Jurisdictions, Personnel, Vehicle, or Capabilities). The Updated Duration Timer is not reset based on any internal system activity, such as when the unit times out. It is only reset based on a user action against the unit.

- Every comment added by a unit is appended in the status monitor window, creating a new line for each comment.

To change the Display Label, click in the Display Label field so the field becomes and editable box, and then type the label you want to display.

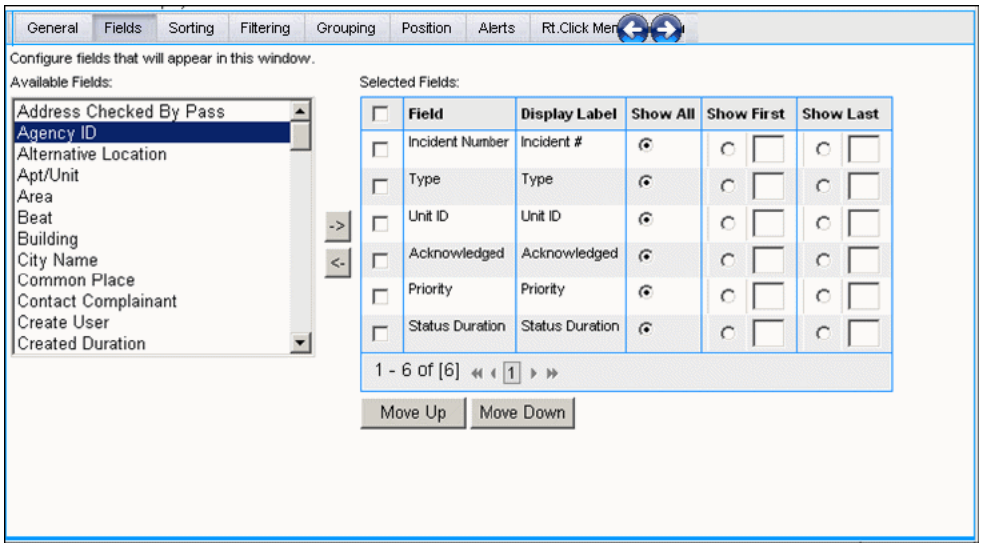


Figure 32-20 Displays Form – Windows Tab, Fields Subtab Showing Selected Fields Table

7. Select one of the following:
   - To show all the values for the field, select the **Show All** button.
   - To show only the first X number of values, select the **Show** button and then enter the number of values you want displayed in the First box.
   - To show only the last X number of values, select the **Show** button and then enter the number of values you want displayed in the Font box.
8. To change the order of the fields' display in the status monitor (from left to right), select a field in the Selected Fields table and click **Move Up** or **Move Down**.
9. Click **Save**.
10. Repeat the previous steps for each window.

Adding Windows Sorting Information

The Sorting tab is where you configure how the fields on each window are sorted.

NOTE
Unit IDs are sorted as strings. Strings are compared from left to right in the order *0-9 A-Z a-z*.

To add windows sorting information:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name that you want apply a sorting feature.

3. Select the Windows tab.

4. Select the Sorting tab.

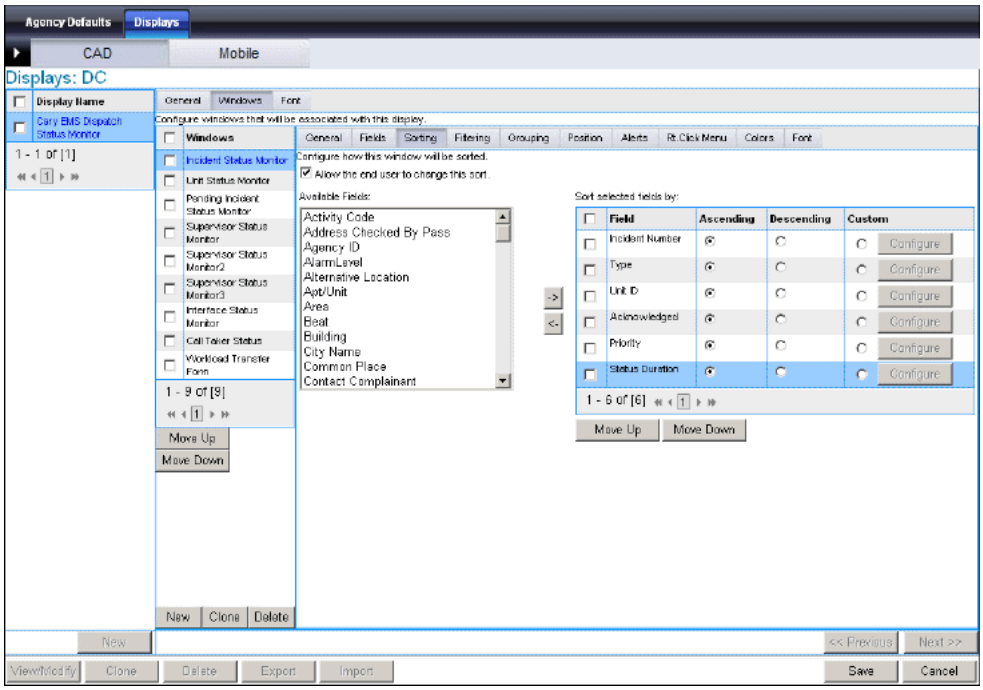


Figure 32-21 Displays Form – Windows Tab, Sorting Subtab

5. From the Windows list on the left, select the window whose fields you want to have the sorting feature.

6. Select whether you want to allow the end user to change the sort.

7. From the Available Fields list, select the fields you want to sort by.

Each field appears in the Sort selected fields by table.

The field Incident updated count is a counter showing the number of times the incident was updated by another dispatcher. This feature allows dispatchers to view how many updates have occurred to an incident since the last time the dispatcher viewed it.

The Incident update counter is based on the incident update transaction type; some incident transactions will not trigger the incident update counter, such as the incident create transaction. If there are two incident update transactions performed by the same user and the interval between the two transactions is less than 15 seconds, then the two transactions will be treated as one transaction and the update count will increase only one.

NOTE
The incident update count does not increment for incident timeouts or for PMDC unit status changes.

8. From the Sort selected fields by table, select how you want to sort each field.

   If you select Custom, click **Configure** and select the values on which to sort.

9. Change the order of the fields by selecting a field in the Selected Fields table and clicking **Move Up** or **Move Down**.

10. Click **Save**.

11. Repeat the previous steps for each window.

Adding Windows Filtering Information

Use the Filtering tab to define how the fields on each window are filtered. Filtering eliminates unnecessary information from your monitors and allows you to view only pertinent data. You select the fields you want to filter, and then indicate the values to filter by.

To add filters:

1. Access the form for a new display. For instructions, see “Adding CAD Status Monitor General Information” on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add filtering information.

3. Select the Windows tab.

4. Select the Filtering tab.

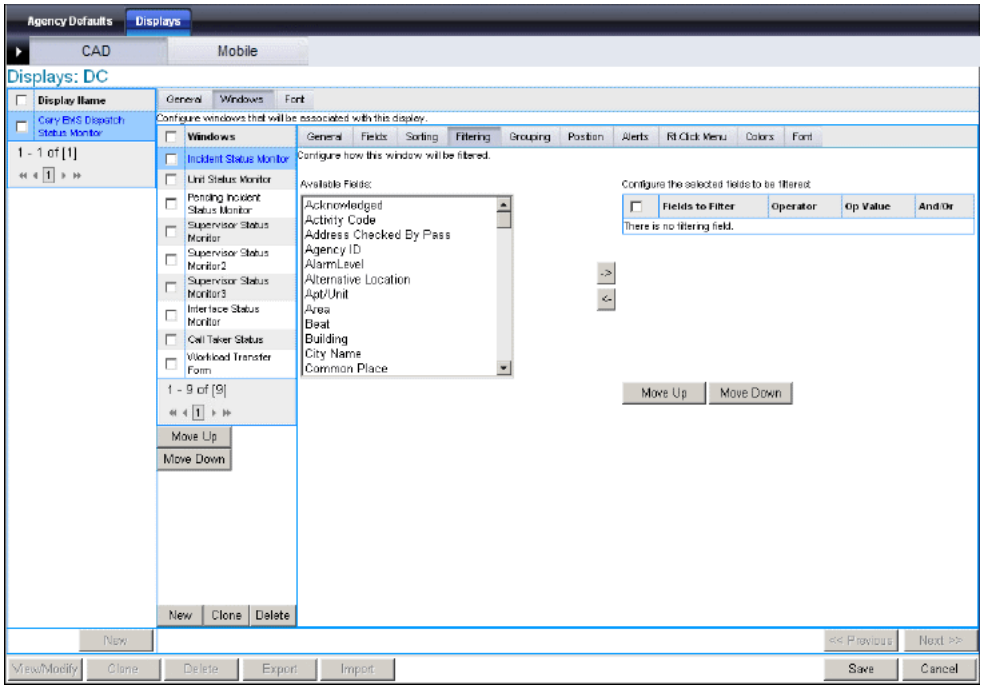


Figure 32-22 Displays Form – Windows Tab, Filtering Subtab

5. From the Windows list on the left, select the window with the fields you want to filter.

6. From the Available Fields list, select the fields you want to filter. The fields need not be present in a window that is used for filtering.

   Each field appears in the Configure how the selected fields be filtered table.

   For the Call and Position type windows, you can type `@My value` to filter the window on “my current position ID” or “my current user ID.” When the filter is used, entries within the corresponding status monitor window are limited to those entries where the current workstation's position ID or currently logged in user’s User ID matches the position ID or user ID associated with the call or position entry.

7. From the table, select how you want to filter each field.

   a. From the Operator list, select the appropriate operator for the field.

   b. In the Op Value field, type or select the appropriate value for the field.

   c. From the And/Or list, select whether you want the filtering to use multiple fields (and) or a single field (or).

8. Click **Save**.

9. Repeat the previous steps for each window.

Adding Windows Grouping Information

Use the Grouping tab to define how each window is grouped and whether any fields are collapsible.

To add windows grouping information:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add grouping information.

3. Select the Windows tab.

4. Select the Grouping subtab.

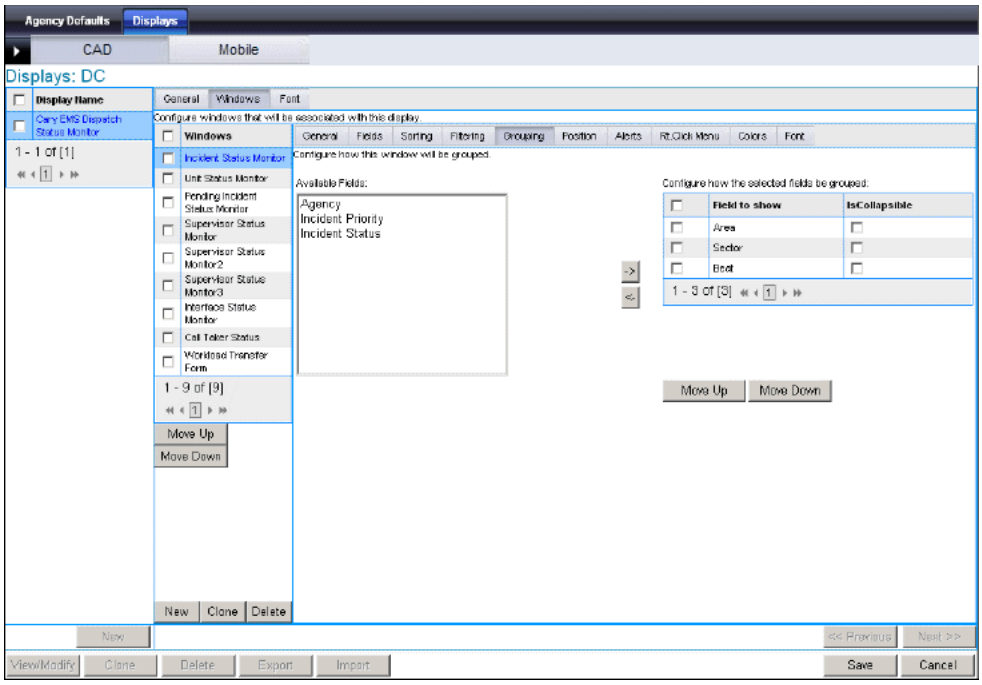


Figure 32-23 Displays Form – Windows Tab, Grouping Subtab

5. From the Windows list on the left, select the window with the fields you want to group.

6. From the Available Fields list, select the fields you want to group.

   Each field appears in the Configure how the selected fields be grouped table.

7. From the table, select which fields, if any, are collapsible.

8. Change the order of the fields by selecting a field in the Selected Fields table and clicking **Move Up** or **Move Down**.

9. Click **Save**.

10. Repeat the previous steps for each window.

Adding Windows Position Information

Use the Position tab to define whether each window can be moved, minimized, maximized, or closed.

To add windows position information:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add position information.

3. Select the Windows tab.

4. Select the Position tab.

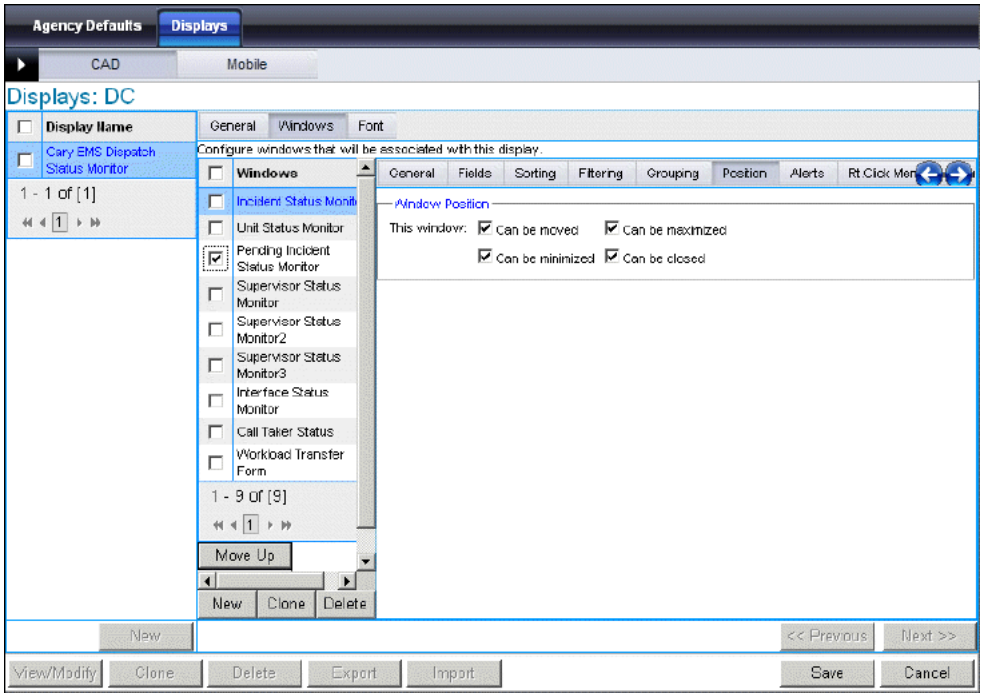


Figure 32-24 Displays Form – Windows Tab, Position Subtab

5. From the Windows list on the left, select the window with the positioning you want to configure.

6. In the Window Position section, select the options for the window. You can select multiple options.

7. Click **Save**.

8. Repeat the previous steps for each window.

Adding Windows Alerts Information

The Alerts tab is where you configure alerts for each window type.

To add windows alerts information:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add windows alerts information.

3. Select the Alerts tab.

Fields and options display for alerts. For Call and Position Monitor status monitors, three other options display if Display as a list in Call Control Window is selected on the General tab.

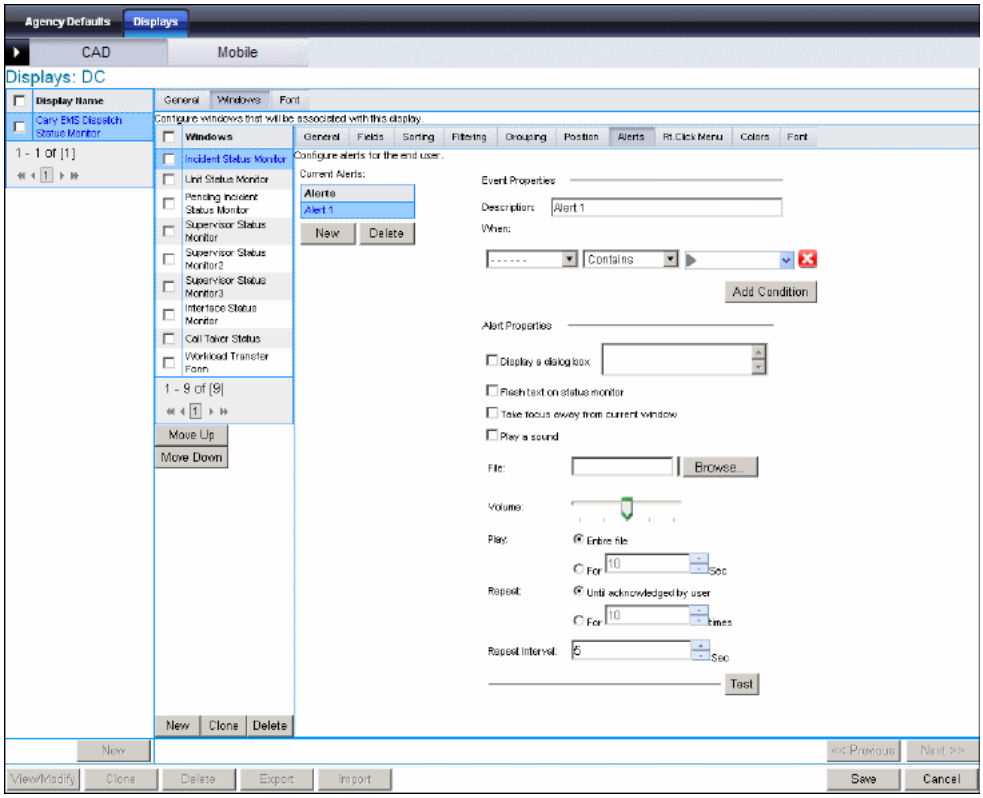


Figure 32-25 Displays Form – Windows Tab, Alerts Subtab

4. From the Windows list on the left, select the window with the alerts you want to configure.

5. At the bottom of the Current Alerts list, click the **New** button.

6. In the Description field, enter a description for the alert.

7. In the When section, select a field.

8. From the adjacent list, select an operator. The operator is used to compare the two fields.

   Options include contains, equals, greater than, greater than or equal to, less than, less than or equal to, and not equals.

9. From the adjacent list, select another field.

NOTE
You can also type the information rather than selecting it from the Field list.

Click **Add Condition** to create an AND or an OR condition.

Example:

When **Common Place** equals **Rocky Mountain Regional Airport.**

10. If you want a pop up dialog box to display for an alert, select the **Display a dialog box** check box.

    Enter the text that you want displayed in the dialog box. You can also use variables to display the value of the item triggering the alert, such as the incident or unit, and the new value, such as that of the unit status or activity code.

    Enter variables in the format `%%variable%%` such as `%%UnitID%%`. The field values must be a valid name from the database; you can view a list of field names in the drop-down list below the `Description` field. The message can contain text before, between, or after the variables.

    Example:

    `Unit %%unit ID%% is now %%UnitStatus%%!`
    (where `%%unitID%%` is the associated unit ID and `%%UnitStatus%%` is the status being tested by the alert).

11. If you want the text to flash on the status monitor, select the **Flash text on status monitor** check box.

12. If you want to take the focus away from the current window on the status monitor to ensure that the user must take an action to continue their current CAD task, select the **Take focus away from current window** check box.

    Use this when the alert is urgent, and you want to ensure that the user pays attention to the alert.

13. For Call and Position status monitors, select one of the following:

    - If you do not want any changes when there is an alert, select **No visual change to tab**.
    - If you want the tab to change color for an alert, select **Change tab color**.
    - If you want the tab to change color and flash for an alert, select **Change tab color & flash**.

      Alerts cannot be set on voice calls that are in the FINISHED state or SMS texts that are in the TERMINATED status.

14. If you want to play a sound for the alert, select the **Play a sound** check box, and then in the `File` field, browse to a sound wave file (`.wav`), and select the sound.

    a. Set the volume for the alert sound.

    b. Select how long you want the alert to sound, if you want it to repeat, and if you want it to continue until it is acknowledged by the user.

    c. If you are repeating the alert sound, set how many times you want it to repeat, and the interval for repeating the sound.

You can test the sound settings by clicking the **Test** button.

15. Click **Save**.

16. Repeat the previous steps for each window.

Adding Windows Right-Click Menu Options

Use the Rt. Click Menu tab to define the options for the right click-menu for each individual status monitor window. These options can take precedence over the agency default options. You can provision unit commands on Incident Status monitors and incident commands on Unit Status monitors.

Incident-related commands are those built from the following:

- AssociateIncidentCommand
- CloneIncidentCommand
- FreeUnitsFromIncidentCommand
- IncidentDispatchCommand
- IncidentHistoryCommand
- IncidentRecallCommand
- IncidentReopenCommand
- IncidentUpdateCommand
- PrimaryUnitCommand
- ReportNumberCommand
- ResetIncidentTimerCommand

Unit-related command are those built from the following:

- PrimaryUnitCommand
- ReportNumberCommand
- ResetUnitTimerCommand
- UMAssignmentCommand
- UMCallStackCommand
- UMMoveUpDownCommand
- UMOffDutyCommand

- UMOnDutyCommand
- UMUnitExchangeCommand
- UMUnitGroupCommand
- UMUnitUpdateCommand
- UnitHistoryCommand
- ReleaseExceptCommand

To add windows right-click menu options:

1. Access the form for displays. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add windows right-click menu options.

3. Select the Windows tab.

4. Select the Rt. Click Menu tab.

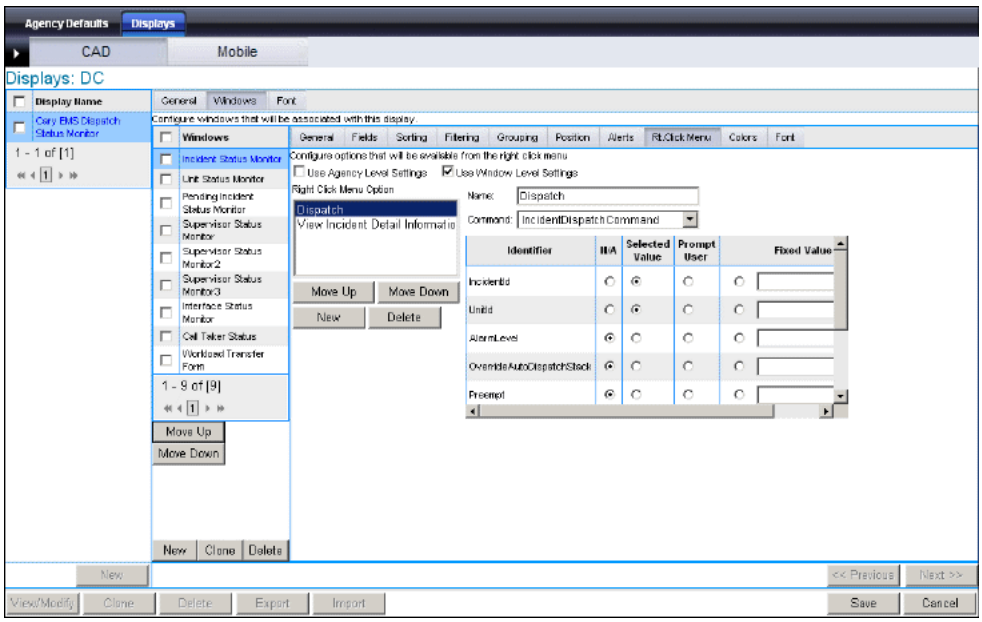


Figure 32-26 Displays Form – Windows Tab, Rt. Click Menu Subtab

5. From the Windows list on the left, select the window with the right-click menu options you want to configure.

6. To use the right-click settings that you enter for the selected status monitor, select use **Window Level Settings**. In this case the right-click settings you enter for the individual status monitor are used.

   To use the right-click settings configured for the agency, select **Use Agency Level Settings**. For details on configuring the agency-level settings, see "Configuring Right-Click Menu Options" on page 32-9. This check box is selected by default. If you select this option, the rest of the steps in this procedure do not apply.

7. At the bottom of the Right Click Menu Option box, click the **New** button.

8. In the Name field, type a name for the new option.

9. From the Command list, select the PremierOne command that corresponds to the menu option.

   If there are identifiers for the option, a table showing the identifiers appears below the Command field. Select how you want to configure the identifiers.

   - N/A – The identifier is not required.
   - Selected Value – Use the value in the status monitor.
   - Prompt User – Prompt the user for a value.
   - Fixed Value – Use the value you enter here.

   When multiple units are assigned to an incident and display in the Call Taker or Incident windows, and the user selects a right-click unit-related command provisioned to Selected Value, the user is prompted for the Unit ID to be used.

   When multiple incidents are stacked against a unit and displayed within the Unit window type, and the user selects a right-click incident-related command provisioned to Selected Value, the user is prompted for the Incident ID to use.

10. Click **Save**.

11. Repeat the previous steps for each window.

Adding Windows Status Color Options

The Colors tab is where you define colors for the Unit Status, Incident Status, and Call Control monitors. Alternatively, you can choose to use the agency default colors.

To add incident, unit, and call control status color options:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add incident and unit status color options.

3. Select the Windows tab.

4. Select the Color tab.

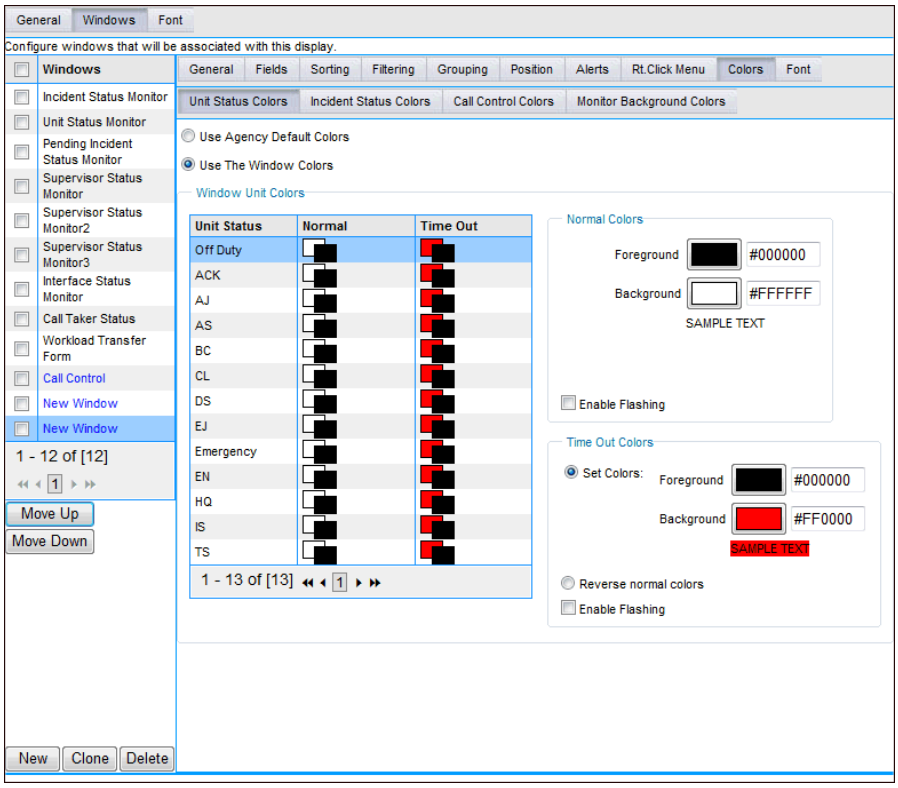


Figure 32-27 Displays – Windows Tab, Color Subtab

5. From the Windows list on the left, select the window with the unit and incident status colors you want to configure.

6. From the Unit Status Colors subtab, select whether you want to use the agency default colors or set colors here.

7. To set unit status colors:

   a. Select a unit status with the colors you want to change by clicking on it.

   b. Set the normal and timeout colors.

      Ensure your text can be easily read by reading the sample text in the box.

      You can reverse the normal colors for your timeout colors by selecting Reverse normal colors in the Time Out Colors box.

   c. If needed, select **Enable Flashing** for the desired states.

8. Click **Save**.

9. Select the Incident Status Colors subtab.

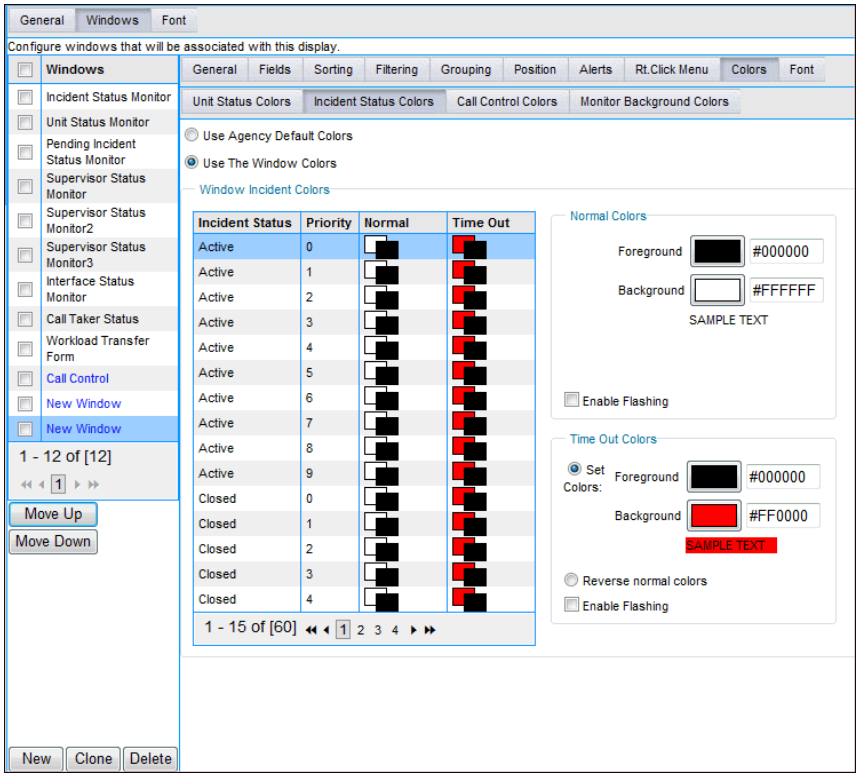


Figure 32-28 Displays Form – Windows Tab, Colors Subtab, Incident Status Colors

10. Select whether you want to use the agency default colors or set colors here.

11. To set incident status colors:

    a. Select an incident status and priority combination with the colors you want to change.

    b. Set the normal and timeout colors.

       Ensure your text can be easily read by reading the sample text in the box.

       You can reverse the normal colors for your timeout colors by selecting Reverse normal colors in the Time Out Colors box.

    c. If needed, select **Enable Flashing** for the desired states.

12. Click **Save**.

13. Select the Call Control Colors subtab.

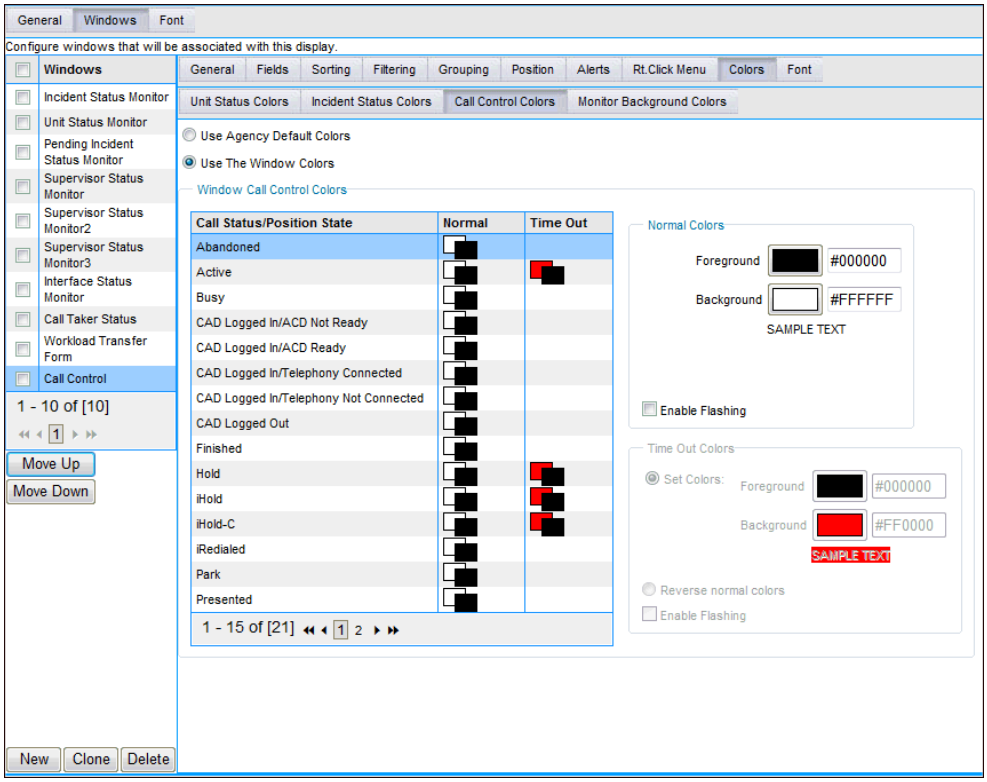


Figure 32-29 Displays Form – Windows Tab, Colors Subtab, Call Control Colors

14. To set call control status colors:

    a. Select the state you want to set colors for.

       Set the normal and timeout colors.

       Ensure your text can be easily read by reading the sample text in the box.

       You can reverse the normal colors for your timeout colors by selecting Reverse normal colors in the Time Out Colors box.

    b. If needed, select **Enable Flashing** for the desired states.

15. Click **Save**.

16. Repeat the previous steps for each window.

Configuring Status Monitor Fonts for Display Sets

The Windows Font tab is where you define fonts for the set of status monitor windows. Fonts that you set in this window apply to all of the status monitors in the Display Set that you select in the Display Name column. Note the following:

- These font settings override the default fonts set for the agency. For details on default agency settings, see "Configuring Status Monitor Fonts for the Default CAD Display" on page 32-18.
- These font settings can be overridden for individual status monitors in the Display Set. For details, see "Configuring Status Monitor Fonts for Display Sets" on page 32-53.

To set status monitor fonts for Display Sets:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. From the Display Name list, select the Display Name for which you want to add font options.
3. Select the Windows tab.
4. Select the Font tab.

   The Font subtab appears.

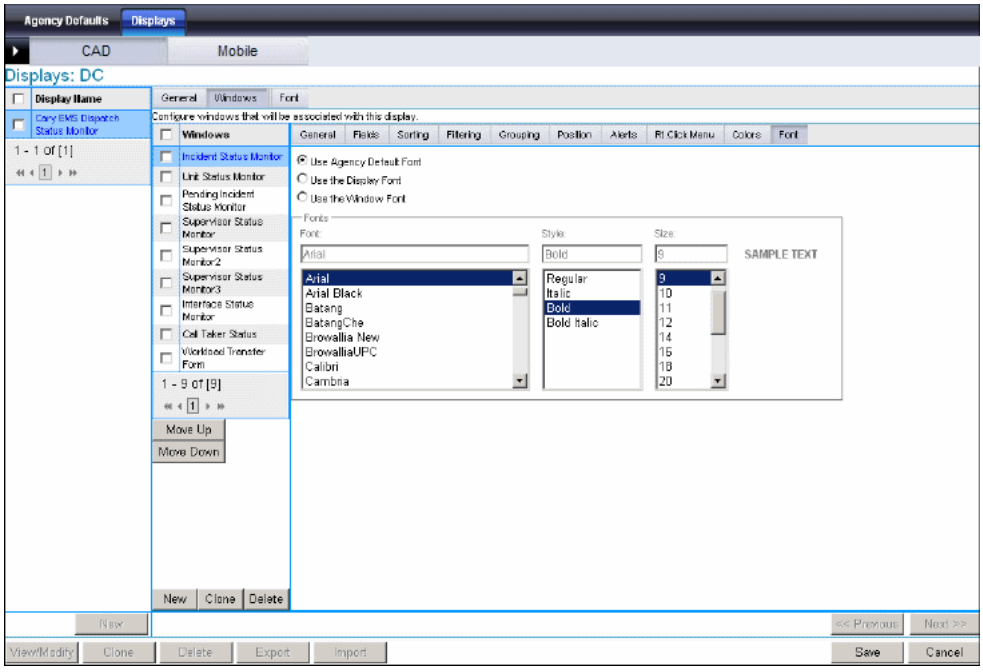


Figure 32-30 Displays Form – Windows Tab, Fonts Subtab

5. From the Windows list on the left, select the Display Set you want to configure.
6. Select **View/Modify**.
7. Select one of the following:
   - Use Agency Default Font – Uses the default settings for fonts that are used for the agency. These are set in "Configuring Status Monitor Fonts for the Default CAD Display" on page 32-18.
   - Use the Display Font – Uses the font settings for fonts set for the Display Names shown on the left pane in this window.
   - Use the Window Font – Uses the fonts that you set for each window, such as the Unit Status monitor or the Incident Status monitor.
8. Select the Font, Style, and Size from the lists, and then click **Save**.
9. Repeat the previous steps for each window.

Configuring Status Monitor Fonts for Individual CAD Monitors

Use the Font tab to define values for font, font style, and font size for individual status monitors in a Display Set. Note the following:

- These font settings override the default fonts set for the agency. For details on default agency settings, see "Configuring Status Monitor Fonts for the Default CAD Display" on page 32-18.
- These fonts settings override the fonts set for Display Sets. For details, see "Configuring Status Monitor Fonts for Display Sets" on page 32-53.

To configure status monitor fonts for individual CAD monitors:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.
2. Select the Font tab.
3. From the Display Name list, select the name of the status monitor.
4. At the bottom of the Fonts form, click **View/Modify**.

The Fonts form refreshes, and the fields are now editable.

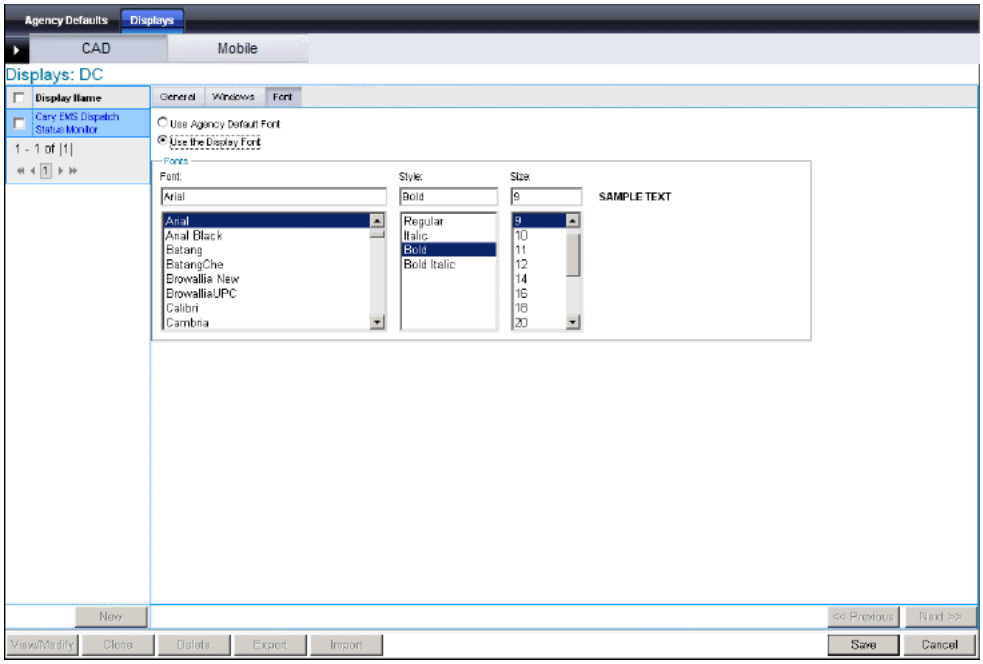


Figure 32-31 CAD Form – Font Tab

5. Select the font, style, and size of text you want to use as the defaults.

   The sample text on the right side of the form displays an example of the selections.

6. Click **Save**.

Configuring Mobile Status Monitor Displays

The Mobile Status Monitor window contains two tabs:

- General – Where you set whether the incident type, incident type alias, or both display in Mobile status monitors.
- Fields – Where you configure the fields that display in Mobile status monitors.

Configuring Incident Type Display Options for Mobile

PremierOne can display the incident type, incident type alias, or both the incident type and incident type alias in Mobile status monitors.

To configure incident type display options for Mobile:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. Click the Mobile tab.

   The Mobile tab appears with the General subtab in focus.

3. Click **View/Modify**.

   The General subtab becomes editable.

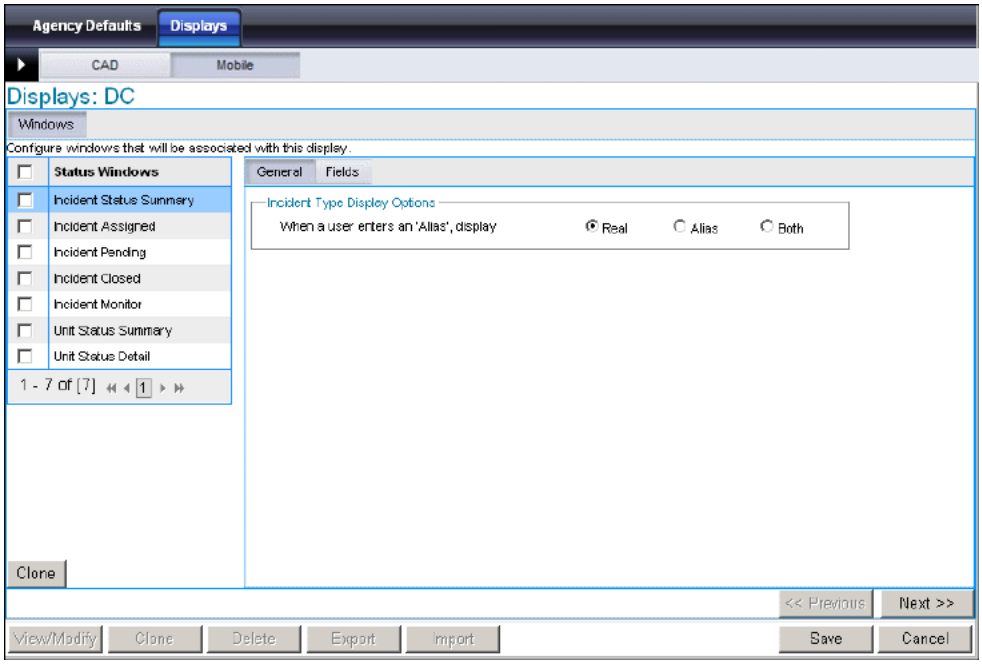


Figure 32-32 Displays Window – Mobile Tab

4. On the left side of the window, select the status window you want to configure.

5. Select the option you want to display in the status monitor: the **Real** incident type, the **Alias** incident type, or **Both**.

6. Click **Save**.

Configuring Display Fields for Mobile

Display field options include the fields that display, the field label, whether one, two, or all rows of information displays, which rows the information display in, and the number of leading or trailing characters.

NOTE
Cloning allows you to copy the display settings to a different Mobile window.

To configure display fields for Mobile:

1. Access the form for a new display. For instructions, see "Adding CAD Status Monitor General Information" on page 32-26.

   The Displays form appears (see Figure 32-14). A list of existing display names appears on the left side of the form.

2. Click the Mobile tab.

   The Mobile tab appears with the General subtab in focus.

3. Click the Fields tab.

4. Click **View/Modify**.

   The fields becomes editable.

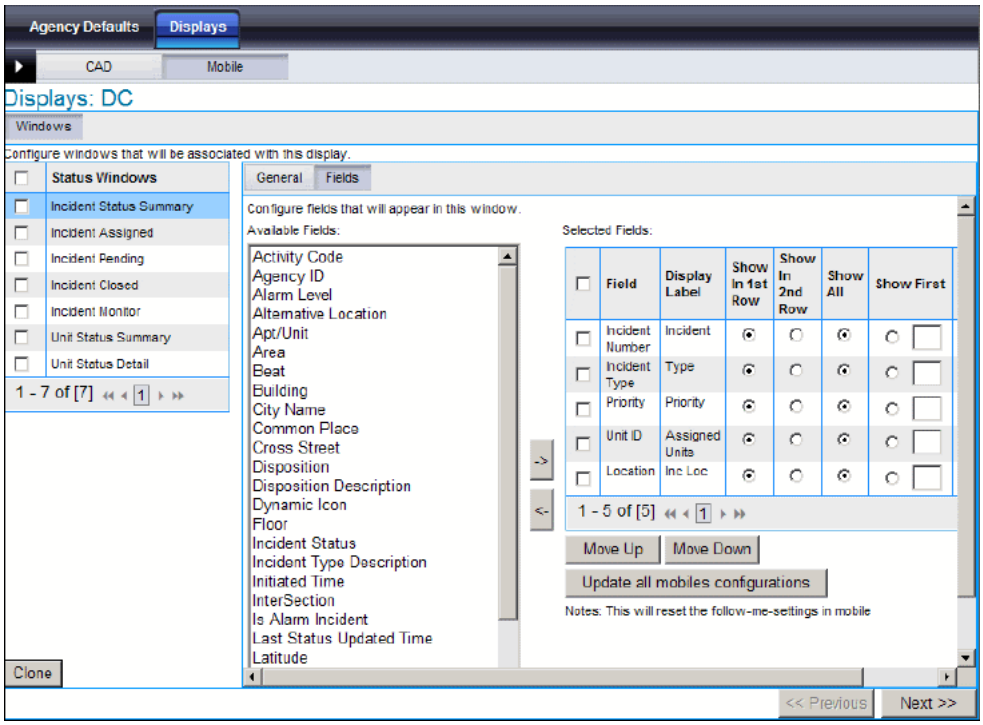


Figure 32-33 Displays Window – Mobile Tab

5. On the left side of the window, select the status window you want to configure.
6. From the list of Available Fields, select the fields you want to display on the status monitor and click the right arrow to add them to the list of selected fields.
7. To display only one row of information for the field, select the **Show in 1st row** button.
8. To display only two rows of information for the field, select the **Show in 2nd row** button.
9. To display all rows of information for the field, select the **Show All** button.
10. To show only some number of leading characters of the field, select the button in the **Show First** column, and then in the next field indicate how many characters to show.
11. To show only some number of trailing characters of the field, select the button in the **Show Last** column, and then in the next field indicate how many characters to show.
12. To update all mobile units, select. the **Update all mobile configurations** button. This resets the follow-me settings in Mobile.

    Mobile users can obtain changes that involve adding or removing fields just by synchronizing with their Mobile clients. If you reorder fields or change labels or display options, only the settings in provisioning are updated, and are not propagated to the clients, even when a manual synchronization is performed on the Mobile client. You must select the **Update all mobile configurations** button to propagate the changes.

    Follow-me settings consist of the specific settings that the Mobile user configures in the Mobile client, such as customizing the status monitors (column width, font size, sorting of comments), chat rooms, messaging, and queries. Customizations that are temporary in the Mobile client are not retained in follow-me settings, such as formatting of messages.
13. Click **Save**.

CHAPTER 33

Configuring Trigger Point Systems

The Trigger Point System configuration item contains the following items:

- Triggers – Where you configure the rules that filter when information is sent to external systems. Trigger points collect CAD events and event data, generate a transaction message to recipients, determine the appropriate recipients of a particular event message, and send the transaction event messages to those recipients. For details, see “Configuring Triggers” on page 33-1.
- Trigger Groups – Where you configure groups to send trigger information to. For details, see “Configuring Trigger Groups” on page 33-4.
- External systems – Where you define the endpoint, trigger group, and schedule on which to send the trigger information. For details, see “Configuring External Systems” on page 33-6.
- Batch Transmission – Where you set up batch transmissions of trigger data. For details, see “Configuring Batch Transmission Information” on page 33-8.

Configuring Triggers

Triggers are rules that filter when information is sent to external systems. Triggers can include information about the originating agency and the message type.

You can add, modify, clone, and delete triggers. For details on modifying, cloning, and deleting, see “Working With Configuration Items” on page 2-9.

To add a trigger:

1. From the navigation panel, select **Trigger Point System**, and then select **Triggers**.

   A list of existing triggers appears.

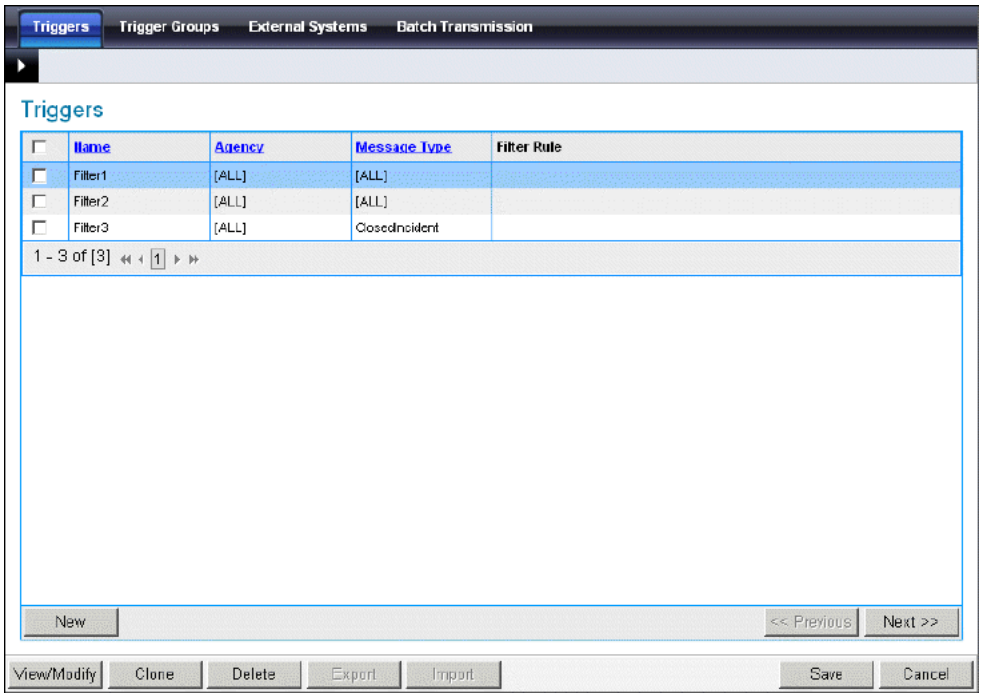


Figure 33-1 Triggers List

2. Click **New**.

The Add Triggers form appears.

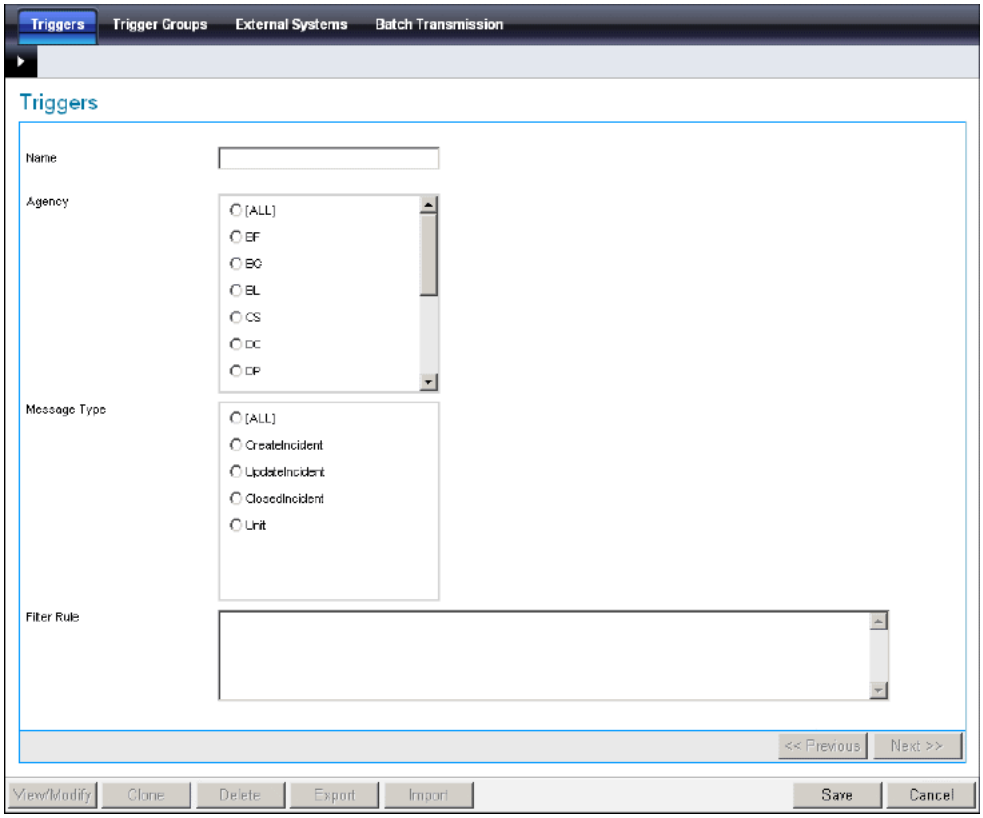


Figure 33-2 Triggers Form

3. In the Name field, type a descriptive name for the trigger.
4. From the Agency list, select the agency this trigger is for. Alternatively, select **[All]**.
5. From the Message Type list, select the message type this trigger will send. Alternatively, select **[All]**.

   If you selected a message type of Incident, Route, or Unit, type the filter in the Filter Rule field. Your filter rule can use only the following:

   Field names for the message types: Incident, Route, Unit

   Operators: Equal (=), Not Equal (!=), AND, OR, IN
6. Click **Save**.

Configuring Trigger Groups

Use the Trigger Groups configuration item to send the triggers as a group rather than individually.

You can add, modify, clone, and delete trigger groups. For details on modifying, cloning, and deleting, see “Working With Configuration Items” on page 2-9.

To add a trigger group:

1. From the navigation panel, select **Trigger Point System**, and then select **Trigger Groups**.

   The Trigger Groups form appears.

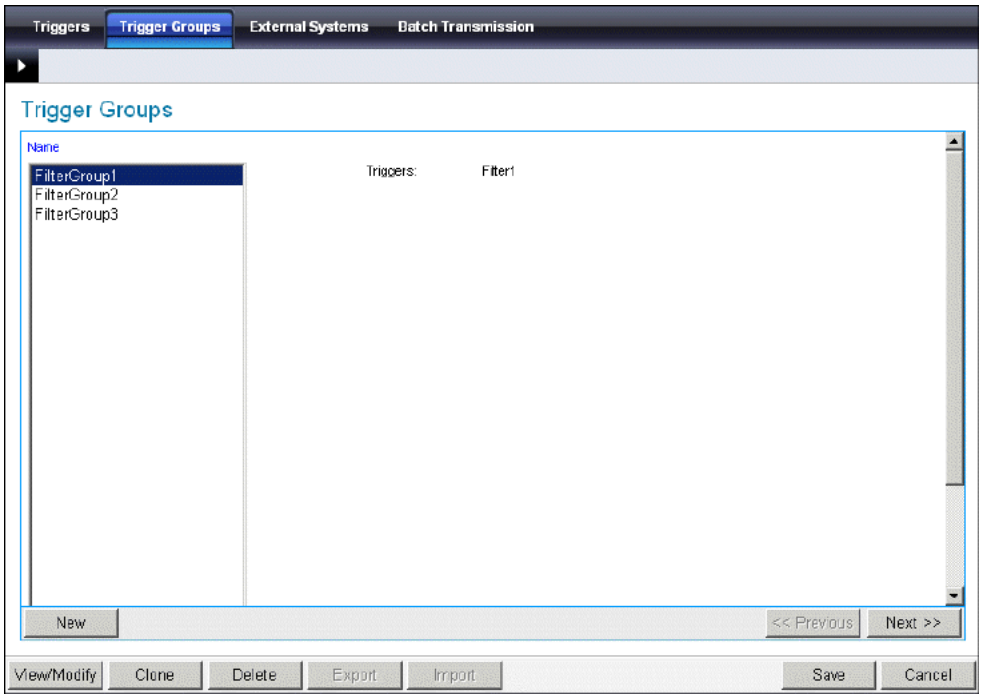


Figure 33-3 Trigger Groups Form

2. Click **New**.

   The Add Trigger Groups form appears.

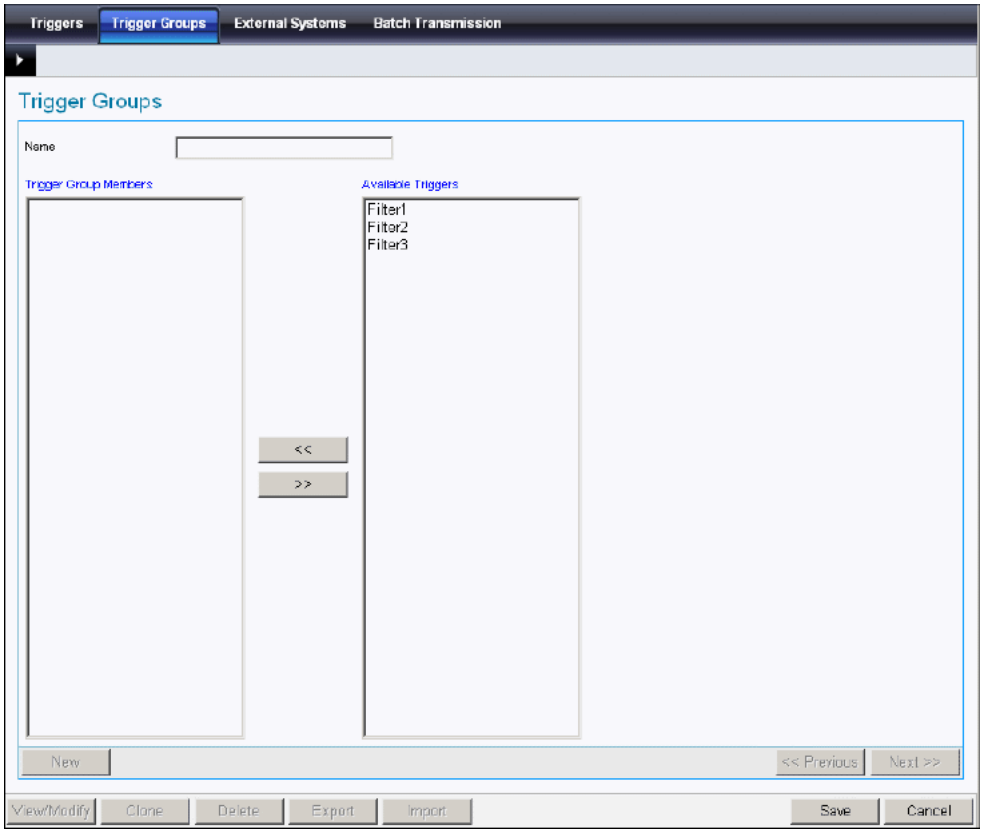


Figure 33-4 Add Trigger Groups Form

3. In the Name field, type a descriptive name for the trigger group.

4. From the Available Triggers list, select the triggers you want to include in the group. Press the **Ctrl** key to select more than one trigger.

5. Click the left arrow key.

   The triggers move to the Trigger Group Members box.

6. Click **Save**.

Configuring External Systems

Use the External Systems configuration item to define the endpoint, trigger group, and schedule on which to send the trigger group.

You can add, modify, clone, and delete external systems. For details on modifying, cloning, and deleting, see “Working With Configuration Items” on page 2-9.

To add an external system:

1. From the navigation panel, select **Trigger Point System**, and then select **External Systems**.

   The External Systems form appears.

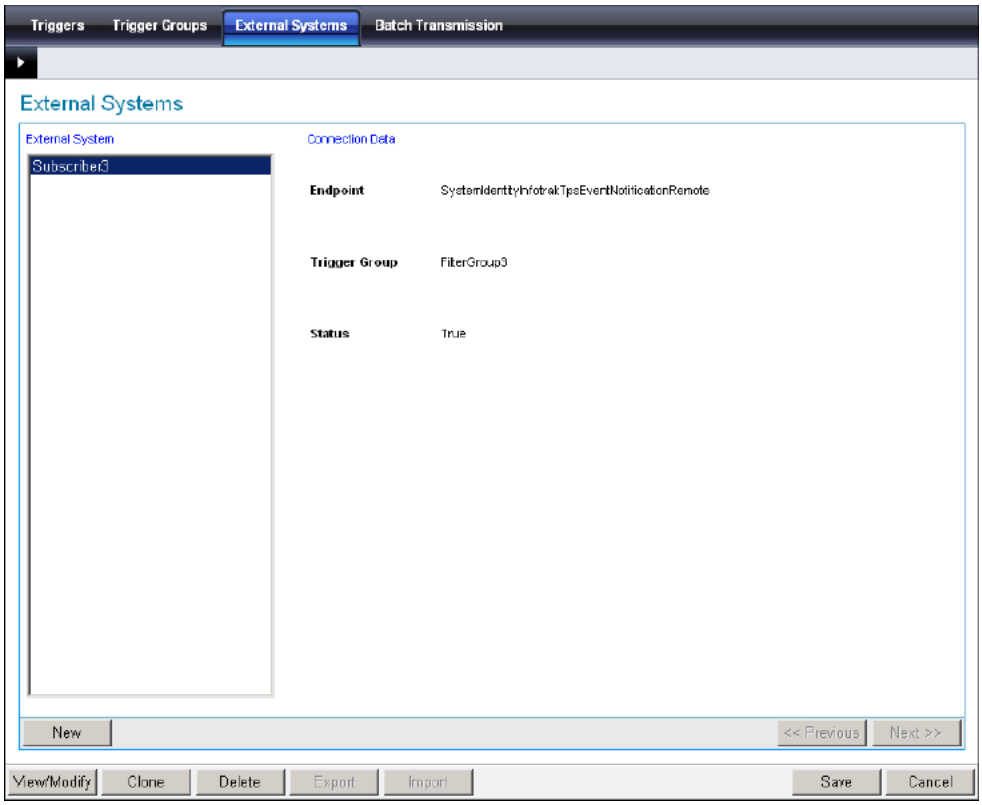


Figure 33-5 External Systems Form – List Of Systems

2. Click **New**.

The Add External System form appears.

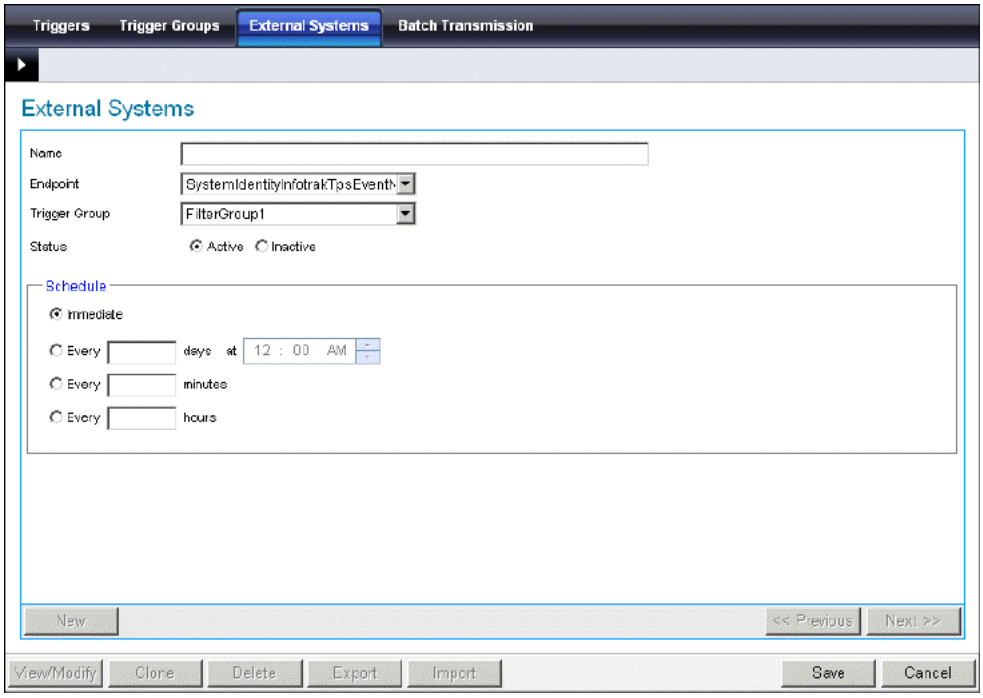


Figure 33-6 External Systems Form – Add

3. In the Name field, type a descriptive name for the external system.
4. From the Endpoint list, select the external system to use as an endpoint.

   This identifies where the Selecting this option causes the incident to be sent to.
5. From the Trigger Group list, select the trigger group you want to send to this external system.
6. In the Status field, select whether the status is active or inactive.
7. In the Schedule section, enter your schedule.
8. Click **Save**.

Configuring Batch Transmission Information

Use The Batch Transmission configuration item to set up batch transmission. This information includes the date range and transfer time for specific historical messages from a specific agency to be sent to a specified system.

To add batch transmission information:

1. From the navigation panel, select **Trigger Point System**, and then select **Batch Transmissions**.

   The Batch Transmissions form appears.

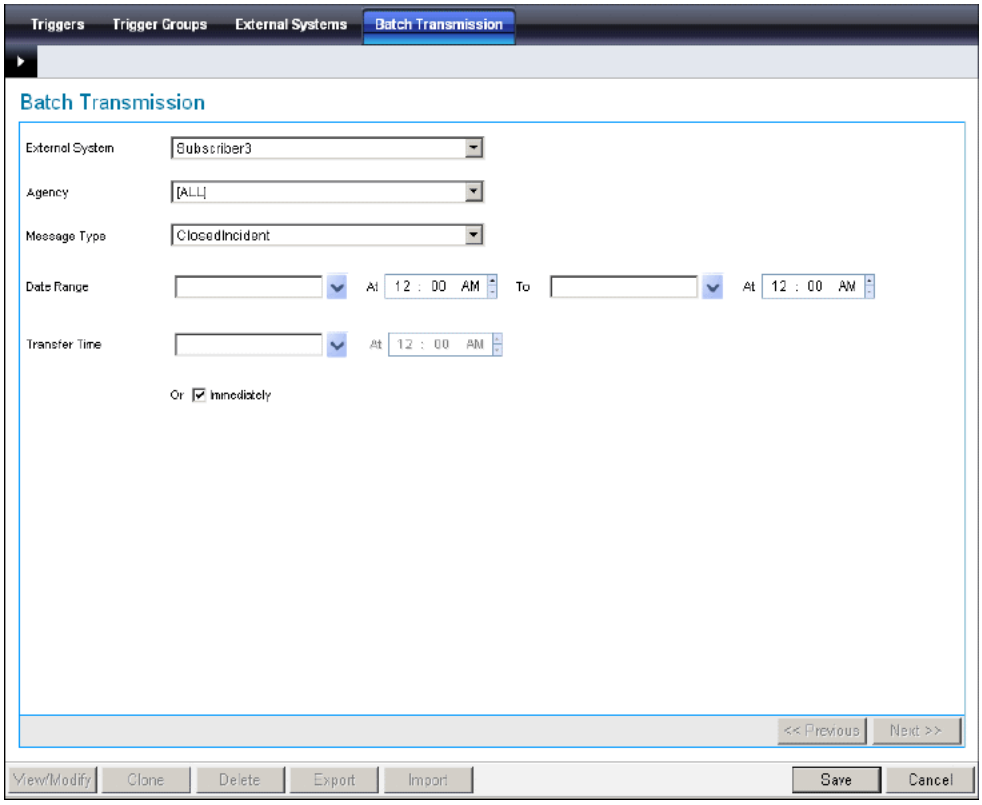


Figure 33-7 Batch Transmissions Form

2. From the External Systems list, select the external system to which the transmission will be sent.

3. From the Agency list, select the agency to which the transmission applies.

4. From the Message Type list, select the message type to which the transmission applies.

5. In the Date Range fields, select the historical dates and times for the data collection.
6. Do one of the following:
   - Select a transfer date and time.
   - Select **Immediately**.
7. Click **Save**.

CHAPTER 34

Internationalization

For internationalization, PremierOne must manage the users input in local or international format, validate users input, store the phone numbers, and display telephone number in local or international format.

Phone numbers have three parts: Area Code, Subscriber Number, and Extension. The maximum number of characters allowed for a phone number (excluding format characters) is 23.

To support various telephone formats PremierOne uses entry validation, which restricts users input as define by the mask. Post entry validation then validates that the format or/and content is valid.

Configuring Phone Number Format

General settings control the display format, the masks for free text phone numbers and formatted phone numbers, and the Mobile prompt character.

To configure phone number format settings:

1. From the navigation panel, select **Internationalization**.

   The Phone Format tab displays.

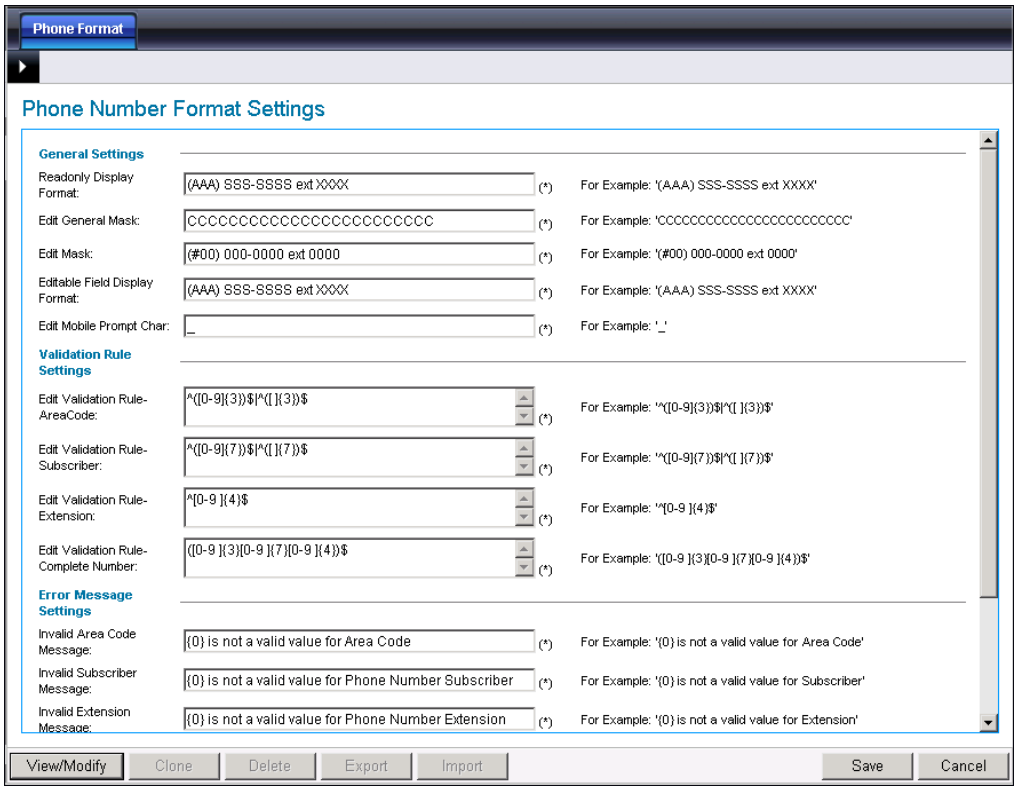


Figure 34-1 Phone Number Format Settings Window

2. In the General Settings section, do the following:

   a. In the Display Format field, enter the format to use when the phone number is displayed as a read-only field.

      - A indicates the alphanumeric characters to display for area code
      - S indicates the alphanumeric characters in the subscriber number
      - X indicates the alphanumeric number of characters in the extension

      All other characters (for example, (,) , -, and ext) are used when the user enters the phone number or for displaying the phone number. To use the characters A, S, or X in a masks, prefix the characters with \ .

   b. In the Edit General Mask field, enter the value to use for free text phone numbers.

      When the user enters a + sign as the first character in an editable field, this field is defined as free text. There are no validation rules associated to the mask.

A + is used international call dialling.

c. In the Edit Mask field, enter the format to use for editable phone number fields. Masking elements are standard coding elements. Common masking elements include the following:

- 0 required digit
- 9 optional digit or space
- # optional digit or space (if the position is blank in the mask it will be rendered as a space; + and - signs are allowed)

For other masking elements, see http://msdn.microsoft.com/en-us/library/system.windows.forms.maskedtextbox.mask.aspx.

3. In the Editable Field display format, enter the format to use for editable field display.

4. In the Edit Mobile Prompt Char field, enter the character to use in the Mobile client to prompt for an address entry.

5. In the Validation Rule Settings section, enter the regular expressions to use to validate the area code, subscriber value, extension, and complete phone number.

   Regular expressions are strings of text and symbols that describe or match a set of strings according to certain syntax rules. These expressions are compared with the data that is entered to determine whether the data is valid.

   The following table contains common symbols used in regular expressions. For details on other symbols, see http://msdn.microsoft.com/en-us/library/hs600312.aspx.

Table 34-1 Filter Operation Symbols

Symbol	Function
[ ]	Begin and end character class symbols. [begins a character class and] ends a character class.
^	Matches the beginning of a string or line.
.	Matches any character except a new line
$	Matches the end of a string or line.
|	Match the part on the left side or the part on the right side.
?	Matches the previous element zero or one time.
{ n} where n is an integer >=1	Repeats the previous item exactly n times

For example, `^([0-9]{3})$|^([]{3})$`

would translate to

Beginning of line, number between 0 and 9, repeated three times, end of line

or

Beginning of line, no value, repeated three times, end of line

6. In the Error Message Settings section, enter the appropriate error messages to use when invalid values are entered.

   The value {0} will be the invalid value entered by the user; do not alter the {0} characters.

7. In the Parse Settings section, do the following:

   - In the Edit Parse field, define how the input string should be split into component fields for validation and storage.

     The splitting rule is defined as a regular expression that specifies three name groups: AreaCode, Subscriber, and Extension. Following is the default expression:

     ```
     ^(?<AreaCode>.{3})?(?<Subscriber>.{7})?(?<Extension>.
     {4})$
     ```

     In the Database Parse field, enter how to retrieve the component fields from the database storage field. Following is the default expression:

     ```
     (?<AREACODE>{3})\T(?SUBSCRIBER>.{7})\T(<EXTENSION>.
     {4})\T
     ```

     The character T represents a tab.

8. Click **Save**.

Recommendation References

This appendix contains detailed explanations of the following PremierOne Recommendation concepts:

- Run Cards
- Alerting: Toning, Paging, and Tear and Run
- Unit Recommendations

Run Cards

Run cards define where and in what order PremierOne looks to find units to dispatch.

Fire Agency Example:

A fire agency may define a dispatch protocol that says, if we have a structure fire in Beat D101, look in Station 1, then Station 4, then Station 9, then Station 3, and so on, for the appropriate units *that can be dispatched* (based on other dispatch protocol rules).

Beat	Order of Stations in Which PremierOne Tries to Locate Units
D101	Station 1; Station 4; Station 9, Station 3; and so on

Therefore, if the structure fire requires **2 Engines**, **1 Truck**, and **1 Battalion Chief**, then PremierOne tries to find these units by looking through the specified order of stations.

Required Units	Station in Which to Look	Station Units	Appropriate Unit(s) Found in Station
2 Engines 1 Truck 1 Battalion Chief	Station 1	BC1 - Battalion Chief (Not Avail) E7 - Engine (Not Avail) **T14 - Truck (Available)**	1-Truck (Unit ID = T14)
2 Engines 1 Battalion Chief	Station 4	E11 - Engine (Not Avail) **E15 - Engine (Available)** L5 - Truck (Available)	1-Engine (Unit ID = E15)

Required Units	Station in Which to Look	Station Units	Appropriate Unit(s) Found in Station
1 Engine 1 Battalion Chief	Station 9	R121 - Rescue (Available) T71 - Truck (Available)	NONE
1 Engine 1 Battalion Chief	Station 3	BC6 - Battalion Chief (Not avail) **E47 - Engine (Avail)** E63 - Engine (Avail)	1-Engine (Unit ID = E47)
1 Battalion Chief	and so on...	and so on...	and so on...

In the previous table, PremierOne was able to find the two Engines (E15 and E47) and the one Truck (T14) that are needed, but the Battalion Chief is still missing. PremierOne will continue to search through the list of stations on the run card looking for a Battalion Chief. If no Battalion Chief is found by the time the end of the list is reached, then no Battalion Chief is available based on the dispatch protocol, so another Battalion Chief or field supervisor may need to be contacted and dispatched to this incident. However, E15, E47, and T14 are dispatched based on the protocol.

Law Agency Example:

A police agency may determine that they need to have three patrol units respond to a structure fire in Beat P143A (the police agency's beat that corresponds to fire's Beat D101). PremierOne looks for units *that can be dispatched* assigned to Beat P143A, then Beat P132, then Beat K1106, then Sector 30, then Area NOR, and so on.

Beat	Order of Jurisdictions in Which PremierOne Tries to Locate Units
P143A	P143A; Beat P132; Beat K1106; Sector 30; Area NOR; and so on

Therefore, if the structure fire requires **3 patrol units**, then PremierOne tries to find these units by looking through the specified order of jurisdictions.

Required Units	Units' Jurisdictional Assignment to Consider	Units' Assigned to the Jurisdiction	Appropriate Unit(s) Found
Patrol	Beat P143A	**13B1 (Available)** 13B2 (Not Avail) 13B3 (Not Avail)	13B1
Patrol	Beat P132	13B4 (Not Avail) 13B5 (Not Avail)	NONE
Patrol	Beat K1106	**14B3 (Available)** **14B8 (Available)**	14B3 14B8
Patrol	Sector 30	11B4 (Available) 11B11 (Available)	N/A
Patrol	Area NOR	1B6	N/A
Patrol	and so on...	and so on...	N/A

In the table above, unit 13B1, 14B3, and 14B8 were the three patrol units identified to be dispatched to the structure fire in Beat P143 based on protocol. PremierOne did not have to continue past the third jurisdictional assignment value (Beat K1106) because it was able to find the three required patrol units by that point.

Alerting: Toning, Paging, and Tear and Run

Alerting is the process of sending all types of alerts. Alerting is also the general term for the three types of alerts: toning, paging, and tear and run.

PremierOne provides all types of alerts–toning, paging, and tear and run–as auto alerts, when enabled, after successful unit dispatch.

All types of alerts can also be sent as a manual alerts using the TN command from the command line and from the TN form. Only one alert type is supported per command.

Creating and Sending Alerts

Because an incident or a unit can have more than one type of alert, PremierOne builds a Unit Alerting List to collect all the necessary data. PremierOne then runs multiple checks, builds the final Alerting List (also known as the Type List), and then sends the alerts.

The following flowchart shows how PremierOne creates and sends alerts.

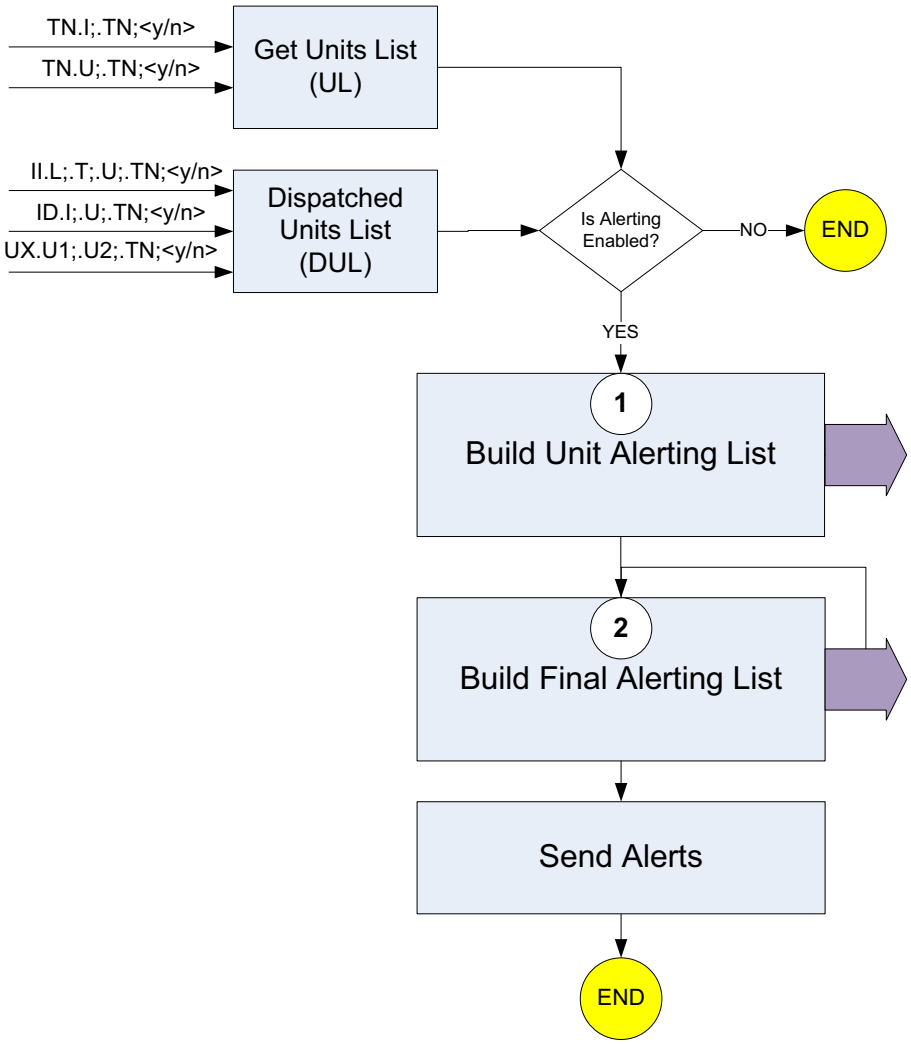


Figure A-1 Creating and Sending Alerts

Explanation of Creating and Sending Alerts Flowchart

1. A user does one of the following:

   - Uses the toning command or the toning form to add an incident- or unit-based alert to the Unit Alerting List. For more information, see “Sending Tones and Pages From the Command Line (TN)” on page 19-6 and “Sending Incident and Unit-Based Alerts” on page 19-3 of the *PremierOne CAD User Guide*.

     ```
     TN...I;...TN;<y/n>
     TN..U;....TN;<y/n>
     ```

   - Uses the II, ID, or UX command with the TN identifier to override the Enable Alerting field in Provisioning. If Enable Alerting is not selected in Provisioning, the user can use the TN identifier with a Y value to add the alert to the Unit Alerting List.

     ```
     II.L;.T;........U;..TN;<y/n>
     ID.I;.U;..TN;<y/n>
     UX.U1;.U2;..TN;<y/n>
     ```

2. PremierOne checks Provisioning to see if Alerting is enabled. If the answer is No, and if the `TN;<y/n>` override identifier did not override this answer, the flowchart ends.

   If the answer is yes, Alerting is enabled, or if the `TN;<y/n>` override has overridden a “no” answer, move on to Build Unit Alerting List.

Building the Unit Alerting List

The following flowchart shows all the checks that PremierOne does in the process of building the Unit Alerting List.

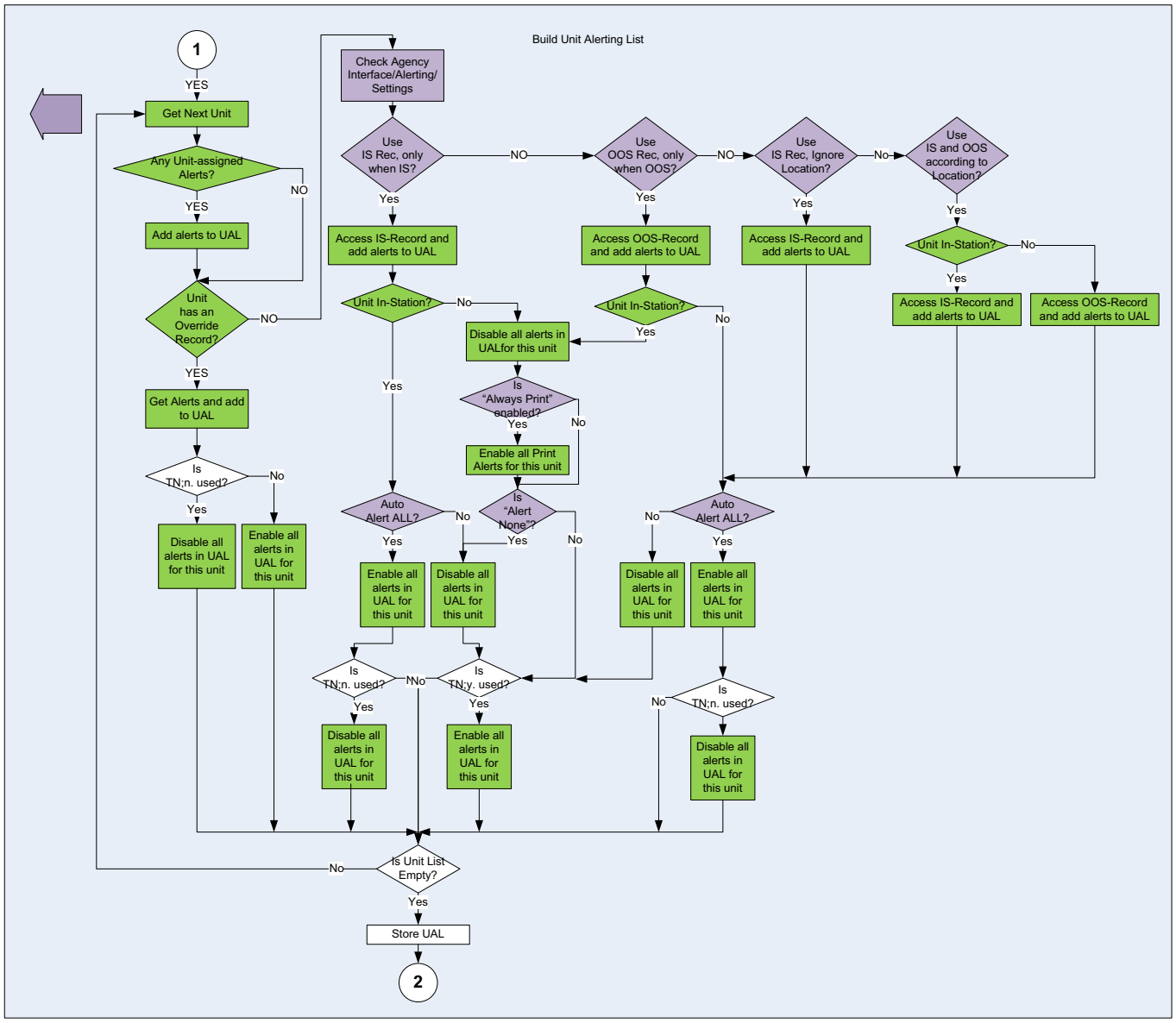


Figure A-2 Building a Unit Alerting List

Explanation of Building a Unit Alerting List Flowchart

The Building a Unit Alerting List flowchart shows all the checks that PremierOne does as it builds the Unit Alerting List.

1. The number 1 indicates that it is a continuation from the previous flowchart where the number 1 appeared. The Yes means yes, build the Unit Alerting List.
2. PremierOne gets the next unit.
3. Decision: Are there any unit-assigned alerts?
   - If Yes, go to step 4.
   - If No, go to step 5.
4. Add alerts to the Unit Alerting List.
5. Decision: Does the unit have an override record?
   - If Yes, go to step 6.
   - If No, go to step 10.
6. Get alerts and add them to the Unit Alerting List.
7. Decision: Is `TN;n` used?
   - If Yes, go to step 8.
   - If No, go to step 9.
8. Disable all alerts in the Unit Alerting List for this unit, and then go to step 43.
9. Enable all alerts in the Unit Alerting List for this unit, and then go to step 43.
10. Check Agency Interface/Alerting Settings.
11. Decision: Is Provisioning set to `Use only In-Station records and only when units are in-station`?
    - If Yes, go to step 12.
    - If No, go to step 18.
12. Access the in-station record and add the alerts to the Unit Alerts List.
13. Decision: Is the unit in the station?
    - If Yes, go to step 14.
    - If No, go to step 21.

14. Decision: Is Provisioning set to Auto alert all on Dispatch by default?
    - If Yes, go to step 15.
    - If No, go to step 26.
15. Enable all alerts in the Unit Alerting List for this unit.
16. Decision: Is TN;n used?
    - If Yes, go to step 17.
    - If No, go to step 43.
17. Disable all alerts in the Unit Alerting List for this unit, and then go to step 43.
18. Decision: Is Provisioning set to Use Out-of-Station records and only when units are out-of-station?
    - If Yes, go to step 19.
    - If No, go to step 34.
19. Access out-of-station record and add alerts to the Unit Alerting List.
20. Decision: Is the unit in the station?
    - If Yes, go to step 21.
    - If No, go to step 28.
21. Disable all alerts in the Unit Alerting List for this unit.
22. Decision: Is Provisioning set to Always Print alert upon dispatch?
    - If Yes, go to step 23.
    - If No, go to step 24.
23. Enable all print alerts for this unit.
24. Decision: Is Provisioning set to Do not auto alert by default (Alert none)?
    - If Yes, go to step 25.
    - If No, go to step 26.
25. Disable all alerts in the Unit Alerting List for this unit.
26. Decision: Is TN;n used?
    - If Yes, go to step 27.
    - If No, go to step 43.

27. Enable all alerts in the Unit Alerting List for this unit, and then go to step 43.
28. Decision: Is Provisioning set to Auto alert all on Dispatch by default?
    - If Yes, go to step 29.
    - If No, go to step 31.
29. Enable all alerts in the Unit Alerting List for this unit.
30. Decision: Is TN;n used?
    - If Yes, disable all alerts in the Unit Alerting List, and then go to step 43.
    - If No, go to step 43.
31. Disable all alerts in the Unit Alerting List for this unit.
32. Decision: Is TN;n used?
    - If Yes, go to step 33.
    - If No, go to step 43.
33. Enable all alerts in the Unit Alerting List for this unit, and then go to step 43.
34. Decision: Is Provisioning set to Use only In-Station records regardless of unit location?
    - If Yes, go to step 35.
    - If No, go to step 37.
35. Access in-station record and add alerts to the Unit Alerting List.
36. Go to step 28.
37. Decision: Is Provisioning set to Use corresponding records based on unit location (Use IS and OOP according to Location)?
    - If Yes, go to step 38.
    - If No, check Provisioning for errors. One of the following must be selected if alerting is enabled:
        - Use corresponding records based on unit location
        - Use only In-Station records and only when units are in-station
        - Use only In-Station records regardless of unit location
        - Use only Out-of-Station records and only when units are out-of-station
38. Decision: Is the unit in the station?

- If Yes, go to step 39.
- If No, go to step 41.

39. Access the in-station record and add the alerts to the Unit Alerting List.
40. Go to step 28.
41. Access the out-of-station record and add the alerts to the Unit Alerting List.
42. Go to step 28.
43. Decision: Is the Unit List Empty?
    - If Yes, go to step 44.
    - If No, go to step 2.
44. Store the Unit Alerting List.

Building the Final Alerting List

The final alerting list is showing in PremierOne as the Type View. The Type View sorts by the specific Alert Types of Toning, Paging, Tear N Run, Two-Tone Paging, FAX, and so on.

The following flowchart shows the steps that PremierOne takes to build the Unit Alerting List.

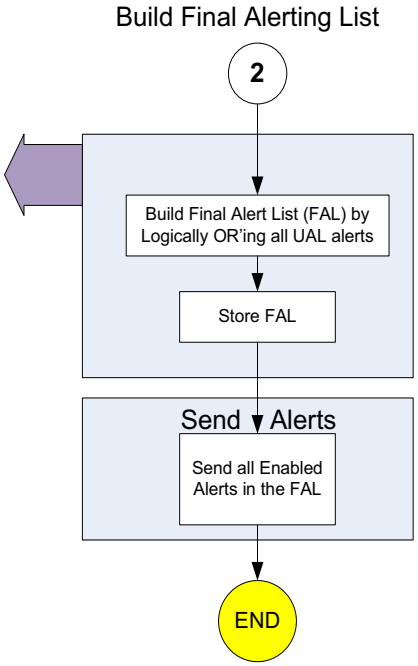


Figure A-3 Building the Final Alerting List

Explanation of Building the Final Alerting List Flowchart

1. The number 2 indicates that it is a continuation from the previous flowchart where the number 2 appeared. The arrow also indicates that it is a continuation from the previous flow chart.

2. Build the final Alert List (FAL) by logically OR'ing all Unit Alerting List alerts. Remember that the Final Alert List is shown as the Type View in PremierOne.

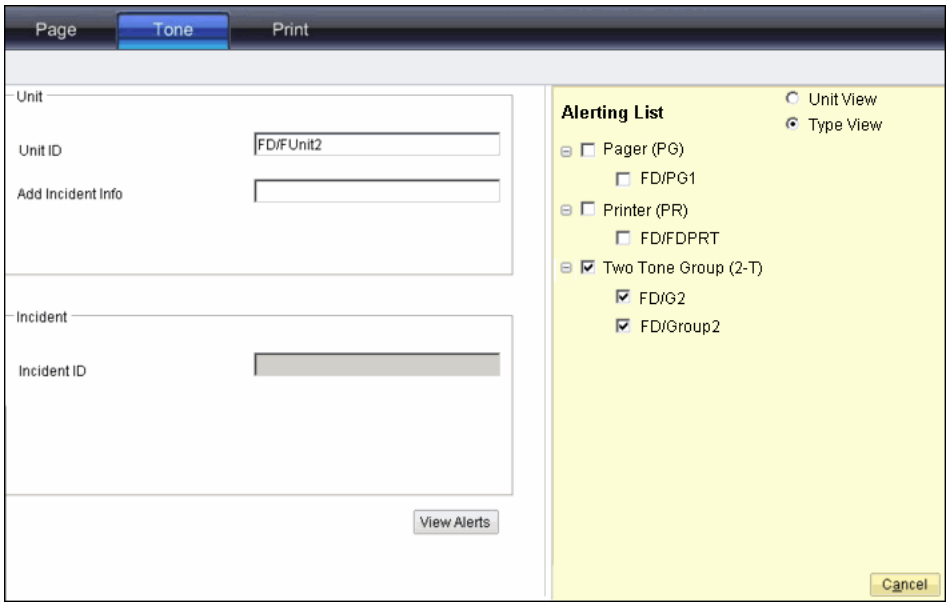


Figure A-4 Alerting List – Type View

"Logically OR'ing" means that PremierOne is identifying all of the alerts and removing any duplicates.

3. Store Final Alerting List.

4. Send Alerts. Send all enabled alerts in the Final Alerting List.

Summary

The following flowchart shows a summary of the steps that PremierOne takes to build the Unit Alerting List and the Final Alerting List or the Type View.

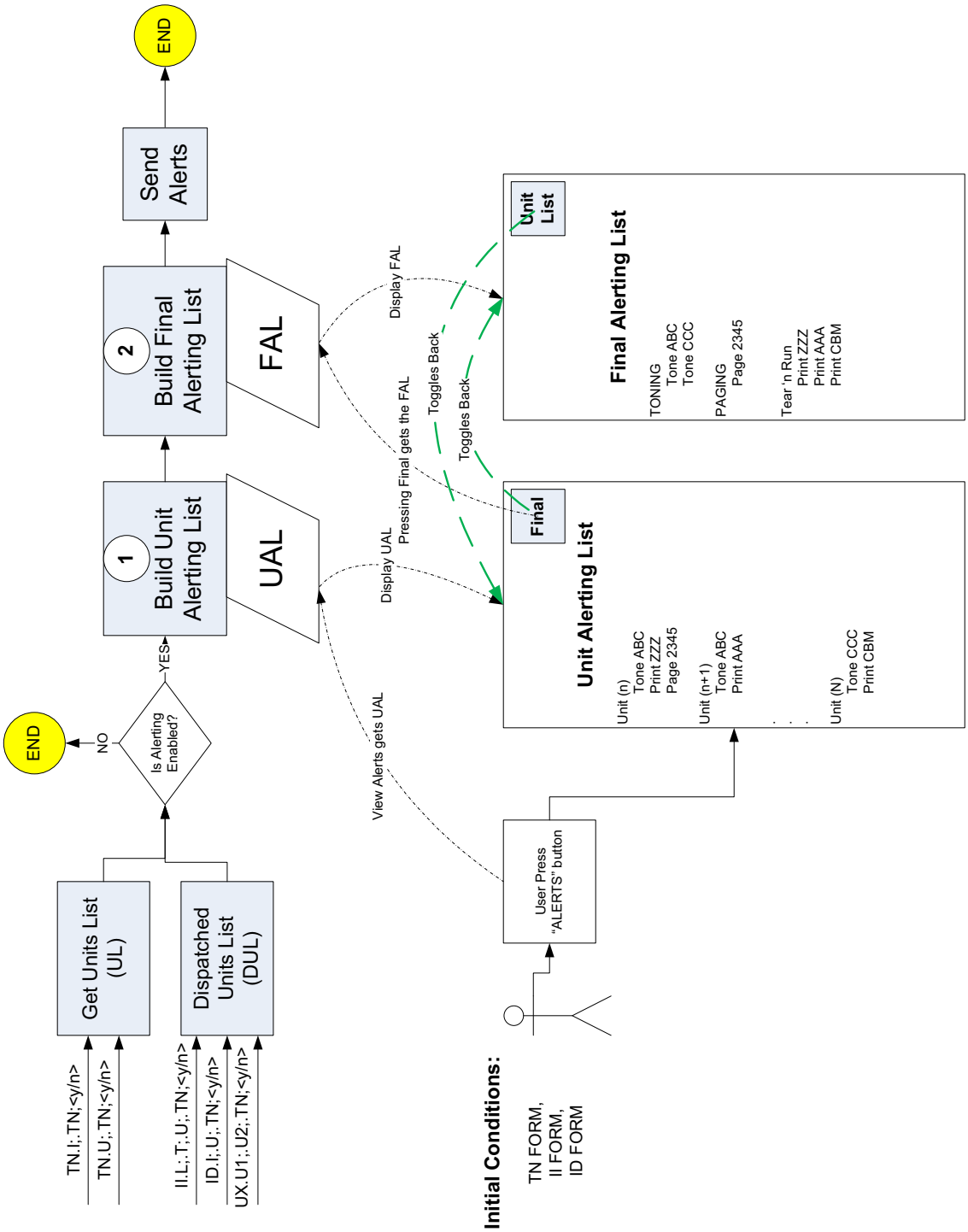


Figure A-5 Building a Unit Alerting List and a Final Alerting List – Summary

NOTE

Remember that you can toggle back and forth between the Unit List and the Type (Final) View.

Alerting by Toning

Toning is the process of sending a specific type of alert through toning equipment (fire station alerting).

Toning is often used to alert fire or EMS stations of incidents. Toning can also be used to create incident- or unit-based alerts that can be for law agencies as well as fire and EMS agencies.

There are several types of toning systems of varying complexity. The toning system can simply open a station's public address system or it can be complex enough to read the incident to the responding personnel. The PremierOne toning interface is configurable to support simple and complex systems. PremierOne also provides different schemes or alerting logic independent of the toning system employed. All but the simplest toning systems can control events in the station and provide feedback to the dispatch user.

Fire Agency Example:

1. While dispatching an incident, the dispatcher receives a recommendation from PremierOne identifying a unit from a fire station that has toning equipment interfaced to the PremierOne system.

2. The dispatcher dispatches the fire unit recommended for the incident (or the dispatcher changes the recommendation to a fire unit that resides within a fire station that is equipped with station toning equipment).

3. PremierOne checks the toning configuration and identifies that there is a dispatch message to be sent to the interfaced toning equipment within the fire station.

4. PremierOne transmits the message to the interfaced toning equipment housed in the fire station.

Law Agency Example:

This is an example of two-tone alerting with Talk Extend. It is only one way of alerting officers. Another way would be a Talk Group from the radio console. How officers are alerted is up to agency protocol.

1. An officer initiates a traffic stop and calls in the plate number.

2. While the dispatcher is running the plate, the officer approaches the car and the driver pulls a gun on the officer while speeding off. The traffic stop has now turned into a high speed chase.

3. The dispatcher wants all officers to receive the update as an alert; therefore he or she sends a two-tone alert followed by a voice message to the pager group that includes all officers on duty in the jurisdiction.

4. The officers in the pager group hear the Beep, Beeeeep, “Vehicle is stolen. Officer states driver has a gun.”

At any time during an active login session, a dispatcher may initiate a toning message (alert) to be sent to interfaced toning equipment. Some reasons for manual tones are:

- Periodic tests of the equipment
- Tone to turn off the stove (we think we left it on when we left the station)
- Tone to close the garage door (we left it open when we left the station)

The following graphic shows an example of a MOSCAD toning system.

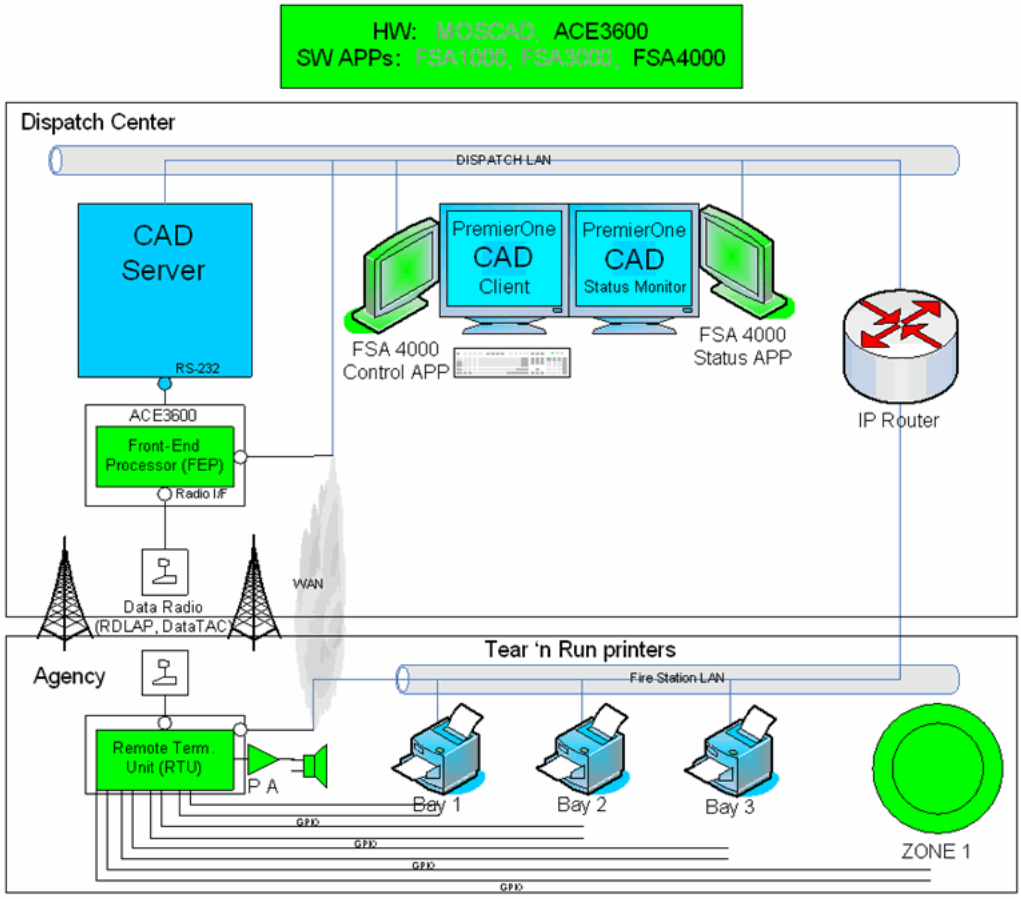


Figure A-6 Toning System Example – MOSCAD

Unit Recommendations

The goal of recommendations in PremierOne is to have multiple methods of recommendations configured so you can plan for a response to any location within your jurisdiction providing any capabilities needed at that location. The multiple methods are:

- Jurisdictional (fixed unit, jurisdictional assignment, and run card)
- Location Based (also referred to as ARL)
- Alternate
- Advanced
- Personnel Skill
- Specific Unit

Recommendations can be logged to the Incident History form. The way they are logged can be provisioned in any of three ways:

- Log Every Time a Recommendation Occurs
- Log Only When a Recommendation Occurs Resulting in a Dispatch
- Do Not Log

Jurisdictional Recommendation Methods

Jurisdictional recommendation methods can be based on the fixed unit, jurisdictional assignment, and run cards.

Recommendations Based on Fixed Unit Responses

The fixed unit responses method allows an agency to explicitly identify the unit IDs and the order in which they are to be recommended for any of the agency's geographic jurisdictional levels (area, sector, beat).

Example:

An agency can define the following fixed unit response:

Beat 101
Fixed Unit Response: Units 701; 718; 703; 726; and so on

When units are being recommended for an incident assigned to Beat 101, PremierOne searches for recommendable units in the specified order: Is unit 701 recommendable? Is unit 718 recommendable? and so on.

Recommendations Based on a Unit's Jurisdictional Assignments

The unit's jurisdictional assignments method allows a set of recommendable units to be retrieved by comparing an incident's geographical jurisdictional assignment against a unit's respective assignments. Further filtering or ordering of the returned set of recommendable units is configurable by each agency.

Example:

If units are being recommended for an incident assigned to beat 102, PremierOne searches for recommendable units whose beat assignments contain beat 102.

An agency can configure the jurisdictional levels (beat, sector, and/or area) that should be used with recommending units. This way, if recommendable units assigned to the incident's beat cannot be found, an agency can elect to then search for recommendable units based on units assigned to the incident's sector, followed by units assigned to the incident's area.

If multiple beats, sectors, or areas are assigned to a unit, they are prioritized for recommendations based on the order in which these assignments are specified for the unit.

Example:

Unit 1A1 has the following beats assigned to it: 101, 103, 105, 102
Unit 1A2 has the following beats assigned to it: 102, 103, 101, 105

If an incident occurs in beat 102, Unit 1A2 is considered for recommendation over 1A1 because beat 102 is 1A2's first beat assignment, while the same beat is the fourth beat assignment for 1A1.

Additionally, an agency can prioritize the units specified in a fixed unit response for the incident's beat with the units recommended based on their jurisdictional assignments.

If an incident occurs in beat 103, both units are equally considered for recommendation based on their jurisdictional assignments because beat 103 is the second beat assignment for both of these units.

An agency can further refine the units considered for recommendation based on the unit's assigned capabilities (unit response requirements), and/or the elapsed time in a recommendable status (enable rotational sub-search). If an agency does not use the rotational sub-search option, the set of units that are recommendable is sorted alphabetically by their call sign prior to the selection of recommended units.

Recommendations Based on Run Card Assignments

The run card assignments method allows a set of recommendable units to be retrieved for an incident based on a predefined order in which jurisdictional areas or stations should be searched. Further filtering/ordering of the returned set of recommendable units is configurable by each agency.

Example:

An agency can define the following run card assignment:

Beat 103
Run card assignment: AR1; AR3; AR5; AR2 (each of these values represents an area)

When units are being recommended for an incident assigned to beat 103, PremierOne first looks for recommendable units that are assigned to AR1, followed by recommendable units that are assigned to AR3, and so on.

A run card can also include a Static Units List within its assignment. These units will always be recommended as long as the unit is in a recommendable status.

Location (ARL) Based Recommendation Methods

Automatic Resource Location (ARL) is a means for determining the geographic location of a resource, often, but not necessarily, a vehicle, and transmitting this information to a point where the information can be used. Most commonly, the location is determined using GPS (global positioning system), and the transmission mechanism is a satellite, terrestrial radio, or cellular connection from the vehicle to a radio receiver, satellite, or nearby cell tower.

A typical system is land-based and is used to simultaneously track the locations of a fleet of vehicles.

Example:

An ambulance fleet has an objective of arriving at the location of a call for service within six minutes of receiving the request. Using an ARL system allows dispatch personnel to evaluate the locations of all vehicles in a fleet in order to pick the vehicle that will most likely get there fastest, meeting the service objective.

In PremierOne, ARL is used in recommendations to track the location of emergency vehicles to determine their present location when requiring units to respond to an incident. By adding ARL recommendations to PremierOne, PremierOne can make recommendations based on the actual location of units rather than recommending units solely based on jurisdictional assignment.

Alternate Recommendation Methods

Alternate recommendations assist an agency in providing the optimal response based on the current system status. This is accomplished by creating responses using a combination of unit types, capabilities, personnel skills, and specific units.

Alternate recommendations allow capabilities to be combined using OR as well as AND. The administrator can determine if the OR grouping is applied immediately or after a certain depth of search has been processed.

Using alternate recommendations, if PremierOne passes over a provisioned optional unit while looking for a primary unit, PremierOne advises the dispatcher. PremierOne also allows a unit to fulfill multiple capabilities for an incident.

Advanced Recommendation Methods

Advanced recommendations extends basic recommendations by allowing an agency to configure the recommending of a different type of unit if the desired unit is not available or is not within a defined time threshold. In addition to sending this different unit, the advanced recommendation can still send the desired unit.

Example:

Consider a type of call being an ambulance request for a suspected heart attack. In this type of call, the desired unit is an ALS (Advanced Life Support) unit that can respond within 5 minutes. PremierOne may search for this recommendation and find that the nearest ALS unit is 8 minutes away but there is a BLS (Basic Life Support) unit that is 3 minutes away. You can configure recommendations to recommend the BLS and ALS units so that the BLS unit response and provides basic support until the ALS unit is able to respond 5 minutes later.

You can manage and use advanced recommendations regardless of whether PremierOne is generating a recommendation using jurisdictional or ARL-based recommendation methods. One difference between the two recommendation methods, however, is that only ARL-based recommendations may be used with a time threshold.

Personnel Skill Recommendation Methods

In addition to unit capabilities, PremierOne must be able to recommend units that are manned by personnel possessing specific skills. A common example of personnel recommendations can be seen when considering medical calls requiring different personnel skill sets.

Often, an EMS agency will have at least two types of staff: those who are fully trained paramedics (able to give medication and perform advanced life saving techniques), and those who are EMTs or paramedics in training (able to simply stabilize a patient and transport to the hospital). In the case of a medical call for a heart attack, having a paramedic respond is the optimal recommendation. If a paramedic is not available however, then an EMT would be sent as the best available option. PremierOne must allow the agency to configure Incident Response Factors (IRFs) to first search for units manned by paramedics before recommending units staffed by EMTs.

Specific Unit Recommendation Methods

For certain incident types, a specific unit may have to be recommended. To prevent the administrator from having to assign capabilities to the unit, the administrator can enter the specific unit's ID as being recommended when the specific incident type has been used.

NOTE

Do not confuse specific unit recommendations with Fixed Unit Response. Fixed unit response occurs due to the location of the incident. Specific unit recommendations are made due to a specific IRF being used.

The assignment of a specific unit ID to an IRF for response is in addition to any other recommendation configuration.

Recommendation Logging

In Provisioning, the system administrator can set how recommendations are logged to the Incident History form. This feature provides your agency with the opportunity to compare the units that were recommended for an incident against the units that were actually dispatched to the incident. The feature allows your agency to evaluate:

- Your recommendation schemes to ensure that the most appropriate units are being recommended
- Your dispatchers to ensure that they are dispatching the most appropriate units to the incident

This feature also allows your agency to automatically log to an incident's history the fact that no units were recommendable at the time of dispatch. This incident history record helps to provide evidence that a delay in responding to an incident was caused by the lack of available resources.

To use Unit Recommendations logging at the agency level:

1. Access Provisioning.
2. From the Navigation panel, select **Unit Recommendation**, and then select **Settings**.
3. On the General tab, select the Log recommendations to Incident History check box, and then select one of the options to provision how logging of recommended units to Incident History should be done:

- "Log Every Time a Recommendation Occurs" on page A-21
- "Log Only When a Recommendation Occurs Resulting in a Dispatch" on page A-21
- "Do Not Log" on page A-21

Recommendation requests can be performed in CAD using the Request button in the Dispatch form or using the ID command from the command line to display the Dispatch form.

Log Every Time a Recommendation Occurs

Use this option to log unit recommendations to Incident History each time recommendations are requested.

This option includes logging an Incident History transaction when no recommended units are found, or when no response card is provisioned for the incident's Incident Response Factor (IRF) or Response ID.

Log Only When a Recommendation Occurs Resulting in a Dispatch

Use this option to log unit recommendations to Incident History only when the requested recommendation is associated with a dispatch, or when no recommendable units were returned.

This option allows logging in two different scenarios: when units are dispatched *and* when recommendations are requested and no units are returned.

This option also includes logging an Incident History transaction when no recommended units are found, or when no response card is provisioned for the incident's IRF or Response ID.

Do Not Log

Use this option to log unit recommendations to Incident History only when recommendations are requested but no recommendable units were returned.

This option is different from the second option. This option allows logging *only* when recommendations are requested and no units are returned. The only other instances where an Incident History transaction is logged are when no recommended units are found, or when no response card is provisioned for the incident's IRF or Response ID.

Units would not be logged that were dispatched or that were requested and recommended.

Index

Numerics

9-1-1 systems, adding 11-67

A

accounts
locking 11-10
unlocking 11-10
acknowledgments
receive when sending incidents 22-31
send when receiving incidents 22-31
action bar, configuring for mobile 16-5
action codes, contractor 15-6
active plan, setting 7-5
activity codes 10-29
adding 10-29
exporting 10-29
importing 10-29
adding 6-6, 10-4
9-1-1 systems 11-67
activity codes 10-29
address book general information 18-2
address books 18-2
agencies by cloning 4-6
alarm records general information 19-4
alarm records incident information 19-6
area, sector, beat settings to response messages . 13-47
call location icons 25-19
camera icons 25-21
capabilities 11-6
capability settings for preassigned units 10-9
chat room member properties 20-11
chat rooms 20-9
codes to lists 6-4, 6-7
coverage groups 13-2
device general information 11-44
device login settings information 11-46
device permissions information 11-50
disposition codes 13-43
duty types 10-31
emergency notifications from the form 24-1
equipment 11-41
existing entries to a group 18-15
existing entries to address books 18-5
frequency settings 31-40
general chat room settings 20-9
general information for incident response factors . 13-37
general information for lists 6-6
general information for roles 8-2
general information for status monitors 32-26
GPS device 11-65
group general information 18-12
groups 18-12
incident icons 25-16
incident type aliases 13-6
incident type code details 13-4
incident type codes 13-4
information to run cards 14-23
IRF information to run cards 14-24
IRFs 13-39
IRFs attributes 13-39
list items 6-6
lists 6-6
manual notifications from the form 24-3
MDTs 11-43
members to chat rooms 20-12
modifying circumstance codes 13-8
new agency details 4-4
new entries to a group 18-17
new entries to address books 18-8
pager groups 11-60
pagers 11-59
permission sets 5-3
permissions for roles 8-5
personnel authorization information 11-14
personnel contact information 11-11
personnel detail information 11-8
personnel resource assignment information 11-16
personnel roles information 11-13
plans from the form 7-2
premise/hazard records 13-58
purge online settings 30-3
query type cascading queries 31-30
query type drill down information 31-33

query type duplicate fields 31-27
query type form fields 31-20
query type hot hits 31-28
query type interface fields 31-19
query type interfaces 31-18
query type response fields 31-24
query type settings 31-16
radios 11-55
reporting data warehouse purge settings 30-5
resources to roles 8-13
response cards for IRFs 14-3
response cards for response IDs 14-3
response categories 14-36
response classes 14-13
response classes for locations 23-4
response descriptors 14-17
response ID information to run cards 14-23
response IDs 14-15
response message subject and text settings 13-46
response modes 14-11
roles 8-2
roles, general information 8-2
run cards 14-20
source codes 13-50
station general information 23-6
station preferred recommendation order 23-8
status code properties 10-11
status code timeouts 10-13
status monitor displays 32-26, 32-55
status monitor window information 32-28
trigger groups 33-4
triggers 33-1
unit capabilities for preassigned units 10-8
unit general preassignments 10-4
unit icons 25-20
unit IDs 10-2
unit status codes 10-11
vehicle information 10-6
watch list exclude settings 31-41
watch list settings 31-38
windows alerts information 32-44
windows fields 32-36
windows filtering information 32-40
windows general information 32-28
windows grouping information 32-42
windows incident and unit status color options . 32-49
windows position information 32-43
windows right click menu options 32-47
windows sorting information 32-39
workstation general information 11-44
workstations 11-43
address book icon, mobile 16-14
address books 18-1
adding 18-2
adding existing entries 18-5
adding existing entries to a group 18-15
adding general information 18-2
adding group general information 18-12
adding groups 18-12
adding new entries 18-8
adding new entries to a group 18-17
cloning 18-1
viewing contacts 18-11
address searches
configuring wildcard 25-7
max distance for matches 25-6
number of results to display 25-8
address verification
displaying high and low cross blocks 25-8
displaying high and low cross streets 25-8
enable display of best match first 25-10
enable Soundex 25-10
enable street search 25-10
matching distance 25-6
returning long/lat coordinates 25-7
addresses
configuring intersections 25-7
configuring max number of returns in search 25-7
using wildcards 25-7
agencies
adding by cloning 4-6
adding details 4-4
concurrent logins 9-4, 11-48
configuring alerting scheme 22-7
working 13-3
agency admin role 8-1
agency settings
modifying for mobile browsers 17-1, 27-1
agency types, adding 4-2
alarm level, IRFs 13-40
alarms
adding alarm records general information 19-4
adding alarm records incident information 19-6
cloning company records 19-1
modifying chronic alarm settings 19-9
modifying false alarms 19-10
alert type, defined 22-2
alerting
attributes for alerting scheme 22-8
auto alerting 22-4
configuring agency scheme 22-7
configuring settings 22-3
configuring two-tone pager groups 11-57
configuring two-tone radio 22-47
defined 22-2, A-3
enabling 22-4
example 22-18
in-station units 22-5

out-of-station units 22-5
printing parameters 22-6
type, defined 22-3
types, All Call 22-5
alerts
All Call alert type 22-5
configuring alerts for in-station 22-10
configuring alerts for out-of-station 22-12
configuring common response parameters for all toning statuses 22-16
configuring existing toning systems at agency level 22-8
configuring unit-based records that override default scheme 22-14
enabling existing toning systems at agency level . 22-8
mobile settings for incident dispatch 13-33
mobile settings for incident updates 13-35
ALI records, incorrect 12-7
alias
address books 18-9
contacts 18-9
alias, messaging 11-10
aliases, incident types 13-6
allow orphan, status monitors 32-31
ALPR
configuring queries from direct hits 31-54
area, override 13-39
areas
adding to response message settings 13-47
setting default location 23-1
ARL
compressing playback data 25-40
playback history defaults 25-40
assigning
default location for area 23-2
default location for beat 23-2
default location for sector 23-2
assigning radios
to personnel 11-16
associated incidents
automatically add comments 13-17
automatically create 13-17
displaying primary units on map 25-25
associated units, displaying on map 25-25
ASTRO device type 11-35
ASTRO message type indicators 11-33
attributes, for alerting scheme 22-8
audio alerts for mobile units 13-33
authentication
configuring general agency settings 9-2
configuring passwords 9-6
configuring system notifications 9-9
enabling emergency mode 9-8
forcing password changes 9-11
auto alerting, defined 22-4
automatically add comments to associated incidents . . 13-17
average speed 4-5

B

background colors for CAD status monitors 32-19
beats
adding to response message settings 13-47
setting default location 23-1
blocks
display format 25-9
geocode location 25-9
keywords 25-9
retain street number 25-10
BOLO fields, text-to-speech 16-25
BOLO messages
configuring 26-11, 26-13
properties 26-11, 26-13
scheduled 26-10

C

cached credentials 11-45
CAD command access, trusted agencies 5-6
cadence
setting person location 25-38
cadence, modifying 25-22
call control center 12-22
debounce factor 12-3
general Call Control Center window settings 12-22
general settings 12-2
incoming line types 12-5
incoming lines 12-4, 12-6
incorrect ALI records 12-7
overview 12-1
permissions for Call Control Center window 12-25
preprogrammed messages 12-19
preprogrammed text messages 12-20
queue buttons for Call Control Center window . . 12-24
voice calls held too long 12-2
call control window settings 12-22
call for service
definitions 22-27
features 22-27
foreign agency provisioning overview 22-29
interface 22-27
local agency provisioning overview 22-28
provisioning 22-28
call location icons
adding 25-19
modifying 25-19
call stacking
allow unit to dispatch next incident 13-20

automatically dispatch next incident 13-20
enabling 13-20
exceed limit by one 13-20
maximum calls 13-20
calltalker status monitor, number of inc to display . . 32-35
camera icons
adding 25-21
modifying 25-21
capabilities 11-7
adding 11-6
configuring 11-4
defined 11-4
modifying 11-7
overview 11-4
provisioning 11-5
setting sort order 14-31
capability groups
adding 11-3
defined 11-2
exporting 11-2
importing 11-2
cascading queries
creating 31-30
defined 31-30
cautions 1-5
channel groups
adding channels 22-54
enabling 22-47
chat fields, selecting for text-to-speech 16-26
chat rooms
adding 20-9
adding general settings 20-9
adding member properties 20-11
adding members 20-12
cloning 20-9
modifying chat settings 20-5
modifying general chat settings 20-7
chat settings, cloning 20-5
child codes 6-6
chronic alarm settings
defined 19-9
modifying 19-9
cloning
address books 18-1
agencies 4-6
alarm company records 19-1
alerts for in-station 22-10
alerts for out-of-station 22-12
chat rooms 20-9
chat settings 20-5
commands 21-2
configuration items 2-10
contractor information 15-2, 15-9
contractor rotation information 15-16
coverage groups 13-2
data elements 16-34
devices 11-43
dispositions 13-43
equipment 11-44
external systems 33-6
GPS device IDs 11-64
groups 18-12
how to 2-10
incident response factors (IRFs) 13-37
incident type aliases 13-6
incident type codes 13-4
manual notifications 24-4
MDTs 11-44
modifying circumstance codes 13-8
override records 22-14
pager groups 11-60
pagers 11-58
personnel records 11-7
plans 7-2
premise/hazard records 13-58
premise/hazard types 13-53
radio groups 11-57
radios 11-55
response messages 13-45
source codes 13-50
status monitor displays 32-26
systems 11-67
trigger groups 33-4
triggers 33-1
unit status codes 10-11
unit-based alerts that override default scheme . . . 22-14
units 10-2
watch lists 31-37
workstations 11-44
closed incidents, duration on status monitors 32-33
closed status 22-37
closing incidents, after last active unit cleared 13-13
codes
activity, adding 10-29
adding to lists 6-4, 6-7
configuring for premise/hazard 13-53
command line
adding commands 21-1
configuring for mobile 16-17
configuring identifiers 21-7
displaying errors 21-10
enabling command-line dispatching 13-38
modifying behaviors 21-10
modifying separators 21-8
requiring review of comments 13-12
unit information 10-22
view required before dispatch 13-12
command permissions, roles 8-7

commands
adding . . . 21-1
cloning . . . 21-2
modifying identifiers . . . 21-5
comments
required for dispo . . . 13-44
reviewing before dispatch . . . 13-38
concurrent logins
agency based . . . 9-4, 11-48
role based . . . 8-4
configuration items
cloning . . . 2-10
deleting . . . 2-11
exporting . . . 2-12
importing . . . 2-13
configure vehicles
overview . . . 11-20
configuring . . . 28-1
alerting interface . . . 22-1
alerting scheme for agency . . . 22-7
alerting settings . . . 22-3
command line identifiers . . . 21-7
external system interface . . . 22-21
icons . . . 25-16
Infotrak interface . . . 22-37
new agency details . . . 4-4
premise/hazard settings . . . 13-56
queries . . . 31-1
radios interface . . . 22-45
trigger groups . . . 33-4
triggers . . . 33-1
units . . . 10-4
configuring foreign agencies . . . 22-33
contact complainant default value . . . 13-16
contacting technical support . . . 1-5
contacts, viewing in address books . . . 18-11
contractor capabilities
adding . . . 15-4
exporting . . . 15-4
importing . . . 15-4
contractor information
business contact . . . 15-9
cloning . . . 15-9
exporting . . . 15-2, 15-9
importing . . . 15-2, 15-9
person contact . . . 15-12
contractor rotations
adding new . . . 15-16
cloning . . . 15-16
configuring . . . 15-16
exporting . . . 15-16
importing . . . 15-16
contractor types
adding . . . 15-2
setting for rotation . . . 15-15
contractors
action codes . . . 15-6
adding new individual . . . 15-9
address information for businesses . . . 15-13
address information for persons . . . 15-14
auto club affiliations . . . 15-8
availability . . . 15-15
configuring individual . . . 15-8
default rotation . . . 15-20
general information for agency . . . 15-2
payment methods . . . 15-8
conventions . . . 1-5
keyboard . . . 1-4
typographic . . . 1-5
copying
response cards . . . 14-10
run cards . . . 14-26
coverage groups
adding . . . 13-2
cloning . . . 13-2
definition . . . 13-2
credentials, saving . . . 11-45
cross staffing groups, defined . . . 10-19
cross staffing, unit status . . . 10-19
customer support, Motorola Online . . . 1-6

D

data elements
cloning . . . 16-34
defined . . . 16-34
modifying . . . 16-34
debounce factor . . . 12-3
default contractor rotation . . . 15-20
default incident type . . . 22-33
default location
assigning . . . 23-2
setting for areas, beats, sectors . . . 23-1
default role . . . 8-1
default sort order for previous incident searches . . . 13-23
default source codes, setting . . . 13-52
default unit status transactions . . . 10-24
definitions
foreign agency . . . 22-27
foreign CAD system . . . 22-27
local agency . . . 22-27
local CAD system . . . 22-28
deleting configuration items . . . 2-11
device profiles
BOLO information . . . 11-24
general information . . . 11-22
incident content . . . 11-27

message content 11-28
notification content 11-30
overview 11-22
query content 11-31
setting emergency notifications 11-26
device types
ASTRO radio 11-35
general information 11-35
login information 11-36
MDT 11-35
overview 11-34
permissions 11-39
printers 11-38
workstation 11-35
devices 11-46
adding a GPS device 11-65
cloning 11-43
exporting 11-43
GPS, cloning 11-64
GPS, configuring 11-64
GPS, creating 11-64
importing 11-43
printer, configuring 11-61
printer, creating 11-61
direct GPS reporting cadence 25-24
display format for blocks 25-9
display on add, status monitors 32-31
display settings
configuring 17-1
overview 17-1
displaying
dynamic help as default 21-10
errors on command line 21-10
dispositions
adding disposition codes 13-43
adding false alarms records for incident 13-44
at least one required 13-12
available for IRFs 13-39
cloning 13-43
closing incidents 13-39
comments required 13-44
defined 13-43
previous phone number search 13-44
report required 13-44
required for all units 13-12
required only for primary unit 13-12
required to close incident 13-12
distance units 4-5
drill down information, adding query type 31-33
duplicate fields, adding query type 31-27
duplicate incident checks 13-18
duty types
adding 10-31
definition 10-30
exporting 10-31
importing 10-31
setting sort order 14-32
dynamic help
defined 21-10
displaying as default 21-10

E

email messages
configuring 26-11, 26-13
properties 26-11, 26-13
emergency mode, enabling 9-8
emergency notifications
adding from the form 24-1
defined 24-1
mobile 24-1
enabling
alerting 22-4
auto alerting 22-4
entity mapping 29-4
equipment
adding 11-41
cloning 11-44
exporting 11-44
importing 11-44
exceed call stack limit by one 13-20
exclude settings, watch list, adding 31-41
exporting
activity codes 10-29
capability groups 11-2
contractor capabilities 15-4
contractor information 15-2, 15-9
contractor rotation information 15-16
devices 11-43
duty types 10-31
equipment 11-44
GPS device IDs 11-64
how to 2-12
incident type aliases 13-6
MDTs 11-44
modifying circumstance codes 13-8
out-of-station information 22-12
override records 22-14
pager groups 11-57, 11-60
pagers 11-58
plans 7-2
premise/hazard records 13-58
premise/hazard types 13-53
radios 11-55
response categories 14-36
response classes 14-13
response descriptors 14-17

response IDs 14-15
response modes 14-11
roles 8-2
run cards 14-19
unit status codes 10-11
workstations 11-44
exporting incident response factors 13-37
exporting incident type codes 13-4
external adapters
configuring agencies 29-3
entity mapping 29-4
overview 29-1
PMDC 29-1
external systems
adding for trigger points 33-6
cloning 33-6
configuring interface 22-21
local agency settings, configuring 22-24
system identification, configuring 22-23
trigger points 33-6

F

false alarms
modifying 19-10
overview 19-10
features, defined 4-7
field initiated incidents 13-19
field interdependencies in provisioning 3-11
filters
using 2-7
using wildcards in filter searches 2-9
fixed areas, status monitors 32-31
flags, incident update 32-35
follow-me settings 32-58
fonts
default CAD display 32-18
display sets 32-53
monitors in display sets 32-54
foreign agencies, provisioning 22-33
foreign agency
configuring 22-33
defined 4-5, 22-27
incident status 22-37
foreign CAD system
defined 22-27
incident received *from*, incident source code . . . 22-36
receive incident update *by* 22-33
receive incident update *from* 22-36
send incident updates *to* 22-33, 22-36
send incidents *to* 22-36
unit status updates received *from* 22-36
unit status updates sent *to* 22-33
foreign CAD systems, provisioning 22-29
foreign units 13-18
form fields, adding query type 31-20
frequency settings for watches, adding 31-40
function keys
modifying for CAD 16-28
modifying for Mobile 16-28, 16-30, 16-32

G

gate status, configuring timeout values 25-41
geocode location for blocks 25-9
geodatabase, exporting the error report 25-4
geodatabase, revalidating provisioned addresses 25-2
geodatabase, setting active 25-1
global offset setting 25-8
GPS cadence, setting 25-22
GPS devices
adding 11-65
cloning 11-64
configuring 11-64
creating 11-64
exporting 11-64
importing 11-64
viewing settings 28-2
groups
adding 18-12
adding existing entries 18-15
adding general information 18-12
adding new entries 18-17
cloning 18-12

H

hazard information. *See* premise/hazard
height units 4-5
high and low cross blocks, displaying 25-8
high and low cross streets
displaying 25-8
hot hits
adding query type 31-28
configuring at the agency level 31-61
defined 31-28, 31-61

I

icons
configuring 25-16
modifying for status monitors 32-3
icons on status monitors
call control 32-8
capability icons 32-8

capability state 32-6
dynamic 32-7
shared unit 32-7
unit 32-7
unit-equipped 32-6
vehicle flag 32-5
icons used in status monitors 32-3
identifiers
configuring 21-7
modifying 21-5
setting default value 21-5
import errors for metadata 31-5
importing
activity codes 10-29
capability groups 11-2
contractor capabilities 15-4
contractor information 15-2, 15-9
contractor rotation information 15-16
devices 11-43
duty types 10-31
equipment 11-44
GPS device IDs 11-64
how to 2-13
incident type aliases 13-6
incident type codes 13-4
MDTs 11-44
metadata for queries 31-2
modifying circumstance codes 13-8
out-of-station records 22-12
override records 22-14
pager groups 11-57, 11-60
pagers 11-58
plans 7-2
premise/hazard records 13-58
premise/hazard types 13-53
radios 11-55
response categories 14-36
response classes 14-13
response descriptors 14-17
response IDs 14-15
response modes 14-11
roles 8-2
run cards 14-19
unit status codes 10-11
workstations 11-44
importing incident response factors 13-37
incident icons
adding 25-16, 25-20
modifying 25-16
incident management fields, text-to-speech 16-22
incident numbers, generating from Records 22-56
incident response factor. *See* IRFs
incident response factors
exporting 13-37
importing 13-37
incident source code
default *for* incident *from* foreign CAD system . . . 22-36
incident status monitors
modifying colors for CAD 32-15
modifying colors for MDT 32-22
incident status, default for foreign agency 22-37
incident type aliases
adding 13-6
cloning 13-6
displaying in CAD 4-5
displaying in status monitors 32-34
exporting 13-6
importing 13-6
incident type codes
adding 13-4
adding details 13-4
cloning 13-4
exporting 13-4
importing 13-4
incident type, default 22-33
incident types, adding settings for response messages . 13-49
incident update counter 32-40
incident update flag 32-35
incident updates
receive *by* the foreign CAD system 22-33
receive *from* foreign CAD system 22-36
send *to* foreign CAD system 22-33, 22-36
incidents
alerts for mobile units 13-33
closing with dispositions 13-39
field initiated 13-19
initial status 13-12
mature status 13-12
requiring comment review before dispatch 13-38
source codes, adding 13-50
traffic stops 13-18
incoming line types
call control center 12-5
incoming lines
ACD 12-7
call control center 12-4, 12-6
intercom 12-7
ring group 12-7
ringdown 12-7
incorrect ALI records 12-7
Infotrak interface, configuring 22-37
initial status for incident 13-12
initiating incidents
auto populate 911 13-16
automatically add comments 13-17
contact complainant default 13-16
create associated 13-17
duplicate incident checks 13-18

field incidents 13-19
form after initiation 13-16
traffic stops 13-18
initiation defaults, modifying 13-15
in-station, configuring alerts for 22-10
interface fields, adding query type 31-19
interfaces
adding query types 31-18
alerting, configuring 22-1
configuring ProQA and ProQA Paramount 22-39
external system, configuring 22-21
external system, using as a call for service interface . . . 22-27
Infotrak, configuring 22-37
ProQA Paramount, configuring 22-39
ProQA, configuring 22-39
radios, configuring 22-45
internationalization
filter operations 34-3
phone number format 34-1
IRFs
adding 13-39
adding attributes 13-39
adding for response cards 14-3
adding general information 13-37
alarm level 13-40
cloning 13-37
definition 13-39
dispositions 13-39
modifying circumstance 13-38
notification message 13-42
overview 13-37
previous incident searches 13-38
priority level 13-40
review incident comments 13-38

J

jurisdictions 23-4
adding response classes for locations 23-4
assigning default location 23-2
assigning printers for stations 23-6
assigning response class 23-2
defining response classes for locations 23-4

K

key fields
query response mapping 31-52, 31-54
keyboard conventions 1-4
keywords for blocks 25-9
keywords, ready reference books 18-9

L

legend, displaying 25-8
list items 6-6
lists
adding 6-6
adding general information 6-6
child codes 6-6
parent codes 6-6
qualifiers 6-4
Related list item 6-6
local agencies, provisioning 22-31
local agency, defined 22-27
local CAD system, defined 22-28
location verification information, modifying 25-6
locations 23-4
adding for response messages 13-48
adding responses classes for 23-4
defining response classes for 23-4
logging in 2-1
logging out 2-15
login icon, mobile 16-14
logins
concurrent for agency 9-4, 11-48
concurrent for roles 8-4
logon
cached credentials 11-45

M

magnetic stripe readers
configuring 28-5
mobile units 28-5
manual notifications
adding from the form 24-3
attaching to IRFs 24-3
cloning 24-4
defined 24-3
external email 24-3
mapping
adding call location icons 25-19
adding camera icons 25-21
adding incident icons 25-16
adding unit icons 25-20
CAD zoom behavior 25-28
configure non-GPS equipped units display 25-32
configuring icons 25-16
configuring person location 25-33
displaying associated units on map 25-25
displaying units of associated incidents 25-25
exporting geodatabase error reports 25-4
fields that display on mobile map 25-27
general agency setting for CAD 25-25

general agency setting for mobile 25-27
modifying cadence 25-22
modifying call location icons 25-19
modifying camera icons 25-21
modifying incident icons 25-16
modifying location verification information 25-6
modifying route solving settings 25-13
modifying unit icons 25-20
person icon, setting for when icon display 25-34
person icon, setting information that displays . . 25-35, 25-37
revalidating provisioned addresses 25-2
route solving settings by vehicle type 25-15
setting mouse hover display 25-30
setting the active geodatabase 25-1
MDT device type 11-35
MDTs
adding 11-43
cloning 11-44
exporting 11-44
importing 11-44
message folders
CAD 26-19
Handheld 26-22
Mobile 26-17
Smart Client 26-21
message types
BOLO 26-11, 26-13
CAD settings 26-12
email 26-11, 26-13
general settings 26-9
Mobile settings 26-10
notification 26-11, 26-13
query 26-11, 26-13
Smart Client settings 26-14, 26-16
messages
folders 26-19
modifying alternative routing 26-24
modifying MDT message types 26-10
messaging
alias 11-10
CAD agency settings 26-5
general agency settings 26-2
Mobile agency settings 26-4
modifying CAD message folders 26-19
modifying CAD message types 26-12
messaging fields, selecting for text-to-speech 16-24
metadata
import errors 31-5
importing for queries 31-2
updating for queries 31-5
mobile browsers, modifying agency settings . . . 17-1, 27-1
mobile settings
action bar 16-5
adding voices 16-21
address book icon 16-14
alerts 13-33
BOLO text-to-speech 16-25
changing voices 16-20
chat fields for text-to-speech 16-26
command line 16-17
fields for query types 16-22
incident fields played as text-to-speech 16-22
login icon 16-14
magnetic stripe readers 28-5
messaging fields played text-to-speech 16-24
modifying function keys 16-30, 16-32
navigation bar 16-10
option buttons 16-7
services area 16-4
status bar 16-13
text-to-speech 16-19
modifying 11-59
agency defaults for status monitors 32-2
agency settings for mobile browsers 17-1, 27-1
alternative routing for messages 26-24
CAD folders 26-19
CAD function keys 16-28
CAD message types 26-12
cadence 25-22
call location icons 25-19
camera icons 25-21
capabilities 11-7
chat settings 20-5
chronic alarm settings 19-9
command line unit information 10-22
data elements 16-34
false alarms 19-10
function keys for CAD 16-28
function keys for Mobile 16-30, 16-32
general chat settings 20-7
icons for status monitors 32-3
incident icons 25-16
incident management query settings 31-64
incident status colors 32-15, 32-22
initiation defaults 13-15
location verification information 25-6
MDT message types 26-10
Mobile function keys 16-28
pagers 11-59
response classes for locations 23-4
right click menu options 32-9
route solving settings 25-13
search defaults 13-23
separators 21-8
service defaults 13-10
service settings 13-10
shift ID code information 10-23

state interface ORI 31-59
state interface settings 31-57
transaction information 10-24
unit icons 25-20
unit status colors 32-13, 32-21
modifying circumstance codes
adding 13-8
cloning 13-8
exporting 13-8
importing 13-8
IRFs 13-38
modifying circumstance, default 22-33
Motorola Online, using 1-6
mouse hover display on maps 25-30
move ups
configuring 10-32
setting up incident creation 13-20
MUD setting 25-12
multi-beat
direction 25-8
displaying after address verification 13-13
distance 25-8
global offset 25-8
multi-unit display 25-12
MW810 button configuration 16-32

N

name of foreign CAD system 22-30
navigation bar, configuring for mobile 16-10
notes 1-5
notes and cautions 1-5
notification message, IRFs 13-42
notification messages
alerts 26-11, 26-13
configuring 26-11, 26-13
manual, cloning 24-4
properties 26-11, 26-13
notify on failure, email addresses 22-31
number of retries 22-31

O

one-pass processing 13-18
open incidents, allowing 13-12
open status 22-37
option buttons, configuring for mobile 16-7
out-of-station
configuring alerts for 22-12
records, cloning 22-12
out-of-station information
exporting 22-12
importing 22-12
override area 13-39
override records
cloning 22-14
exporting 22-14
importing 22-14
owning agency 5-1

P

pager groups
adding 11-60
cloning 11-60
configuring two-tone 11-57
exporting 11-57
importing 11-57, 11-60
pagers 11-58, 11-59
adding 11-59
cloning 11-58
exporting 11-58
importing 11-58
parent codes 6-6
passwords
configuring for agency 9-6
forcing changes 9-11
peripherals
viewing GPS settings 28-2
viewing printer settings 28-1
permission sets
adding 5-3
overview 5-2
permissions
call control center 8-7
for device types 11-39
for query types 8-9
person location
setting cadence 25-38
setting icon display information 25-35
personnel
adding authorization information 11-14
adding contact information 11-11
adding detail information 11-8
adding resource assignment information 11-16
adding roles information 11-13
cloning records 11-7
required to place unit on duty 10-27
placing units on duty
require odometer reading 10-27
validate odometer reading 10-27
validate unit ID 10-27
plans
active plan, setting 7-5
adding from the form 7-2
cloning 7-2

exporting 7-2
importing 7-2
modifying 7-4
viewing active 7-6
PMDC configuration 29-1
preempt
default value for FI 13-13
default value for ID 13-13
default value for II 13-13
defined 13-13
premise/hazard
adding records 13-58
codes and proximities, configuring 13-53
editing records 13-58
records, cloning 13-58
records, exporting 13-58
records, importing 13-58
settings, configuring 13-56
types, cloning 13-53
types, exporting 13-53
types, importing 13-53
premise/hazard types
exporting 13-53
importing 13-53
preprogrammed SMS messages 12-20
previous incident searches
default sort order 13-23
IRFs to include 13-38
search distance 13-23
previous phone number searches 13-44
previous subject/vehicle searches
adding roles 13-24
including persons/vehicles from previous searches 13-24
setting height units 13-24
setting initial defaults 13-24
setting weight units 13-24
printer devices
configuring 11-61
creating 11-61
printers 28-1
assigning for stations 23-6
configuring 11-61
viewing settings 28-1
printing
parameters for alerting 22-6
priorities
configuring 13-25
properties 13-25
priority level, IRFs 13-40
priority updates
day colors for MDT 13-30
enabling for CAD 13-28
enabling for MDT 13-30
night colors for MDT 13-30
notifications for CAD 13-28
selecting fields for CAD 13-28
selecting fields for MDT 13-30
ProQA 22-39
ProQA Paramount 22-39
ProQA Paramount, configuring 22-39
ProQA, configuring 22-39
provision
name of foreign CAD system 22-29, 22-30
notification recipients 22-29
number of retries 22-31
receive acknowledgments when receiving incidents . . . 22-31
retry interval 22-31
send acknowledgments when receiving incidents . 22-31
whom to notify on failure 22-31
provisioning
agency 3-1
agency type 3-1
call for service interface 22-28
default incident source code for foreign agency . . 22-36
default incident status for foreign agency 22-37
field interdependencies 3-11
foreign agencies 22-33
foreign CAD systems 22-29
global 3-1
local agencies 22-31
provisioning overview
foreign agency 22-29
local agency 22-28
provisioning permissions roles 8-7
Provisioning window, overview 2-4
proximities, configuring for premise/hazard 13-53
pseudoarea 7-1
purge operations
adding online settings 30-3
adding reporting data warehouse settings 30-5

Q

qualifiers 6-4
queries
adding frequency settings 31-40
adding query type cascading queries 31-30
adding query type drill down information 31-33
adding query type duplicate fields 31-27
adding query type form fields 31-20
adding query type hot hits 31-28
adding query type interface fields 31-19
adding query type interfaces 31-18
adding query type response fields 31-24
adding query type settings 31-16
adding watch list exclude settings 31-41

adding watch list settings 31-38
adding watch lists 31-38
agency-level hot hits 31-61
configuring 31-1
configuring at Suite level 31-7
configuring CAD settings 31-13
configuring for ALPR hits 31-54
configuring MDT settings 31-12
configuring two-factor authentication 31-56
importing metadata 31-2
mapping query types 31-34
modifying incident management query settings . 31-64
modifying state interface ORI 31-59
modifying state interface settings 31-57
overview of processing 31-1
PremierOne Records 31-6
response throttling 31-10
settings, configuring 31-10
query fields, selecting for text-to-speech 16-22
query messages
configuring 26-11, 26-13
properties 26-11, 26-13
query responses
copying to incidents 13-13
key fields 31-52, 31-54
mapping fields to Person or Vehicle form 31-52
query set, defined 31-19
query types
adding cascading queries 31-30
adding drill down information 31-33
adding duplicate fields 31-27
adding form fields 31-20
adding hot hits 31-28
adding interface fields 31-19
adding interfaces 31-18
adding response fields 31-24
adding settings 31-16
permissions 8-9
query types, configuring for mobile 16-22

R

radio groups
cloning 11-57
configuring 11-57
radio PTT status monitors 32-35
radio system ID 22-45
radios
adding 11-55
adding channels to channel groups 22-54
channel groups 22-47
cloning 11-55
configuring systems 22-45
exporting 11-55
importing 11-55
overview 22-45
RIN 11-56
talkgroups 22-53
ready reference books
call control numbers 18-9
fields 18-9
keywords 18-9
recommendations
advanced methods A-19
alternate methods A-18
based on AVL/ARL A-18
based on fixed unit responses A-16
based on location A-18
based on run card assignments A-17
based on unit's jurisdictional assignments A-17
personnel skill methods A-19
settings, holding units for dispatch 14-29
settings, setting sort order for capabilities 14-31
settings, setting sort order for duty types 14-32
specific unit methods A-20
Related Lists item, lists 6-6
report required for dispo 13-44
resetting lock accounts 11-10
resources
adding 9-1-1 systems 11-67
adding device general information 11-44
adding device login settings information 11-46
adding device permissions information 11-50
adding personnel assignment information 11-16
adding personnel authorization information 11-14
adding personnel contact information 11-11
adding personnel detail information 11-8
adding personnel roles information 11-13
adding to roles 8-13
MDTs 11-43
workstations 11-43
response cards
adding for IRFs 14-3
adding for response IDs 14-3
copying 14-10
definition 14-2
response categories
adding 14-36
definition 14-36
exporting 14-36
importing 14-36
response classes
adding 14-13
assigning by jurisdiction 23-2
exporting 14-13
for locations 23-4
importing 14-13

response descriptors
adding 14-17
definition 14-17
exporting 14-17
importing 14-17
response fields, adding query type 31-24
response IDs 14-23
adding 14-15
adding for response cards 14-3
definition 14-15
exporting 14-15
importing 14-15
response messages
adding area, sector, beat settings 13-47
adding incident types settings 13-49
adding locations settings 13-48
adding subject and text settings 13-46
cloning 13-45
response modes
adding 14-11
definition 14-11
exporting 14-11
importing 14-11
retry interval 22-31
reviewing incident comments before dispatch 13-38
right click menu options, modifying 32-9
RIN 11-56
roles
adding 8-2
adding general information 8-2
adding permissions 8-5
adding resources to 8-13
agency admin 8-1
chat permissions 8-7
command permissions 8-7
concurrent logins 8-4
default 8-1
exporting 8-2
group permissions 8-7
importing 8-2
messaging permissions 8-7
provisioning permissions 8-7
query permissions 8-7
viewing a preview of permissions 8-13
route solving settings
by vehicle type 25-15
modifying 25-13
row color, status monitors 32-31
run cards
adding 14-20
adding IRF information 14-24
adding response ID information 14-23
copying 14-26
definition 14-19
exporting 14-19
importing 14-19
order, adding 14-20
searching 14-19
tie breaking rules 14-27
run cards, detailed explanation A-1
run minimized, status monitors 32-31

S

scheduled BOLOs 26-10
search defaults, modifying 13-23
search distance for previous incidents 13-23
searching
run cards 14-19
using filters 2-9
using wildcards 2-9
sectors
adding to response message settings 13-47
setting default location 23-1
send incidents *to* foreign CAD system 22-36
separators, modifying 21-8
service defaults, modifying 13-10
service settings
modifying 13-10
modifying initiation defaults 13-15
modifying search defaults 13-23
modifying service defaults 13-10
priorities 13-25
services area, mobile unit 16-4
services, defined 4-7
setting provisioning access, trusted agencies 5-7
settings
active geodatabase 25-1
active plan 7-5
adding query type 31-16
maximum speed for a vehicle type 14-34
watch list, adding 31-38
shift ID code information, modifying 10-23
signing off 2-15
signing on 2-1
skills
assigning to personnel 11-10
configuring 11-4
defined 11-4
Smart Client 26-1
Smart Copy Query Responses
provisioning for CAD 13-13
SMS calls held too long 12-2
SMS calls, held to long 12-2
source codes
adding 13-50
cloning 13-50

- defined . . . 13-50
- setting default . . . 13-52

state interface settings, modifying . . . 31-57
station alert status monitor . . . 32-35
stations
- enabling . . . 4-5
- general information, adding . . . 23-6
- preferred recommendation order, adding . . . 23-8
- setting information for . . . 23-6

status
- closed . . . 22-37
- open . . . 22-37

status bar, configuring for mobile . . . 16-13
status codes
- properties . . . 10-11
- timeouts . . . 10-13

status duration timer . . . 32-37
status monitors
- active includes in pending monitor . . . 32-35
- adding displays . . . 32-26, 32-55
- adding windows incident status color options . . . 32-49
- alerts information . . . 32-44
- allow orphan . . . 32-31
- associated units on incident monitor . . . 32-34
- background colors for monitors . . . 32-19
- closed incidents on incident monitor . . . 32-34
- coverage and monitored areas . . . 32-31
- coverage areas . . . 32-31
- display horizontal . . . 32-33
- display on add . . . 32-31
- display vertical . . . 32-33
- displaying incident aliases . . . 32-34
- displays, cloning . . . 32-26
- duration for closed incidents . . . 32-33
- fields . . . 32-36
- filtering information . . . 32-40
- fixed areas . . . 32-31
- fonts for default CAD display . . . 32-18
- fonts for display sets . . . 32-53
- fonts for monitors in display sets . . . 32-54
- general information . . . 32-26
- grouping information . . . 32-42
- icons . . . 32-3
- incident update counter . . . 32-40
- modifying agency defaults . . . 32-2
- modifying icons . . . 32-3
- modifying incident status colors . . . 32-15, 32-22
- modifying right click menu options . . . 32-9
- modifying unit status colors . . . 32-13, 32-21
- monitored areas . . . 32-31
- number of incidents to display . . . 32-35
- off duty units . . . 32-35
- pending incidents on incident monitor . . . 32-34
- position information . . . 32-43
- radio PTT . . . 32-35
- right-click menu options . . . 32-47
- row color . . . 32-31
- run minimized . . . 32-31
- sorting information . . . 32-39
- station alert . . . 32-35
- supervisor . . . 32-35
- toning system . . . 32-36
- unit status color options . . . 32-49
- window information . . . 32-28
- windows general information . . . 32-28

suite-level query configuration . . . 31-7
supervisor status monitors . . . 32-35
support, contacting . . . 1-5
system notifications, configuring . . . 9-9
systems
- adding 9-1-1 . . . 11-67
- cloning . . . 11-67

T

talkgroups, configuring . . . 22-53
technical support, contacting . . . 1-5
text-to-speech
- BOLO fields . . . 16-25
- Chat fields . . . 16-26
- configuring for mobile . . . 16-19
- incident fields . . . 16-22
- messaging fields . . . 16-24
- selecting incident management fields . . . 16-22
- selecting messaging fields . . . 16-24
- selecting query fields . . . 16-22

time format . . . 4-5
toning
- configuring existing systems at agency level . . . 22-8
- defined . . . 22-2, A-14
- enabling existing systems at agency level . . . 22-8
- system code . . . 11-69
- system name . . . 11-69
- system status monitors . . . 32-36

traffic stop settings . . . 13-18
transaction information, modifying . . . 10-24
trigger groups
- adding . . . 33-4
- cloning . . . 33-4
- configuring . . . 33-4
- configuring trigger groups . . . 33-4

trigger point system
- adding batch transmission information . . . 33-8
- adding trigger groups . . . 33-4
- adding triggers . . . 33-1
- configuring triggers . . . 33-1

triggers

adding 33-1
cloning 33-1
configuring 33-1
trusted agencies
adding permission sets 5-3
overview 5-1
owning agency 5-1
permission sets 5-2
setting CAD command access 5-6
setting permissions by owning agencies 5-9
setting provisioning access 5-7
trusted agency 5-1
two-pass processing 13-18
two-tone
pager groups, configuring 11-57
radio alerting 22-47
radio alerting, defined 22-50
typographic conventions 1-5

U

unit equipment, adding 10-7
unit history, include personnel names 10-27
unit icons, modifying 25-20
unit IDs, adding 10-2
unit management
adding capabilities 11-6
adding capability information for preassigned units 10-8
adding capability settings for preassigned units . . 10-9
adding general preassignments 10-4
adding status code properties 10-11
adding status code timeouts 10-13
adding unit equipment 10-7
adding unit status codes 10-11
adding vehicle information 10-6
modifying capabilities 11-7
modifying command line information 10-22
modifying shift ID code information 10-23
modifying transaction information 10-24
unit recommendations
detailed explanation A-16
jurisdictional methods A-16
unit status and cross staffing 10-19
unit status codes
adding 10-11
cloning 10-11
exporting 10-11
importing 10-11
unit status colors, modifying 32-13, 32-21
unit status monitors
status duration timer 32-37
updated duration timer 32-37
unit status updates
received *from* foreign CAD system 22-36
send *to* foreign CAD system 22-33
units 10-4
adding capabilities information for preassignments 10-8
adding capability setting for preassignments 10-9
adding equipment information for preassignments . 10-7
adding general preassignments 10-4
adding personnel information for preassignments . 10-6
adding preassignments 10-4
adding unit vehicle information for preassignments 10-6
call stacking settings 13-20
capabilities, adding for preassigned units 10-8
capability settings, adding for preassigned units . . . 10-9
cloning 10-2
default unit status transactions 10-24
displaying for associated incidents 25-25
enabling call stacking 13-20
holding for dispatch 14-29
include personnel names in unit history 10-27
personnel required to place on duty 10-27
preassignments 10-4
require odometer reading when placing on duty . . 10-27
require validate odometer reading for on duty . . . 10-27
validate unit ID when placing on duty 10-27
validating unit location 10-25
unlocking accounts 11-10
unprocessed incidents
defined 13-18
setting timeout 13-18
updated duration timer 32-37
updating metadata for queries 31-5
use cached credentials 11-45
using, Motorola Online 1-6

V

validating unit location on every transaction 10-25
vehicles
adding to units 10-6
roles for previous vehicle search 13-24
setting maximum speed for a vehicle type 14-34
viewing
active plans 7-6
GPS settings 28-2
preview of role permissions 8-13
printer settings 28-1
visual alerts for mobile units 13-33
voice calls, held to long 12-2
voices, adding 16-21

W

watch lists

adding 31-38
adding non-system generated 31-40
cloning 31-37
exclude settings, adding 31-41
settings 31-38
weight units 4-5
wildcards
symbols 2-9
using in filter searches 2-9
using with addresses 25-7
windows
alerts information 32-44
fields 32-36
filtering information 32-40
general information 32-28
grouping information 32-42
incident and unit status color options 32-49
position information 32-43
right click menu options 32-47
sorting information 32-39
work area, overview 2-5
working agency 13-3
workstation device type 11-35
workstations
adding 11-43
cloning 11-44
configuring 11-43
exporting 11-44
importing 11-44

Z

zooming, settings for CAD map 25-28