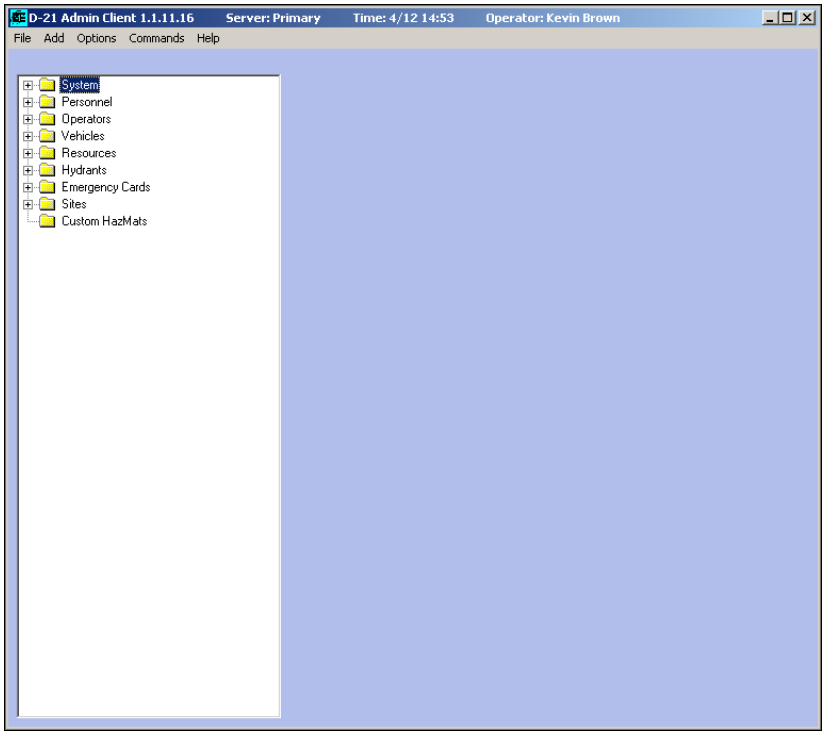


D-21 Admin Client Revision 1.1.32
User Guide

Contact Information

Monaco Enterprises, Inc. P.O. Box 14129, Spokane Valley, WA 99214-0129; 14820 E. Sprague Ave., Spokane Valley, WA 99216-2149
Phone (509) 926-6277 **Fax** (509) 924-4980 **E-mail** service@monaco.com **Web** www.monaco.com

Document Information

Identification

D-21 Admin Client Revision 1.1.32 User Guide
001-399-00 Revision V.3 9/17

Trademark Notice

The Monaco Enterprises, Inc. (Monaco) logo and MEI are registered trademarks of Monaco. All other product names and logos in this manual are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

Copyright Notice

© 2017 by Monaco Enterprises, Inc. All rights reserved. This document contains proprietary information and is for exclusive use by Monaco customers. Use or reproduction other than by Monaco customers is expressly prohibited unless authorized in writing by Monaco.

Content Disclaimer

Monaco makes every attempt to keep this document up-to-date and accurate. However, these instructions are not intended to cover all details or variations in equipment nor to provide for every possible contingency to be met in connection with installation, operation, or maintenance. The user is responsible to ensure that the requirements of the project are being met, design details are verified, and the equipment is correctly installed, operated, and maintained to meet all applicable codes, standards, and regulations.

Monaco makes no representation or warranty, express or implied, as to the reliability of this document and will not be held liable for damages due to inaccuracies. If further information is needed or a particular problem arises that needs to be further described, contact Monaco.

Suggestions

If you have comments or suggestions on how we may improve this document, send them to:

Monaco Enterprises, Inc. Attention: Technical Publications, P.O. Box 14129, Spokane Valley, WA 99214-0129

Warranty and Liability

Subject to the exceptions and conditions below, Monaco agrees to repair or replace any defect of material or workmanship of equipment manufactured by Monaco that develops within 12 months from the date of delivery but no more than 14 months after date of shipment from Monaco (whichever is earlier), free of charge F.O.B. Spokane, Washington. You must notify Monaco of any defect and provide either satisfactory proof of the defect or return the defective equipment to Monaco for examination at your expense in order for the equipment to be repaired or replaced under warranty.

Monaco does not provide warranty for expendable components or accessories incorporated or used with equipment manufactured by Monaco, such as batteries, visual indicators, fusing devices, etc. In addition, Monaco does not warrant components or accessories not manufactured by Monaco; however, Monaco may help you seek adjustment from the manufacturer if the expendable components or accessories are under warranty.

You assume full responsibility for whether or not the equipment and any programs meet your specifications, capacity, capabilities, versatility, and other requirements; the installation and the condition and effectiveness of the operating environment in which the equipment and software are to function; and maintaining the equipment as specified.

All Monaco Central Receiving server installations require an authorized Monaco representative.

Exceptions and Conditions

The following are exceptions and conditions to this warranty:

- Except as stated in this warranty, Monaco makes no warranty, expressed or implied (either in fact or by operation of law), statutory, or otherwise. All warranties not expressly stated in this document are waived by you.
- Monaco is not responsible for damage to any product from accident, unauthorized alteration, abuse, acts of God, misuse, misapplication, or inappropriate or faulty installation.
- This warranty covers only those products that have been properly installed using factory-approved wiring and installation techniques.
- Monaco assumes no liability for products damaged in shipment to Monaco for repair or replacement.
- Monaco disclaims any liability to anyone for any damages of any kind from any cause associated with the manufacture, sale, handling, repair, maintenance, replacement, or use of its equipment.
- Monaco's liability and purchaser's or consumer's exclusive remedy is limited to repair or replacement of nonfunctional product at the factory. Monaco is not liable for incidental or consequential damages, including but not limited to, installation or replacement labor costs.
- Any representation and/or warranty made by any person including dealers, distributors, and representatives of Monaco that are inconsistent or in conflict with the terms of this warranty are not binding unless they are approved in writing by an Officer of Monaco.
- This warranty shall be construed in accordance with and governed by the laws of the State of Washington.
- This warranty gives you specific legal rights and you may also have other rights that may vary from state to state.

Return Procedure

Before returning your equipment, contact a Monaco Customer Service Representative at (509) 926-6277 to receive a return authorization. The return authorization number must be clearly marked on any box in which the returned items are shipped and on all documents related to the return. *Monaco will not accept equipment for repair without prior Return Authorization.*

Replacement and/or repair is subject to review by Monaco and will be done in accordance with this warranty. If the equipment is not under warranty or if the warranty is not in effect because of the Exceptions and Conditions, you will be asked to provide a purchase order for payment of the repair when the Return Authorization number is given. The amount of the purchase order will be based on an estimate of the cost of the repair. If a repair is not feasible, either because of cost or performance reliability of the repaired equipment, Monaco will contact you.

Software License

Monaco grants license to use its software on one computer subject to the following conditions:

- Except as provided in the software license, applicable copyright laws apply to the software.
- You may copy the software for the sole purpose of backup in support of its use on a single computer. All copies must include the copyright notice.
- You may transfer the software and license to another party if the other party agrees to accept the terms and conditions of this agreement. If you transfer the software, you must, at the same time, transfer all copies to the same party or destroy any copies not transferred.
- You may not use, copy, or transfer the software or any copy, in whole or in part, except as expressly provided in this license. If you transfer possession of any copy to another party, your license is automatically terminated.
- This license is effective until terminated. You terminate the license by destroying the software and all copies in any form. License automatically terminates if you fail to comply with any term or condition of this license, in which case, you must destroy the software and all copies of it.

Before You Begin

How to Get Assistance

If you need help with your Monaco products, contact one of our Customer Service Representatives at (509) 926-6277. For other methods of contacting us, see “Contact Information” on page ii.

For Use With

This document is for use with:

Part Number	Description
207-830-00	D-21 Fire Client
207-836-00	D-21G Fire Client with Graphics
207-833-00	D-21M Fire Client with Map and Graphics
207-831-00	D-21 Security Client
207-837-00	D-21G Security Client with Graphics
207-834-00	D-21M Security Client with Map and Graphics
207-832-00	D-21 Fire and Security Client
207-838-00	D-21G Fire and Security Client with Graphics
207-835-00	D-21M Fire and Security Client with Map and Graphics
207-842-00	D-21 Mass Notification System Client
207-848-00	D-21G Mass Notification System Client with Graphics
207-849-00	D-21M Mass Notification System Client with Map and Graphics

Factory Mutual Approval

The D-21, D-21G, and D-21M are approved by Factory Mutual as Public Reporting Coded Radio Alarm Systems. While these products continue to evolve through the addition of new features, the core functionality that allows them to be approved as a Public Reporting Coded Radio Alarm System remains intact.

Overview

The D-21, D-21G, and D-21M Radio Alarm Systems (referred to as the D-21 throughout this document) are Windows®-based Radio Central Receiving Systems. A system can consist of a single client/server workstation or of a server with multiple clients on a LAN or WAN network.

The D-21 includes one or more narrowband radio frequency modems (RFMs) or hard-wire modems. RFMs communicate with remote units via coded radio signals on carrier frequencies in UHF ranges of 406-430 MHz and 450-470 MHz, or the VHF range of 136-174 MHz, or unlicensed spread spectrum. Hard-wire modems use a proprietary protocol to communicate via RS-232 or RS-485.

The D-21 monitors communication status, zone alarm or troubles, ac power failures, battery and charger faults, as well as returns to normal conditions for the following types of Monaco remote units:

- **Building Transceiver** BT2-3, BT2-4, BT2-7, BT2-8, BT2-8S, BT-X Communicator, and Communicator Plus.
- **Fire Alarm Control Panel (FACP) with Integrated Transceiver** M-1, M-2.
- **Fire Alarm Control Panel connected to Building Transceiver** Vulcan I.
- **Addressable FACP with Integrated Transceiver** M-1 and M-2 Monaco Analog Addressable Panel (MAAP).

D-21 incident processing is prioritized so that you can run other Windows-based programs without sacrificing the integrity of the system.

The D-21 software consists of one server and two client programs:

- **D-21 Server** is the database and core of the system.
- **D-21 Admin Client** is used to set up the software for operation. The system administrator uses the D-21 Admin Client to define remote interface drivers (RIDs), remote units, zones, response plans, people, operators, sites, and facilities.
- **D-21 Incident Client** is used by an operator to acknowledge alerts, process incidents, and dispatch resources to the incident site.

Installation

Monaco has installed the appropriate software on your D-21 computers. For information on installing D-21 software, contact Monaco.

Important! *The D-21 server software is preconfigured for redundant, mobile, or stand-alone operation during installation. The server software must be reinstalled to change its function. For information on installing D-21 software, contact Monaco.*

Third-Party Software

The software installed on your D-21 workstation includes the following third-party products:

Important! *Do not remove this software from your system. Do not update this software or install a different version of this software without prior approval from Monaco.*

- **Acrobat Reader** The D-21 Incident Client uses Adobe® Acrobat® Reader® to display aircraft graphics.
- **DWGDirectX** The D-21 software integrates DWGDirectX for viewing some types of graphics.

- **Easy Media Creator** Roxio™ Easy CD and DVD Creator® is installed with the D-21 Fire Incident Client and is used to backup database and media files to CD. For further information about Easy CD and DVD Creator, see the Easy CD Creator User's Guide.
- **pcAnywhere** Symantec™ pcAnywhere™ is installed on the D-21 server and lets Monaco product support technicians remotely access a problem D-21 system (with operator authorization). For further information about pcAnywhere, see the pcAnywhere User's Guide.
- **WSpell ActiveX Spelling Checker** The D-21 software uses WSpell ActiveX Spelling Checker Copyright © 1997-2002 Wintertree Software Inc. to provide spell checking of text fields in the D-21 Incident Client.

Document Summary

This document describes how to use the D-21 Admin Client program to set up the pre-installed D-21 software. The following table identifies the sections of this document with a brief description of the content of each. Refer to "Contents" on page ix for a detailed table of contents.

Section	Description
1	**Starting, Quitting, and Navigating** Read this section to learn how to start, quit, and navigate within the D-21 Admin Client.
2	**Creating the D-21 Database** Read this section to learn how to enter data into the D-21 database.
3	**Setting Up Incident Processing** Read this section to learn how to set up the information required when responding to incidents. This section also contains instructions for customizing the way alerts and incidents are handled.
4	**Customizing the D-21** Read this section to learn how to customize D-21 look-up lists, map settings, and other workstation options.
5	**Adding Media Files** Read this section to learn how to add floor plans, icons, response graphics, and sound files to the Media folder.
6	**Adding the BT-X Communicator** Read this section to learn how to add a multi-application BT-X to the D-21 database.
7	**Configuring Mass Notification** Read this section to learn how to configure remote units for in-building and wide-area mass notification.
8	**Configuring Access Control** Read this section to learn how to configure and operate an access control system in the D-21 Security Client.
9	**Configuring Intrusion Detection** Read this section to learn how to configure remote units for intrusion detection using the D-21 Security Client.

Section	Description
10	**Configuring an E-911 System** Read this section to learn how to configure an E-911 remote interface driver and phone number database for your site.
11	**Configuring Tone Alerting** Read this section to learn how to configure tone alerting with a Tone Generator or a Tone Alert Unit.
12	**Configuring Cameras and Remote Displays** Read this section for information on setting up the D-21 Incident Client's Camera Viewer and the View Generator.
A	**Glossary of Terms**
B	**Configuration Tables**

Associated Documents

Part Number	Description
001-391-00	D-21 Hardware Installation, Operation, and Maintenance Manual
001-392-00	D-21 Incident Client User Guide
001-399-01	D-21 Remote Interface Driver Guide
001-399-02	D-21 Maintenance Guide
001-464-00	D-21 Map Options User Guide

Unpacking and Inspection

Monaco ships the D-21 workstation with the D-21 software installed. For information on unpacking and setting up the D-21 hardware, see the D-21 Hardware IOM Manual (P/N 001-391-00).

Warnings and Cautions

The D-21 Hardware IOM Manual (P/N 001-391-00) provides warnings and cautions regarding the D-21 hardware.

Virus Protection

Because virus protection requirements vary between sites, Monaco does not include virus protection software on D-21 systems.

Caution! *Your system administrator must install the virus protection software necessary to meet your site requirements. Monaco recommends scanning all media and incoming files introduced to the system. Monaco is not responsible for D-21 problems caused by viruses. Service required as a result of a virus may not be covered under warranty.*

Prerequisites

Before running the D-21 software, ensure that the following has been completed:

- The D-21 hardware is assembled, installed, and powered on. See the D-21 Hardware IOM Manual (P/N 001-391-00).
- The remote units are installed and in good working condition. See the documentation included with the remote units.

Contents

Section 1. Starting, Quitting, and Navigating

Starting and Quitting the D-21 Admin Client 1-2
Starting the Single-Server D-21 Admin Client 1-2
Starting a Multi-Server D-21 Admin Client 1-3
Navigating the D-21 Admin Client 1-7
Navigating the Tree Pane 1-7
Menus 1-8
Dialog Boxes 1-11

Section 2. Creating the D-21 Database

Order for Entering Data 2-2
Sites 2-3
Facilities 2-13
Adding Floor Plans 2-27
Remote Interface Drivers (RIDs) 2-30
Adding a RID for the RFM 5000 2-31
Adding a RID for the RFM 7000 and RFM-X 2-38
Reload All RIDs 2-50
Enabling and Disabling RIDs, Units, Zones, and Outputs 2-50
Remote Units 2-51
Unit Class 2-52
Numbering Remote Units 2-54
Creating Remote Unit Groups 2-62
Zones 2-64
Zone Class 2-64
Zone Priority 2-65
Point Reporting Zones 2-71
Outputs 2-74
Creating Output Groups 2-78
Personnel 2-85
Standard Personnel Information 2-86
Custom Personnel Information 2-93
Operators 2-97
Vehicles 2-101
Resources 2-103
HazMats 2-106
Editing HazMats 2-107
Hydrants 2-109
Placing Items on the Map (D-21M) 2-112

Section 3. Setting Up Incident Processing

Response Plans 3-2
Emergency Cards 3-20
Pre-Plans 3-23

Actions 3-27
Using Actions. 3-27
Attaching Actions to Custom Buttons 3-36
Attaching Actions to Status Changes. 3-37
Standard Operating Procedures (SOPs) 3-38
Incident Processing. 3-44
Setting Up Alert Processing. 3-45
Customizing Incident Numbers 3-53
Customizing Incident Class and Status Colors 3-55
Setting Alert Sounds 3-57
Resetting Incident Editing Controls. 3-58
Dispatch Configuration 3-58
Incident Types 3-61
Resource Classes 3-65
Resource Groups 3-66

Section 4. Customizing the D-21

Customizing Lists. 4-2
General Lists 4-2
Fire Lists 4-12
Security Lists 4-14
Personnel Lists. 4-23
Permit/Work Order Lists 4-25
Setting Map Options (D-21 M) 4-33
Configuring Shortest Routes 4-33
Setting Road Closure Color 4-35
Configuring Incident Relocating 4-36
Setting Hydrant Colors. 4-37
Creating Rosters 4-38
Creating a Summary Statistics Log 4-46
Setting Workstation Options 4-49

Section 5. Adding Media Files

Media Files. 5-2
Programs for Generating Media Files 5-2
Floor Plans, Pre-Plans, and Response Graphics. 5-3
Conventions for Naming Media Files 5-4
Importing Floor Plans, Response Graphics, and Pre-Plans 5-5
Icons 5-12
Sounds 5-12

Section 6. Adding the BT-X Communicator

Adding the Multi-Application BT-X 6-2
Adding the BT-X Communicator 6-3
Adding the BT-X Communicator Plus 6-4
Configuring Dual Communication Channels. 6-4
Dual Communication Status 6-5

Dual Communication Testing 6-5

Section 7. Configuring Mass Notification

Within-Building and Wide-Area Mass Notification 7-2
MNS Message Types. 7-2
Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts 7-3
Enabling the RFM 7000 RID for Mass Notification 7-4
Adding Pre-Recorded Messages 7-6
Creating Message Groups 7-7
Adding Broadcast Messages 7-11
Adding a RID for the ACU-1000 Radio Switch 7-13
Configuring Workstations for Multiple Live-Voice Sources 7-16
Adding a BT-X with Mass Notification. 7-18
Pre-Configuring MNS Messages 7-24
Configuring AutoMNS in the D-21 7-29

Section 8. Configuring Access Control

Overview of Access Control 8-2
Setting Up Access Control Units and Readers 8-3
Creating Access Control Groups. 8-4
Creating Access Schedules 8-6
Adding a BT-X with Access Control 8-10
Downloading Settings to Access Control Units 8-20
Operating an Access Control System 8-23
Assigning Cards and PINs. 8-23
Changing Card Assignments. 8-27
Tracking Card Usage. 8-30

Section 9. Configuring Intrusion Detection

Overview of Intrusion Detection 9-2
Setting Up the BT2-8S Security Unit 9-2
BT2-8S Zone Types 9-3
Master Control Zones on the BT2-8S 9-4
Setting Up the BT-X Security Unit 9-11
BT-XS Zone Types 9-11
Master Zones on the BT-XS 9-12
Adding a BT-X with Intrusion Detection 9-14
IDS iButton and PIN Assignments 9-24
Enrolling Administrators. 9-25
Enrolling Users 9-29
Managing iButtons 9-37
Downloading iButton Authentications 9-43

Section 10. Configuring an E-911 System

Configuring an E-911 System 10-2
Creating an E-911 Phone Number Database 10-8

Section 11. Configuring Tone Alerting
Configuring Tone Alerting with a Tone Generator 11-2
Configuring Tone Alerting with a Tone Alert Unit 11-6

Section 12. Configuring Cameras and Remote Displays
Configuring the Camera Viewer 12-2
Configuring the View Generator 12-2

Section 13. Remote Access
Using pcAnywhere 13-2

Glossary of Terms
Glossary of Terms A-2

Configuration Tables
Servers B-2
Clients B-3

How to...

A

Access the IDS Central Enrollment switchboard 9-28
Add a broadcast file 7-11
Add a broadcast message 7-12
Add a BT2-8S security remote unit 9-4
Add a BT-X for in-building mass notification 7-19
Add a BT-X for wide-area mass notification 7-22
Add a BT-X/ACS (M) remote unit 8-12
Add a call list to a response plan. 3-3
Add a custom SOP 3-41
Add a facility. 2-13
Add a floor plan to a facility 2-27
Add a hydrant 2-109
Add a Monaco pre-plan to a response plan. 3-5
Add a multi-application BT-X unit to the D-21 database. 6-2
Add a new entry type to the Security Desk Journal 4-14
Add a new hazardous material 2-106
Add a Permit Type 4-31
Add a person 2-86
Add a phone number to the E-911 database 10-9
Add a pre-plan file to a response plan. 3-7
Add a remote unit 2-55
Add a resource. 2-103
Add a response plan 3-3
Add a RID for an RFM 2-31
Add a RID for an RFM 5000 2-31
Add a RID for an RFM 7000 2-38
Add a Tone Alert Unit. 11-9
Add a vehicle to the database 2-101
Add a View Generator Repeater Display 12-5
Add a zone. 2-65
Add a zone to an output group (D-21G or D-21M) 2-83
Add an action to a response plan. 3-15
Add an AutoMNS message. 7-31
Add an AutoMNS unit group 7-29
Add an E-911 RID 10-3
Add an emergency card. 3-20
Add an IDS application unit 9-21
Add an IDS Master unit 9-14
Add an IDS Master unit with iButton keypad control 9-18
Add an IDS user authentication 9-29
Add an item to a personnel list 4-23
Add an operator. 2-97
Add an output 2-74

Add badging information to personnel 2-93
Add Desk Journal organizations 4-15
Add dispatch instructions to a response plan. 3-9
Add graphics to a response plan 3-12
Add Hazmats to a facility response plan 2-23
Add hydrant information to a response plan 3-13
Add mutual aid resources to a response plan. 3-11
Add new sound or voice files for assignment to tone sequences 11-14
Add notification organizations 4-13
Add perimeters to a response plan. 3-16
Add pre-recorded messages. 7-6
Add security information to personnel 2-96
Add the ACU-1000 RID for broadcast and live-voice sources 7-14
Add the BT-X Communicator unit 6-6
Age a PIN 9-40
Assign a new access card or PIN. 8-24
Assign a vehicle to a person 2-94
Assign a View Generator to a View Generator Repeater Display. 12-6
Assign automatic tone sequences to incident classes 11-15
Associate an action with a status change. 3-37

C

Change alert sounds. 3-57
Change an ACS unit assignment for a card or PIN 8-27
Change the color of alerts 3-55
Change the color of special status alerts 3-56
Configure alternate E-911 systems over IP 10-6
Configure Firehouse options 4-10
Configure global Tone Generator settings. 11-2
Configure live-voice sources at a workstation. 7-17
Configure the Alert Manager. 3-50
Configure within-building and wide-area mass notification 7-3
Configure workstation options 4-49
Copy a shift template. 4-44
Create a custom button 3-36
Create a Facility Access Report. 9-42
Create a law enforcement incident disposition list 4-17
Create a list of firing action types for law enforcement 4-22
Create a list of law enforcement incident sources 4-18
Create a list of law enforcement mutual aid 4-20
Create a list of law enforcement notifications 4-19
Create a message group 7-8
Create a Reminder action. 3-34
Create a remote command action 3-29
Create a remote unit group 2-62
Create a Run External Program action 3-32
Create a shift template 4-40

Create a Summary Statistics Log 4-47
Create a tone sequence for the Tone Alert Unit 11-11
Create a tone sequence for the Tone Generator 11-3
Create a tone sequence list for the Tone Alert Unit 11-13
Create a tone sequence list for the Tone Generator 11-5
Create an access group 8-5
Create an access schedule 8-6
Create an AutoMNS action 3-28
Create an output group (D-21) 2-79
Create an output group (D-21G or D-21M) 2-80
Create custom facility types and symbols 4-8
Create custom log entries 4-4
Create custom note types 4-5
Create custom personnel fields 4-24
Create custom Text-to-Speech entries for facilities 11-18
Create holiday types for access schedules 8-8
Create lists of weapon types for law enforcement 4-21
Create multiple fire districts for tracking incidents 4-12
Create roster duty types 4-43
Create secondary incident ID numbers 3-54
Customize perimeter types 4-9
Customize the "Site" label 4-7
Customize the D-21 Incident Client Daily Activity viewers 4-6

D

Deactivate an access card or PIN 8-28
Deactivate an assigned iButton (temporary) 9-37
Define content for the View Generator 12-4
Delete a facility from the map 2-120
Delete a hazardous material 2-106
Delete a hydrant 2-112
Delete a hydrant from the map 2-120
Delete a person record 2-92
Delete a remote unit 2-61
Delete a resource 2-105
Delete a RID 2-50
Delete a shift template 4-46
Delete a vehicle 2-103
Delete a zone 2-70
Delete an emergency card 3-23
Delete an operator 2-100
Delete an output 2-78
Delete Desk Journal entry types 4-15
Delete Desk Journal organizations 4-15
Determine if an iButton has been assigned to a user 9-40
Disable alerts from auxiliary zones 3-46
Disable alerts from relay outputs 3-47

Disable and enable unattended alarm alerts 3-52
Disable E-911 map warnings 3-51
Display the Alarm ID or Box Number on alerts 3-51
Display zone numbers in alert log entries 3-51
Download all pending IDS authentication records 9-43
Download IDS authentication records for a specific BT-X 9-44
Download recent changes to one or more existing ACS remote units 8-23
Download the entire unit configuration to a new ACS remote unit 8-22
Download the entire unit configuration to an existing ACS remote unit 8-22

E

Edit a custom button 3-37
Edit a custom perimeter type 4-9
Edit a facility 2-26
Edit a facility Hazmat 2-25
Edit a HazMat 2-107
Edit a holiday 4-11
Edit a hydrant 2-112
Edit a message group 7-10
Edit a Permit Type 4-32
Edit a person record 2-92
Edit a phone number in the E-911 database 10-10
Edit a pre-plan template 3-24
Edit a reader 8-19
Edit a remote unit 2-61
Edit a remote unit group 2-63
Edit a resource 2-105
Edit a shift template 4-44
Edit a site 2-3
Edit a zone 2-70
Edit an access schedule 8-9
Edit an emergency card 3-22
Edit an emergency card HazMat 3-21
Edit an IDS user authentication 9-34
Edit an operator 2-100
Edit an output 2-77
Edit an output group (D-21G or D-21M) 2-84
Edit an SOP 3-38
Enable automatic acknowledgement of alerts 3-48
Enable automatic shortest routes 4-34
Enable mass notification for the RFM 7000 RID 7-5
Enable or disable a RID, unit, zone, or output 2-51
Enable or disable a unit watch 9-47
Enable PACAF incident codes 3-64
Enroll the IDS primary administrator 9-25
Enter a single quotation mark or apostrophe 1-11
Enter address abbreviations 4-3

Enter time zone information 2-4

I

Import floor plans 5-8
Import pre-plans 5-10
Import response graphics 5-5

L

Launch the D-21 Admin Client 1-2

M

Make a floor plan graphic available to the D-21 system 5-3
Make a pre-plan file available to the D-21 system 5-4
Make a response plan graphic available to the D-21 system 5-3
Make a wave file available to the D-21 system 5-12
Make an icon available to the D-21 system 5-12
Make your computer accessible to a Monaco product support specialist 13-2
Modify a Permit drop-down list 4-30
Modify a Work Order drop-down list 4-27

N

Name media files for floor plans and graphics 5-4

P

Place a single facility or hydrant on the map 2-119
Place multiple facilities on the map 2-113
Place multiple hydrants on the map 2-116
Populate a Permit drop-down list 4-28
Populate a Work Order drop-down list 4-25
Pre-configure a live-voice message 7-27
Pre-configure a pre-recorded message 7-25
Print a card inventory report 8-33
Print a facility's E-911 phone numbers 10-10

Q

Quit the D-21 Admin Client 1-5

R

Re-activate an assigned iButton 9-38
Reassign an inactive card 8-29
Record a card lost or stolen and deactivate it 8-32
Record a card lost or stolen and track it 8-32
Reload all RIDs 2-50
Remove a custom button 3-36
Remove a custom perimeter type 4-10
Remove a custom SOP 3-43
Remove a facility Hazmat 2-26
Remove a holiday 4-11
Remove a message group 7-10
Remove a Permit Type 4-32

Remove a remote unit group 2-63
Remove a response plan perimeter 3-19
Remove an access card 8-27
Remove an access group 8-5
Remove an access schedule 8-10
Remove an action 3-35
Remove an emergency card HazMat 3-22
Remove an IDS user authentication 9-36
Remove an item from a personnel list 4-23
Remove an output group 2-84
Rename an action 3-35
Reset the incident editing control in the D-21 Incident Client 3-58
Resound trouble alerts at regular intervals 3-51

S

Schedule holidays 4-11
Set a default map location for incidents without map coordinates 4-36
Set hydrant colors based on flow rate 4-37
Set the color for closed roads 4-35
Set up AutoMNS 7-29
Set up cameras for the Camera Viewer 12-2
Set up timeouts for mass notification 7-4
Start the multi-server D-21 Admin Client 1-3
Suppress duplicate trouble and normal alerts 3-49
Switch from one server to another on a multi-server client workstation 1-4

T

Track all cards presented at an existing reader 8-30
Track one card at all readers 8-31
Transfer an iButton assignment from one user to another 9-39

U

Unassign a vehicle to a person 2-95

V

View ACS remote units that have changes to be downloaded 8-21
View facilities with response plans attached 3-19
View IDS download results and retry an unsuccessful download 9-46
View point properties 2-71
View remote units with dual communication enabled 6-10
View the users with access to a Master Zone 9-41

Section 1
Starting, Quitting, and Navigating

Read this section to learn how to start, quit, and navigate within the D-21 Admin Client.

Contents

Starting and Quitting the D-21 Admin Client 1-2
- Starting the Single-Server D-21 Admin Client 1-2
- Starting a Multi-Server D-21 Admin Client 1-3

Navigating the D-21 Admin Client 1-7
- Navigating the Tree Pane 1-7
- Menus 1-8
- Dialog Boxes 1-11

Starting and Quitting the D-21 Admin Client

The D-21 Server launches as soon as you start the server computer. You must double-click the D-21 Admin icon to launch the D-21 Admin Client.

Starting the Single-Server D-21 Admin Client

The single-server configuration is the most common D-21 configuration. Each D-21 Admin Client connects to the same server with one D-21 database containing all site, personnel, and hardware device information.

If you are running the D-21 Admin Client on a computer other than the server computer, the server computer must also be running.

To launch the D-21 Admin Client

1. If the computer is not already on, turn it on by pressing the power switch. For more information on the D-21 hardware, see the D-21 Hardware I-O-M Manual (P/N 001-391-00).
2. When prompted to do so, enter your Windows 2000/XP login. If you do not know your login, contact the system administrator.
3. On the desktop, double-click the D-21 Admin icon.

The D-21 Admin Client launches and the Operator Login dialog box appears.

4. Select your name from the Operator on Duty drop-down list.

   The Admin operator login is always available, and the Monaco representative who set up your D-21 system notified the administrator of the Admin operator password. Additional operator names were added by the Monaco representative who set up the system, or by the administrator. If your name is not in the Operator on Duty list, contact the system administrator.
5. Enter the case-sensitive password and click **Login**.

NOTE *An operator can be logged in to one instance of the D-21 Admin Client and one instance of the D-21 Incident Client at the same time. An operator cannot log in to more than one instance of either the D-21 Admin Client or the D-21 Incident Client at the same time.*

Starting a Multi-Server D-21 Admin Client

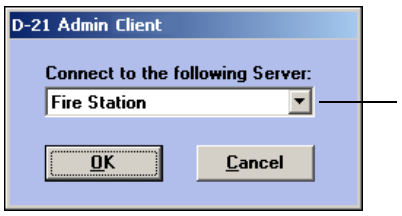
When the Multi-Server Client option is enabled, the D-21 Admin Client can log into any available D-21 server. Each server has its own D-21 database with its own site, personnel, and hardware information. It is only possible to log into one server at a time, and the operator must have the correct privileges to gain access to each server database.

For information on switching from one server to another, see "To switch from one server to another on a multi-server client workstation" on page 1-4.

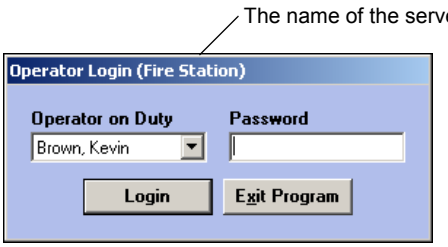
To start the multi-server D-21 Admin Client

1. If the computer is not already running, turn it on by pressing the power switch. For more information on the D-21 hardware, see the D-21 Hardware I-O-M Manual (P/N 001-391-00).
2. When prompted, enter your Windows 2000/XP login. If you do not know your login, contact your system administrator.
3. On the desktop, double-click the D-21 Admin icon.

4. In the Select Server dialog box, select the name of the server you want.



5. Click **OK**. The Operator Login dialog box for the selected server's database appears.



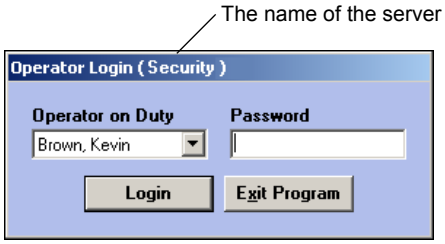
6. Select your name from the Operator on Duty drop-down list.
7. Type your case-sensitive password in the Password box.
8. Click **Login**. The D-21 Admin Client window appears populated with data from the D-21 database on the selected server.

To switch from one server to another on a multi-server client workstation

1 Select **File > Change Server**.

2 Select a different server in the drop-down list.

3 Click **OK**. The Operator Login dialog box for the selected server's database appears.



4 Select your name from the Operator on Duty drop-down list.

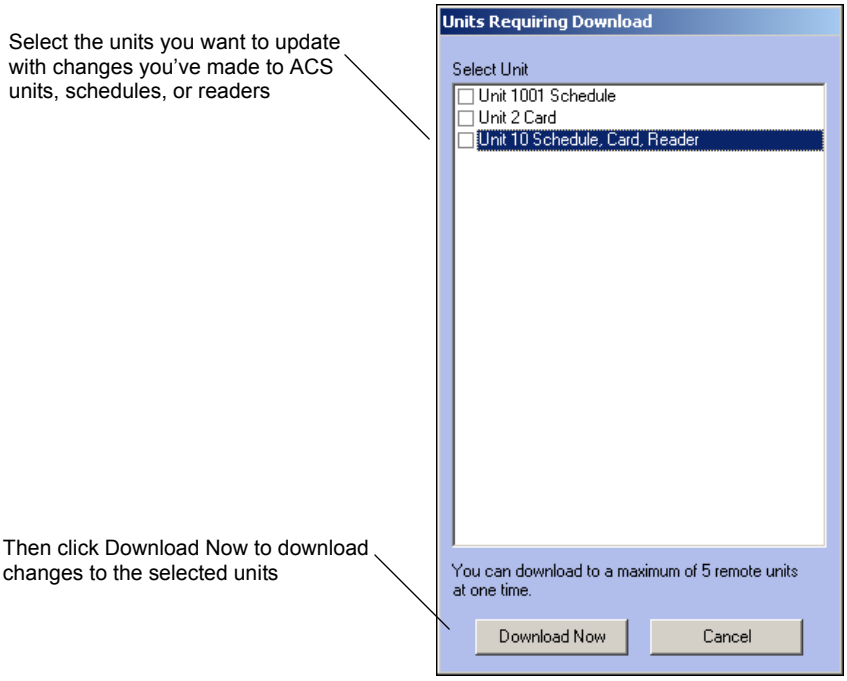
5 Type your case-sensitive password in the Password box.

6 Click **Login**. The D-21 Admin Client window appears populated with data from the D-21 database on the selected server.

To quit the D-21 Admin Client

1 Click ✕ at the top right of the D-21 Admin Client window.

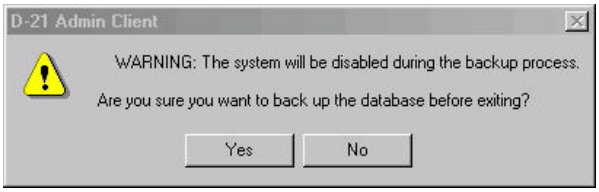
NOTE *If you have access control (ACS) enabled on your D-21 system, the following message appears. See "Downloading Settings to Access Control Units" on page 8-20 for more information.*



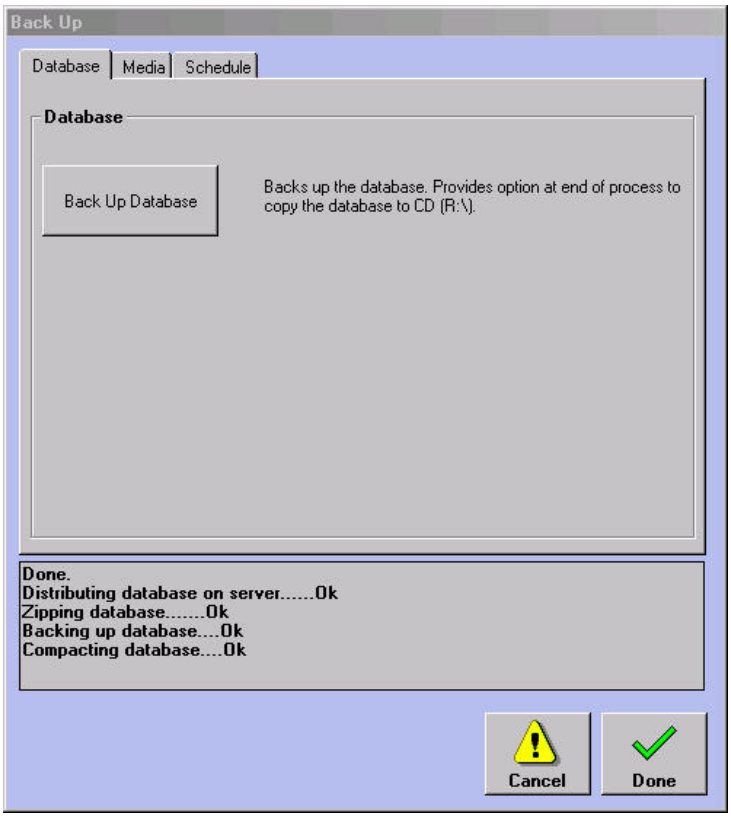
2 A message appears, asking whether you want to back up the database.

3 Click the desired button:

- **Cancel** Click **Cancel** to return to the D-21 Admin Client.
- **No** Click **No** to quit the program without backing up the database.
- **Yes** Click **Yes** to back up the database before quitting the program. If you click **Yes**, you are prompted to confirm your choice and told that the system is disabled during the backup process.



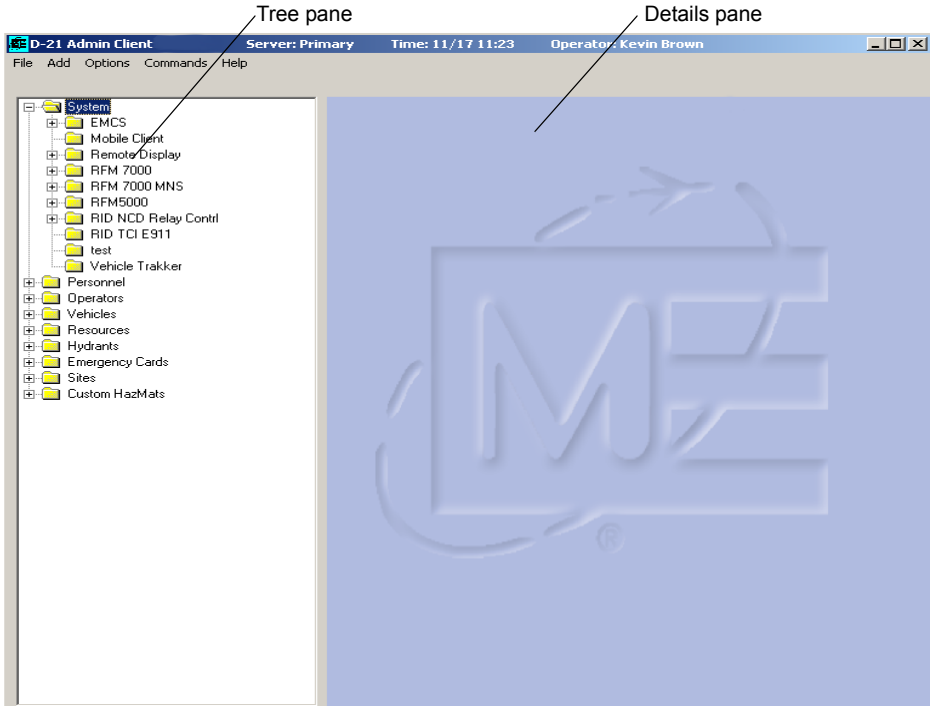
After you click **Yes**, the D-21 Admin Client displays the Backup dialog box. See "Backing up the database" in the D-21 Maintenance Manual (P/N 001-399-02) for a full discussion of backup commands and options.



4 When the backup process is complete, click **Done**. The Admin Client program closes.

Navigating the D-21 Admin Client

The main, rectangular area in which D-21 Admin Client elements are displayed is called a 'window'. The Admin Client window consists of two panes: the tree pane (left side) and the details pane (right side, blank in the illustration below). The details pane displays data associated with the selection in the tree pane.

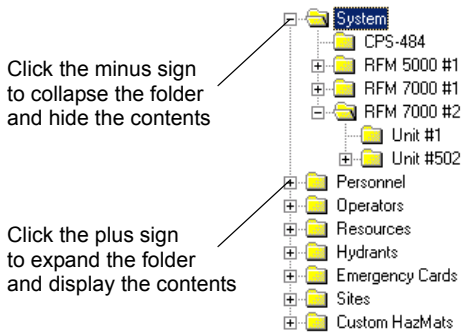


Navigating the Tree Pane

Expanding and Collapsing Folders

Click the plus sign (+) to the left of a folder to expand it and display the contents. Click the minus sign (-) to the left of a folder to collapse it and hide the contents.

Figure 1-1 *Expanding and collapsing folders*



Opening Edit dialog boxes from the Tree Pane

You can open the edit dialog box for most database entries by right-clicking the associated icon in the tree pane.

Menus

Select D-21 menu items just as you select menu items in other Windows programs. The D-21 Admin Client provides the menus described in the table below.

NOTE *Some menu items may not be available, depending on the D-21 options installed*

Menu	Menu Item	Use to...
File	Import	Import files for response graphics, floor plans, and maps. See "Adding Media Files" on page 5-1.
	Export	Export D-21 data for use with Monaco D-700R Programmer software or third-party Firehouse software. See the D-21 Maintenance Guide (P/N 001-399-02).
	Archive	Archiving should only be done at the request of a Monaco Representative. See the D-21 Maintenance Guide (P/N 001-399-02).
	Backup	Backup the database or media files. See the D-21 Maintenance Guide (P/N 001-399-02).
	Restore	Allows the restoration of media files. See the D-21 Maintenance Guide (P/N 001-399-02).
	Compact	Compact the database. See the D-21 Maintenance Guide (P/N 001-399-02).
	Exit	Exit the D-21 Admin Client. See "Starting and Quitting the D-21 Admin Client" on page 1-2.

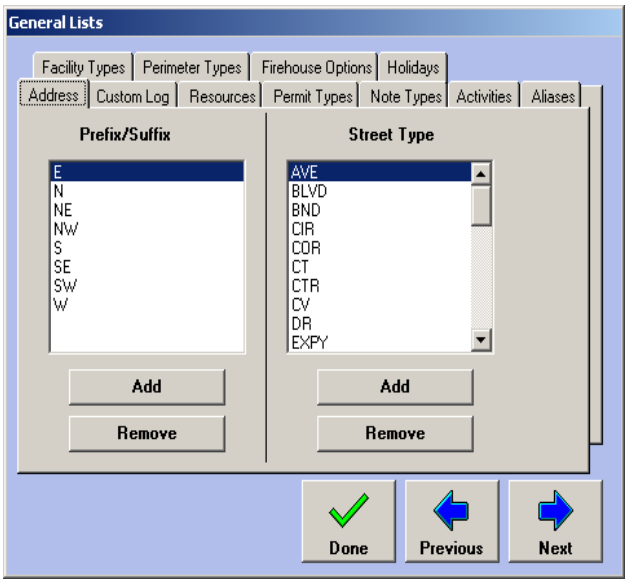
Menu	Menu Item	Use to...
Add	RID	Add a remote interface driver. See “Remote Interface Drivers (RIDs)” on page 2-30.
	Remote Unit	Add a remote unit. See “Remote Units” on page 2-51.
	Zone	Add a zone. See “Zones” on page 2-64.
	Output	Add an output. See “Outputs” on page 2-74.
	E911 Phone Listing	Add an E911 phone listing to the D-21 database. See “Configuring an E-911 System” on page 10-2.
	Person	Add personnel. See “Personnel” on page 2-85.
	Operator	Add an operator. See “Operators” on page 2-97.
	Vehicle	Add a vehicle. See “Vehicles” on page 2-101.
	Resource	Add a resource such as a fire truck, chief, or pump. See “Resources” on page 2-103.
	HazMat	Add a custom hazardous material. See “HazMats” on page 2-106.
	Hydrant	Add a hydrant. See “Hydrants” on page 2-109.
	Emergency Card	Add a response plan for a topic. See “Emergency Cards” on page 3-20.
	Site	Add a site. See “Sites” on page 2-3.
	Facility	Add a facility. See “Facilities” on page 2-13.
Options	Actions	Define actions. See “Using Actions” on page 3-27.
Options	Access Control	Configure an access control system. See “Overview of Access Control” on page 8-2.
	Dispatch Config	Select a dispatch mode and create incident types and resource groups. See “Dispatch Configuration” on page 3-58.
	Groups	Create a remote unit group or output group. See “Creating Remote Unit Groups” on page 2-62 and “Creating Output Groups” on page 2-78.
	Edit HazMats	Edit a custom hazardous material or the trade name of a standard hazardous material. See “Editing HazMats” on page 2-107.
	Fire Lists	Create or edit lists used with fire incidents. See “Fire Lists” on page 4-12.
	General Lists	Create or edit the data that appears in drop-down lists for addresses, log entries, resource classes, permit types, and notes. See “General Lists” on page 4-2.
	Hydrant Color	Assign colors to hydrant icons to signify flow rate. See “Setting Hydrant Colors” on page 4-37.
	IDS Central Enrollment	Manage authentications for BT-X Keypads and BT-X iButton Keypads. See “IDS iButton and PIN Assignments” on page 9-24.
	Incident Processing	Set preferences for how incidents are handled. See “Incident Processing” on page 3-41.
	Map Object Settings	Set default values for certain Map Options. See “Setting Map Options (D-21 M)” on page 4-33.
	MNS Settings	Set up a mass notification system. See “Configuring Mass Notification” on page 7-1.
	Personnel Lists	Create or edit the data that appears on rosters and call groups. Define field labels for the custom fields in personnel. See “Personnel Lists” on page 4-23.

Menu	Menu Item	Use to...
	Permit/Work Order Lists	Populate drop-down lists used when managing permits and work orders. See “Permit/Work Order Lists” on page 4-25.
	Pre-Plans	Add, edit, and remove pre-plan templates. See “Pre-Plans” on page 3-23.
	Roster	Create or edit roster shifts and duties. See “Creating Rosters” on page 4-38.
	Security Lists	Create or edit lists for the Security Desk Journal and Law Enforcement. See “Security Lists” on page 4-14.
	SOPs	Edit standard operating procedure documents. See “Standard Operating Procedures (SOPs)” on page 3-38.
	Summary Statistics Log	Create a Daily Activities form to track statistics in the D-21 Incident Client. See “Creating a Summary Statistics Log” on page 4-46.
	Tone Options	Create tone sequences to be used with a Tone Generator Panel. See “Configuring Tone Alerting with a Tone Generator” on page 11-2.
	Workstation Options	Configure the D-21 workstation. See “Setting Workstation Options” on page 4-49.
Devices	Cameras	Configure cameras to be monitored in the D-21 Incident Client. See “Configuring the Camera Viewer” on page 12-2.
	Tone Alerting	Create tone sequences to be used with a Tone Alerting unit. See “Configuring Tone Alerting with a Tone Alert Unit” on page 11-6.
	View Generator	Configure the display for a View Generator unit. See “Configuring the View Generator” on page 12-2.
	View Generator Displays	Assign workstations to View Generator displays. See “Configuring the View Generator” on page 12-2.
Commands	Enable/Disable Commands	Enable or disable RIDs, remote units, zones, and outputs from the D-21 Admin Client. See “Enabling and Disabling RIDs, Units, Zones, and Outputs” on page 2-50.
	Reload All RIDs	Reload all remote interface drivers. See “Reload All RIDs” on page 2-50.
	Reset Edit Incident Control	Reset the control that allows only one operator at a time to edit an incident. See “Resetting Incident Editing Controls” on page 3-58.
	Access Control	Download access control unit configuration settings to ACS remote units. See “Downloading Settings to Access Control Units” on page 8-20.
	Override Redundant Data Changes	Used to reset replication flags when a primary server is brought back on line. Consult Monaco technical support before using this command.
Help	D-21 Library	Displays the D-21 Admin Client User’s Guide as a PDF file.
	Contact Monaco	Displays addresses and phone numbers for contacting Monaco Enterprises, Inc.
	About D-21 Admin	Display version and copyright information for the D-21 software.

Dialog Boxes

Many D-21 dialog boxes have multiple tabs. Navigate to a tab by clicking it or by using the **Previous** and **Next** buttons at the bottom of the dialog box. The button actions "loop" so that clicking **Next** when the right-most tab is in the foreground brings the left-most tab to the foreground, and clicking **Previous** when the left-most tab is in the foreground brings the right-most tab to the foreground.

Figure 1-2 *D-21 dialog box showing* **Previous** *and* **Next** *buttons*



Text Entries in Boxes

The generic single quotation mark or apostrophe character (') on the key to the left of the **Enter** key cannot be used in D-21 name boxes (person name, site name, facility name, and so on). It is possible to use an alternate character in their place.

To enter a single quotation mark or apostrophe

1. Click where you want the apostrophe to appear.
2. Make sure Num Lock is on. (The Num Lock LED is on the keyboard. If the LED isn't illuminated, press **Num Lock** on the number pad.)
3. Hold down **Alt** while using the number pad to type `0146`. The right single quotation mark appears.

Section 2
Creating the D-21 Database

Read this section to learn how to enter data into the D-21 database.

Contents

Order for Entering Data 2-2
Sites 2-3
Facilities 2-13
    Adding Floor Plans 2-27
Remote Interface Drivers (RIDs) 2-30
    Adding a RID for the RFM 5000 2-31
    Adding a RID for the RFM 7000 and RFM-X 2-38
    Reload All RIDs 2-50
    Enabling and Disabling RIDs, Units, Zones, and Outputs 2-50
Remote Units 2-51
    Unit Class 2-52
    Numbering Remote Units 2-54
    Creating Remote Unit Groups 2-62
Zones 2-64
    Zone Class 2-64
    Zone Priority 2-65
    Point Reporting Zones 2-71
Outputs 2-74
    Creating Output Groups 2-78
Personnel 2-85
    Standard Personnel Information 2-86
    Custom Personnel Information 2-93
Operators 2-97
Vehicles 2-101
Resources 2-103
HazMats 2-106
    Editing HazMats 2-107
Hydrants 2-109
Placing Items on the Map (D-21M) 2-112

Order for Entering Data

The D-21 database is relational, and therefore the data records are associated in complex ways. Because of this, it is important to enter data in the correct order. For instance, you must define a remote unit before you can create a zone, and you must define a person before you can create an operator.

Monaco recommends entering data in the following order:

1. Facilities
2. RIDs
3. Remote units
4. Zones, Outputs
5. Personnel
6. Operators
7. Vehicles, Resources, HazMats, Hydrants
8. Response Plans, Emergency Cards

This section contains instructions for setting up 1-7 above. Response Plans and Emergency Cards are covered in Section 3.

NOTE *Response plans can be created from within a facility or zone record, but may require prior set up of personnel or resources. When you create facilities and zones, leave the response plan set-up until after you have created everything else.*

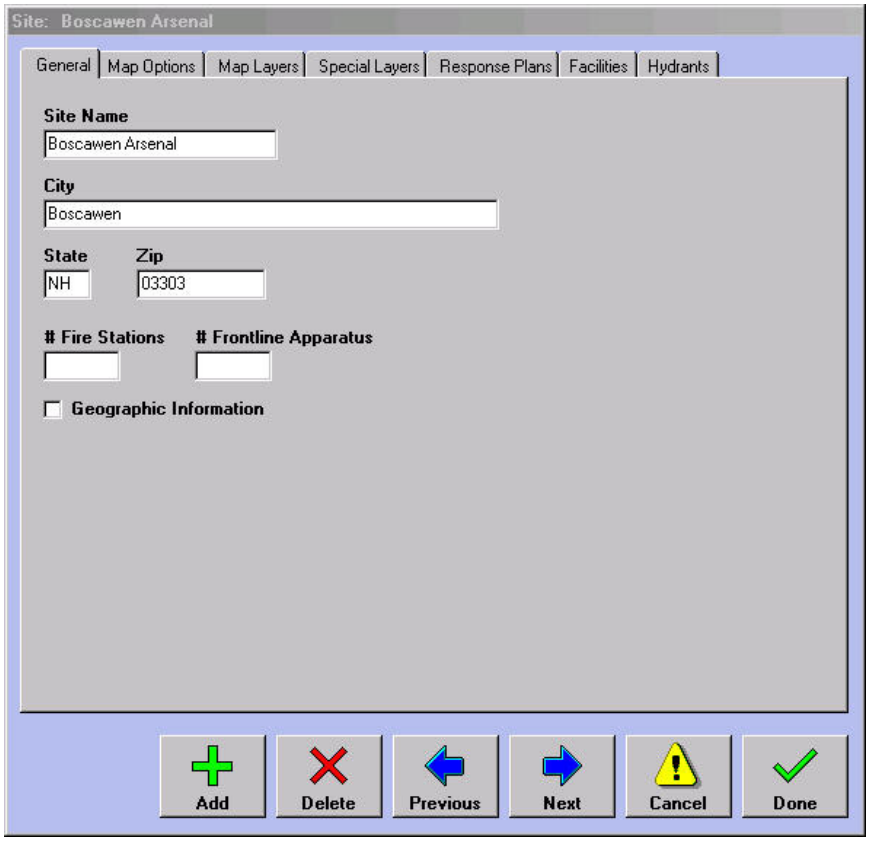
Sites

The first entity defined in a new D-21 database is a Site. If more than one site is necessary, use the Site command on the Add menu to add a site to the database.

IMPORTANT *Monaco configured your system to include all applicable sites. Consult Monaco before adding a site to the database.*

To edit a site

1 In the tree pane, click the [+] next to Sites to show all available sites. Right-click the name of the site you want to edit. The Site dialog box appears.



- **Site Name** The name of the site.

NOTE *If the name includes an apostrophe, see "To enter a single quotation mark or apostrophe" on page 1-11.*

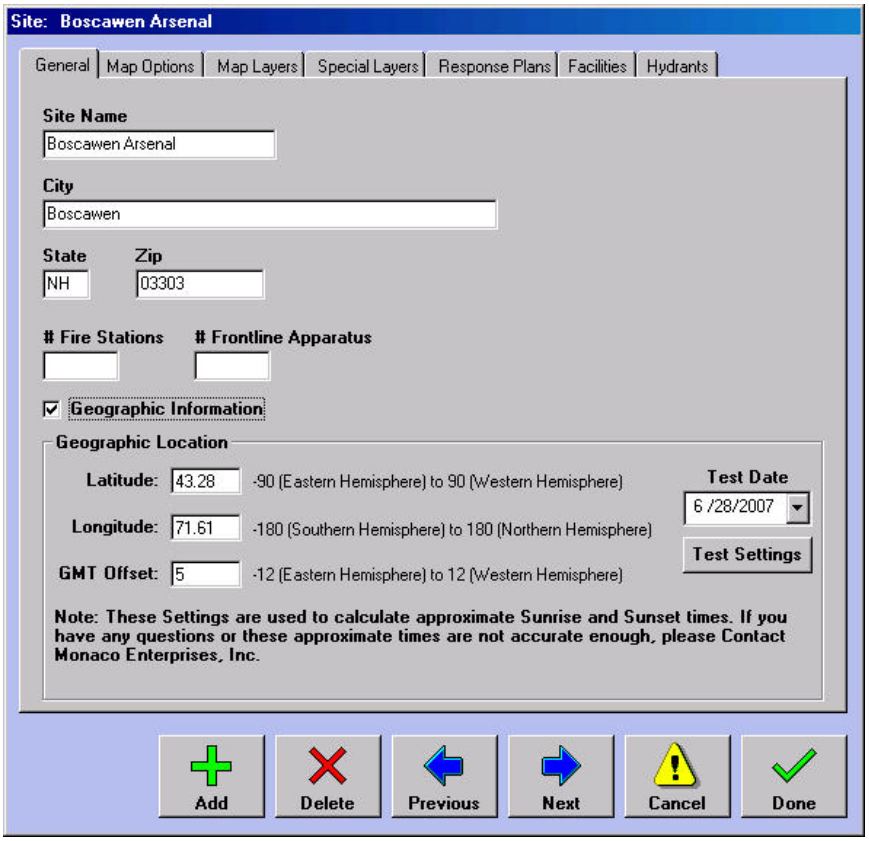
- **City/State/Zip** The city, state, and zip code of the site.
- **# Fire Stations** The number of fire stations that are located on the site.

- **# Frontline Apparatus** The number of frontline apparatus that operate on the site.

NOTE *The number of frontline apparatus is not automatically updated when you add or delete resources.*

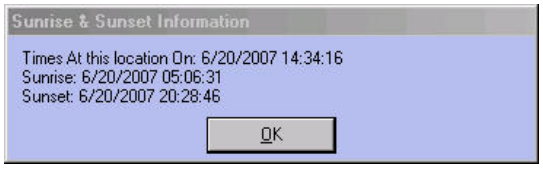
- **Geographic Information** Check this box if you wish to enter details about the geographic location of the site. These details allow the D-21 to calculate sunrise and sunset times at your location so that automatic actions can be scheduled at sunrise and sunset.

  When you check this box the General tab displays an additional area for data entry.

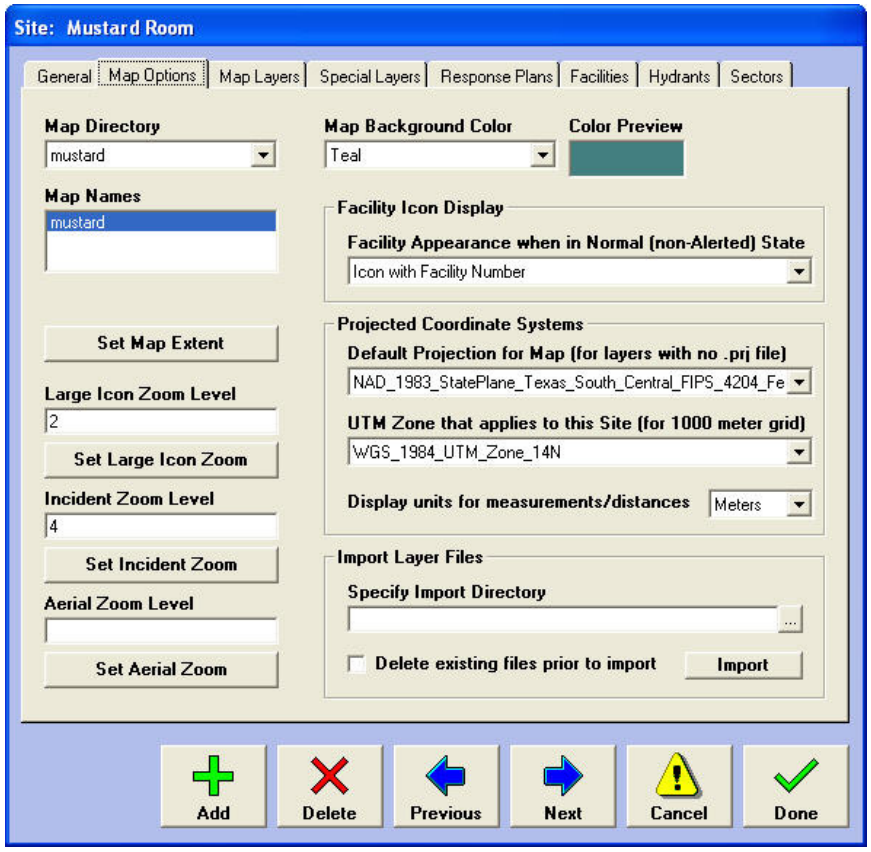


- **Latitude** Enter the latitude of your location.
- **Longitude** Enter the longitude of your location.
- **GMT Offset** Enter the difference between the time at your location and the Greenwich Mean Time.
- **Test Date** Select a date for which you want to check the calculated sunrise and sunset times at your location.

- **Test Settings** When you click this button, the Sunrise & Sunset Information dialog box opens allowing you to check the calculated sunrise and sunset times at your location for the test date selected.



2 Click **Next** to advance to the Map Options tab. (The Map Options tab is only available if you have the D-21M installed.)



- **Map Directory/Map Names** Select the map directory and map name.
- **Map Background Color** Select the map background color. The Color Preview window displays the selected background color.
- **Set Map Extent** Click **Set Map Extent** to automatically set the zoom level at which the map is initially displayed when it is opened in the D-21 Incident Client.
- **Large Icon Zoom Level** At smaller map magnifications, facility and hydrant icons are displayed as small dots. The number entered in this box determines the magnification above which the D-21 Incident Client displays the icons at their larger size. You may either enter the value in the text box or click **Set Large Icon Zoom** and zoom to the

magnification at which you want icons to appear in their larger size. For information on working in the dialog box that appears after you click **Set Large Icon Zoom**, see "Placing Items on the Map (D-21M)" on page 2-112.

NOTE *Type* `1` *in the Large Icon Zoom Level text box to display facility and hydrant icons at the same zoom level you specified for the Map Extent.*

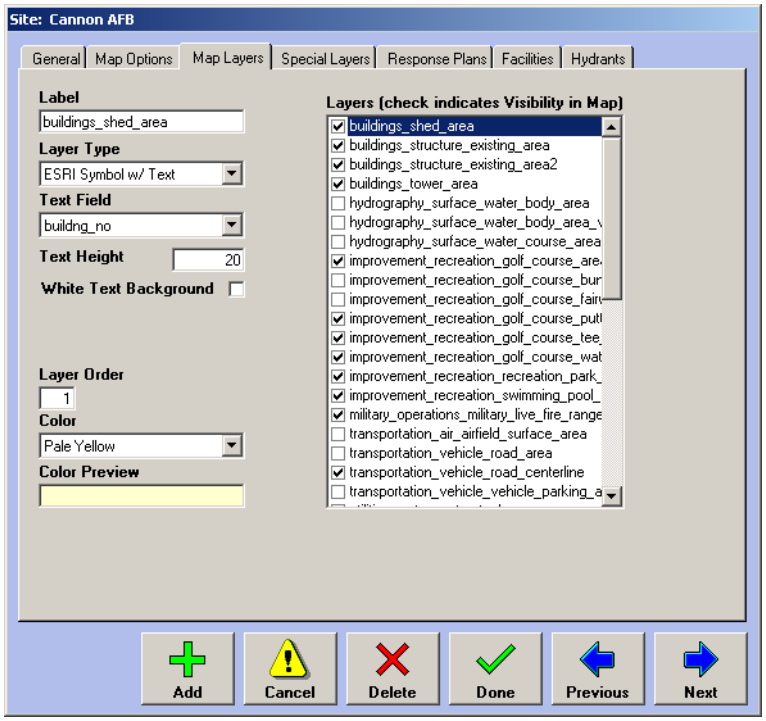
- **Incident Zoom Level** The default magnification at which the map appears when the D-21 Incident Client operator clicks Map View from within an incident. You can either enter the value in the text box or click **Set Incident Zoom** and zoom to the magnification at which you want maps to display by default in the D-21 Incident Client. For information on working in the dialog box that appears after you click **Set Incident Zoom**, see "Placing Items on the Map (D-21M)" on page 2-112.

NOTE *Type* `1` *in the Incident Icon Zoom Level text box to display incident icons at the same zoom level you specified for the Map Extent.*

- **Aerial Zoom Level** The magnification at which the aerial photograph, if there is one, appears as the background of the Map View. You can either enter the value in the text box or click **Set Aerial Zoom** and zoom to the magnification at which you want the aerial to display. For information on working in the dialog box that appears after you click **Set Aerial Zoom**, see "Placing Items on the Map (D-21M)" on page 2-112.
- **Facility Icon Display** Choose from the drop-down list to define how you want D-21 facilities to appear on the map when they are in a normal (non-alerted) state. The default is to display an icon with the facility number underneath.
- **Projected Coordinate Systems** These options are used to configure grid coordinates for the site map if the Grid Coordinates feature is installed on your system. Monaco has configured your map for grid coordinates before installing your D-21. Do not change these selections unless instructed to do so by a Monaco technical representative.
- **Display units for measurements/distances** Choose from the drop-down list to select either feet or meters as the unit of measurement for objects displayed on the map (perimeters, for example).
- **Import Map Layer Files** If you have added or removed any buildings or hydrants, specify the directory location for importing new site map layer files. To replace existing map layer files, click **Delete existing files prior to import**. Click **Import** to import new map layer files.

3 Click **Next** to advance to the Map Layers tab. (The Map Layers tab is only available if you have the D-21M installed.)

The layers of the map are stored in the map directory specified on the Map Options tab. Each layer of a map contains a different kind of information, such as buildings, roads, ditches. The Layer Type depends on how a specific layer was generated.



4 Select the map layer you want to manipulate. The D-21 auto-detects the layer type and displays it in the Layer Type drop-down list.

- **ESRI Symbol Only** ESRI shape (.shp) file with no text.
- **ESRI Symbol with Text** ESRI shape file populated with text that will appear on the map, such as building numbers or road names.
- **ESRI Raster Image** ESRI bitmap file, usually used for background photographs for site maps.
- **ESRI image Catalog** An image file from the ESRI catalog.
- **AutoCAD Text** ESRI text layer file that originated as an AutoCAD file.
- **AutoCAD Symbol with Text** ESRI shape file with text that originated as an AutoCAD file with text.

5 If the layer contains text, select the text field and specify a text height. Entering a text height number overrides the original height imported with the layer file.

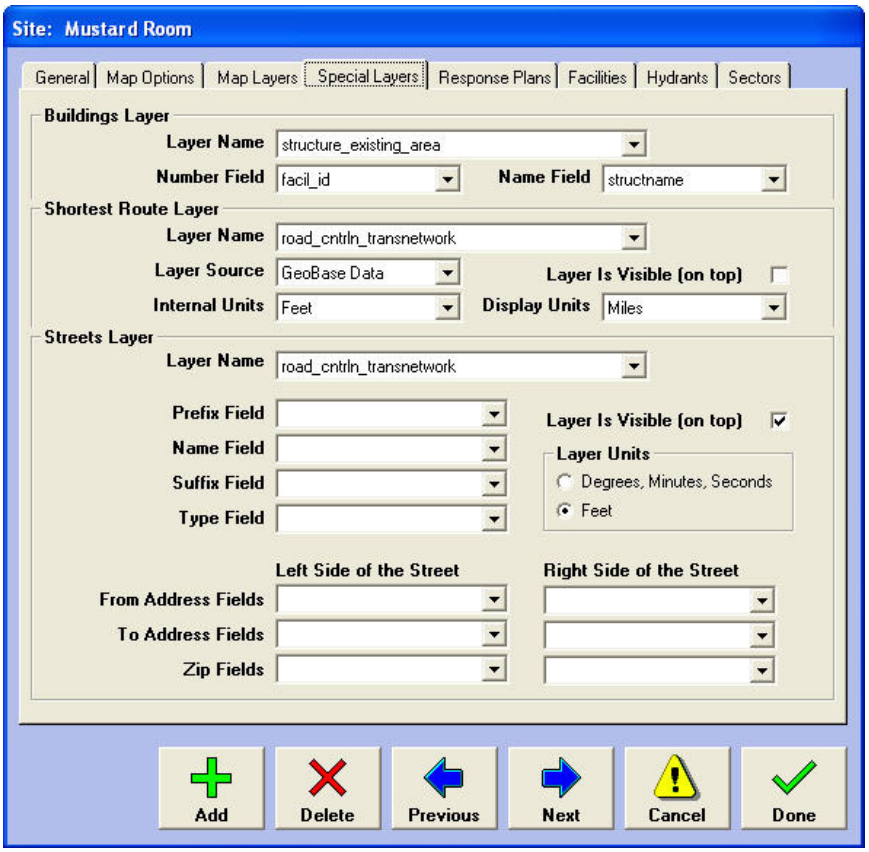
6 The Layer Order box allows you to specify the order in which each layer is drawn. The lower the number, the closer to the top the layer. So Layer 1 is drawn on top of all other layers, Layer 2 is drawn beneath layer 1 but on top of all other layers, etc.

7 Pick the color for the selected layer in the Color drop-down list.

NOTE *You cannot pick a color for ESRI Raster Images.*

8 Check the box next to the layer name in the Layers list if you usually want the layer to be displayed when you view the map.

9 Click **Next** to advance to the Special Layers tab. (The Special Layers tab is only available if you have the D-21M installed.)



The **Special Layers** tab allows the Administrator to configure the Building, Shortest Route, and Streets mapping layers in the D-21 map.

Buildings Layer Defines the layer that identifies building locations on the site.

- **Layer Name** Specifies the layer that contains the building objects.
- **Number Field** Specifies the field that contains the building numbers.
- **Name Field** Specifies the field that contains the building names.

Shortest Route Layer Defines the layer that identifies roads to be used by the Shortest Route and Road Closed/Open features.

NOTE *The Shortest Route Layer section is only available when Shortest Route option is enabled on the D-21 Server.*

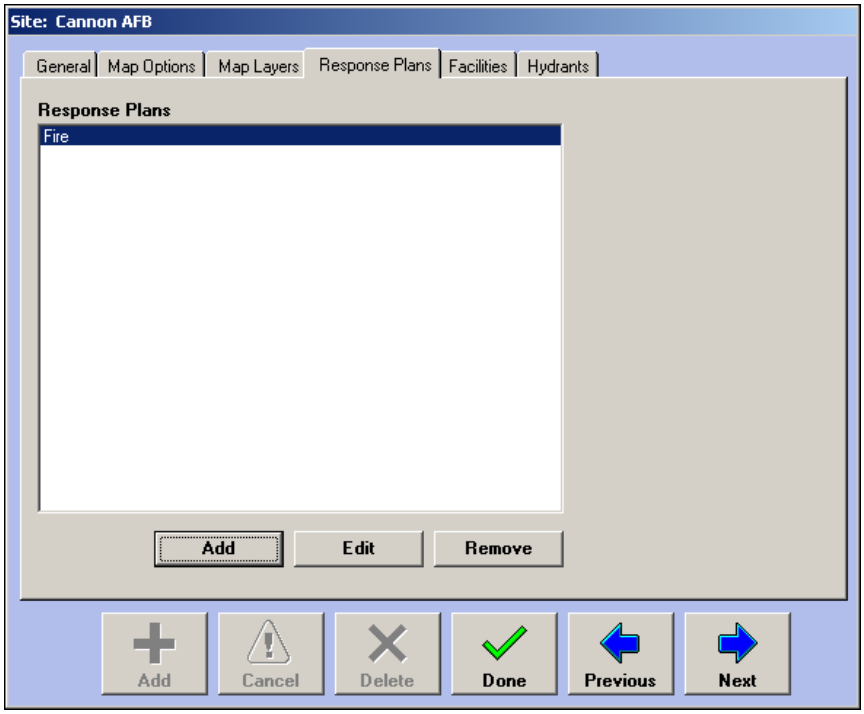
- **Layer Name** Specifies the layer that contains road lines.
- **Layer Source** Specifies the application source for the road line data.
- **Layer Is Visible (on top)** Unchecking this option hides the Shortest Route layer by placing it beneath the background image layer. Do this when a more visually appealing street layer is available.
- **Internal Units** Specifies the measurement units used internally by the Shortest Route layer. Consult Monaco technical support before changing this setting.
- **Display Units** Select from the drop-down list to choose the units of measurement in which shortest route directions should be given.

Street Layer Specifies the map layer that stores the street address data. The type of street address layer determines which fields are required in the Street Field Mappings area. For example, a street address layer that originates from TIGER/Line® data uses the mappings indicated in the graphic above, but a street layer from another mapping service may use different fields and field names. The Street Layer section is used to configure the address and cross street information for incidents on the map. When an incident occurs that is not associated with a facility in the D-21 database, the incident can be placed on the map using street address or street name.

NOTE *Some elements of the Street Layer section are only available when Auto Addressing is enabled on the D-21 Server.*

- **Layer Name** Specifies the name of the layer to be used by the D-21 for the street layer.
- **Prefix Field** Specifies the field in the street layer data that contains the directional prefix (N., N.E., N.W., etc.) for the address.
- **Name Field** Specifies the field in the street layer data that contains the street name.
- **Suffix Field** Specifies the field in the street layer data that contains the directional suffix (S., S.E., S.W., etc.) for the address.
- **Type Field** Specifies the field in the street layer data that contains the street type.
- **Layer is Visible (on top)** Unchecking this option hides the street address layer by placing it beneath the background image layer. Do this when a more visually appealing street layer is available.
- **Layer Units** Specifies the units of measurement used by the street address layer.
- **Left Side of the Street/Right Side of the Street** The **From Address** and **To Address** fields contain values that specify the distribution of odd and even numbered addresses. The **Zip** fields are used to specify the zip code on either side of a street.

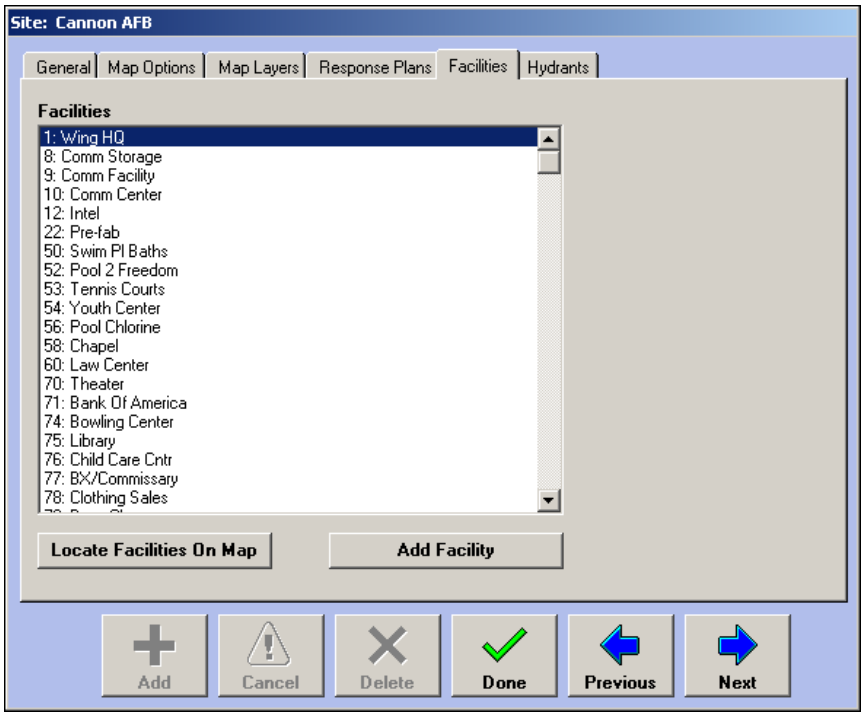
10 Click **Next** to advance to the Response Plans tab.



11 If you want to add a response plan for the entire site, click **Add** and choose a class (Aircraft, Fire, Security, EMS, etc.) from the drop-down list. Then click **OK** to begin creating the response plan. For more information on creating and editing response plans, see "Response Plans" on page 3-2.

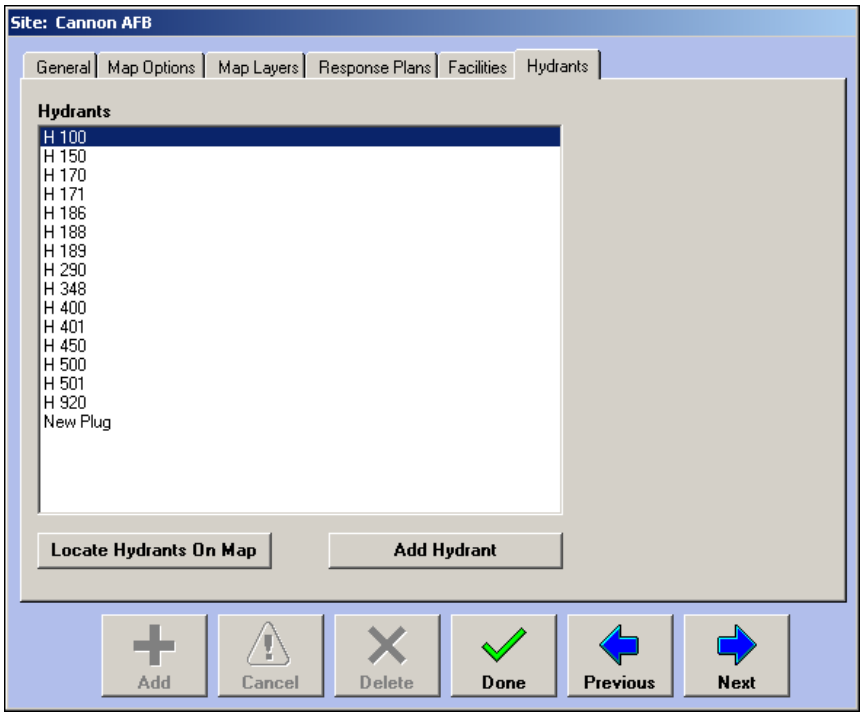
If you want to edit a response plan, select it and click **Edit**. To delete a response plan, select it and click **Remove**; then click **Yes** to confirm that you want to delete the plan.

12 Click **Next** to advance to the Facilities tab.



- **Add Facility** Displays the Add Facility dialog box. For information on adding a facility, see "Facilities" on page 2-13.
- **Locate Facilities On Map** Displays the Locate Facilities On Map dialog box. Use this dialog box to place multiple facilities on the site map. See "To place multiple facilities on the map" on page 2-113.

13 Click **Next** to advance to the Hydrants tab.



- **Add Hydrant** Displays the Add Hydrant dialog box. For information on adding a hydrant, see "Hydrants" on page 2-109.
- **Locate Hydrants On Map** Displays the Locate Hydrants On Map dialog box. Use this dialog box to place multiple hydrants on the site map. See "To place multiple facilities on the map" on page 2-113.

14 When you are finished adding the site, click **Done**.

Facilities

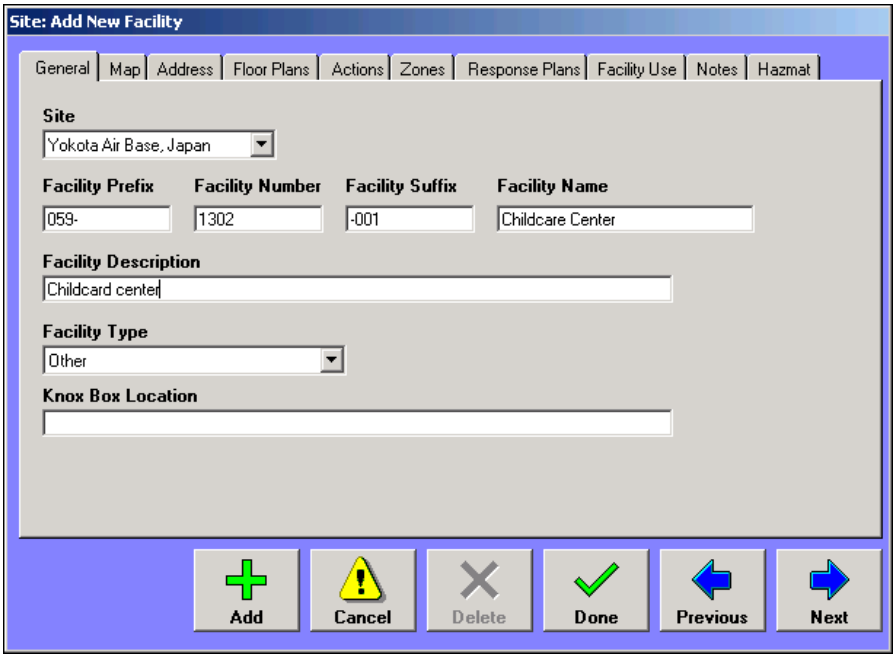
Any protected building or location that is reporting its status to the D-21 should be entered into the D-21 database.

Before you begin

Enter any custom directional prefixes and suffixes as well as street labels in the Address tab in the General Lists dialog box to make them available as you add facilities. See "Customizing Lists" on page 4-2.

To add a facility

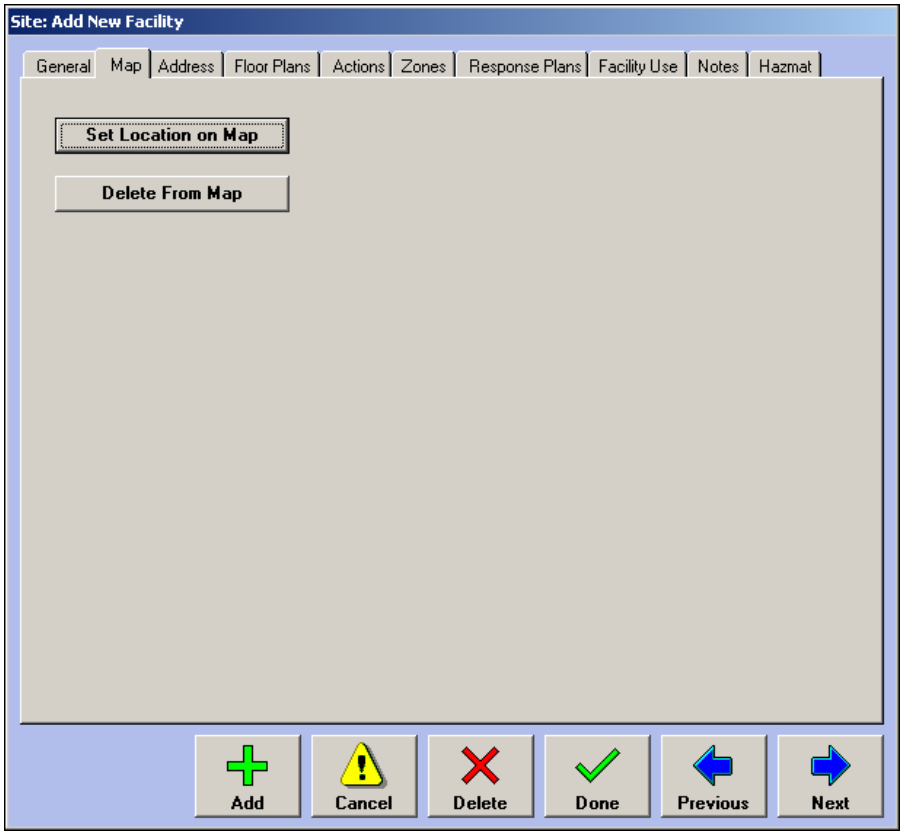
1. Select **Add > Facility**.
2. If the appropriate site name does not already appear in the Site box, select it from the drop-down list.
3. Enter a facility prefix, number, suffix, and name. Throughout the D-21 system the facility is identified by this prefix, number, and suffix followed by a colon and the name.



The facility prefix and suffix can be either text or numeric. The facility number must be a numeric entry. The D-21 Incident Client would designate the facility in the above graphic as: **059-1302-001: Childcare Center**.

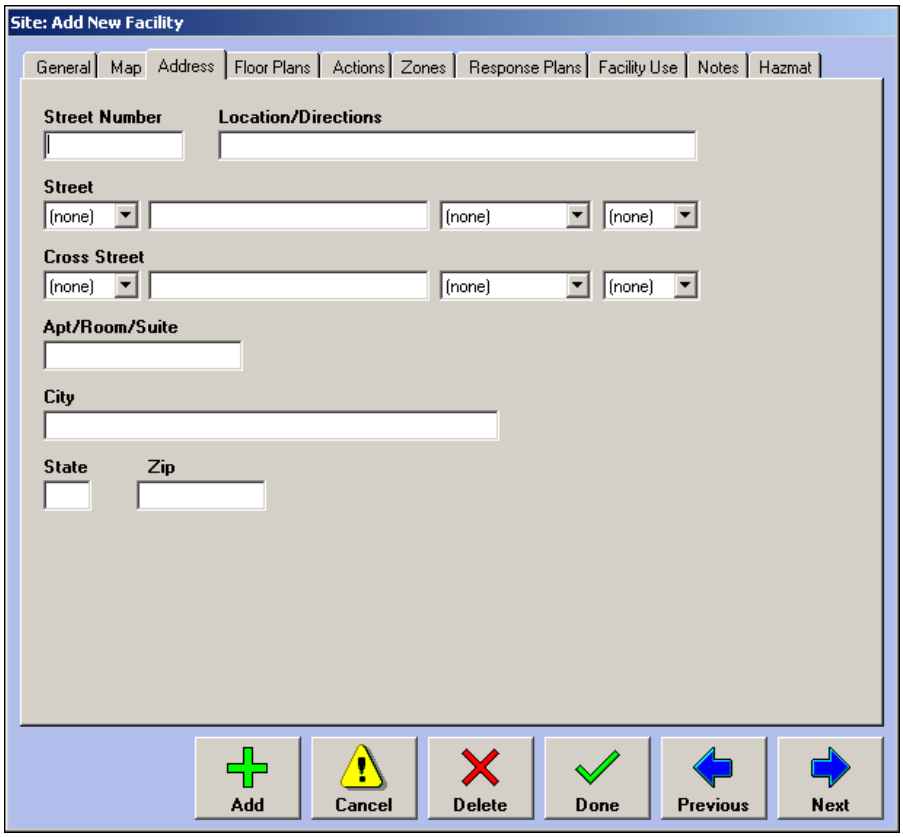
4. Enter a description of the facility.
5. Select the facility type from the drop-down list. The facility type is used to generate icons and labels for facilities that are placed on the map.
6. If the facility has an armored key box, enter its location in the **Knox Box Location** box.

7 Click **Next** to advance to the Map tab. (This tab appears only in the D-21M.)



8 If you want to add the facility to the site map, click **Set Location on Map.** (If the facility is incorrectly placed on the site map, click **Delete From Map** first.) For information on using the Select Map Location dialog box, see "Placing Items on the Map (D-21M)" on page 2-112.

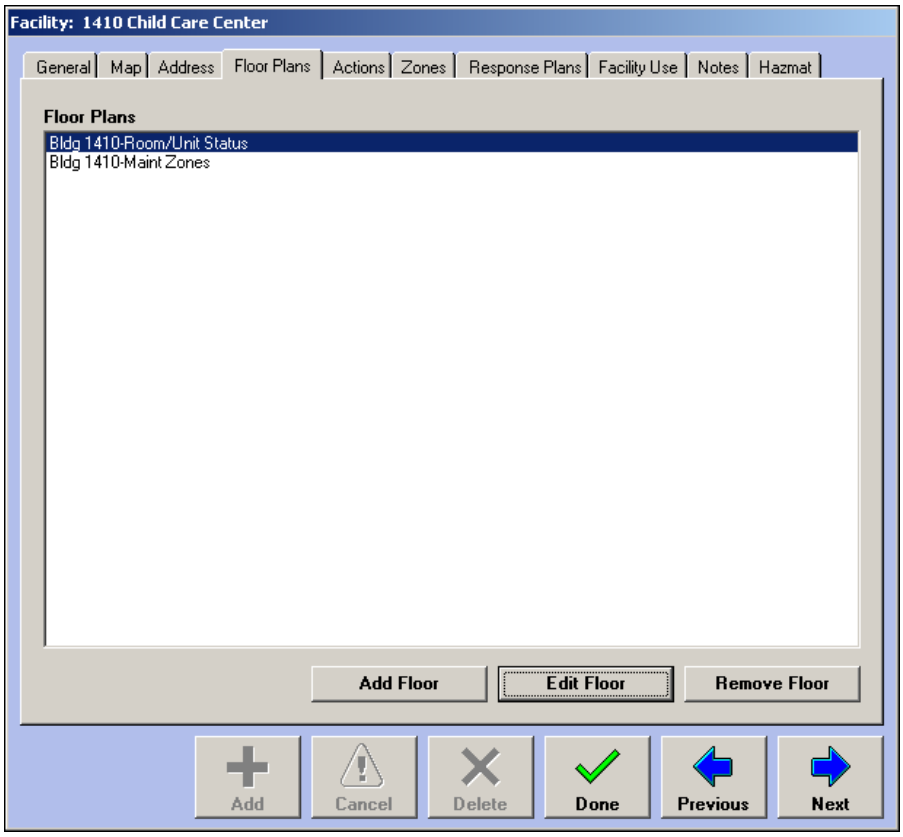
9 Click **Next** to advance to the Address tab.



10 Enter the address, choosing the directional prefix/suffix (N, NW, etc.) and street types (Ave, St, etc.) from the drop-down lists.

NOTE *You can add to, delete from, and edit the items that appear in the directional prefix/suffix list and street types list via the Address tab of the Lists dialog box. See* *"Customizing Lists" on page 4-2*.

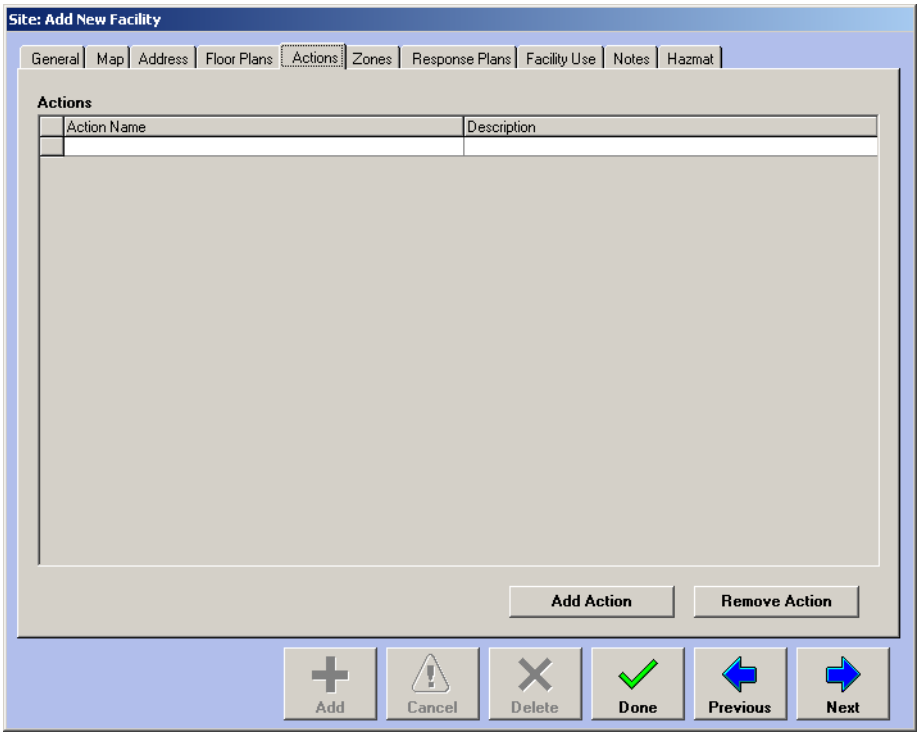
11 Click **Next** to advance to the Floor Plans tab.



12 Associate a floor plan with the new facility. For more information on adding floor plans, see "To add a floor plan to a facility" on page 2-27.

IMPORTANT *When you add a floor plan, you can attach labels to it that identify the location of remote units, outputs, and zones for the facility. However, since facilities are defined before their associated remote units and zones, you cannot add these floor plan labels until after both the facility and the units have been created.*

13 Click **Next** to advance to the Actions tab.

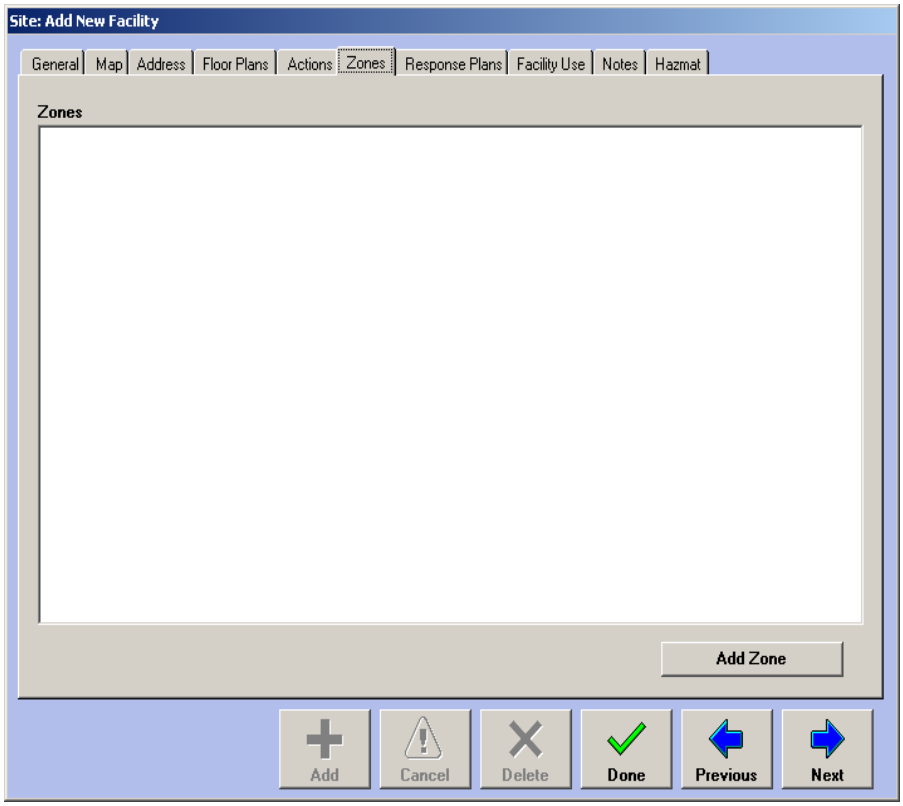


14 If you want to add an action to this facility, click **Add Action**, select the desired action from the dialog box that appears, and click **OK**.

NOTE *You must first create an action using* **Options > Actions** *before the action is available in this dialog box.*

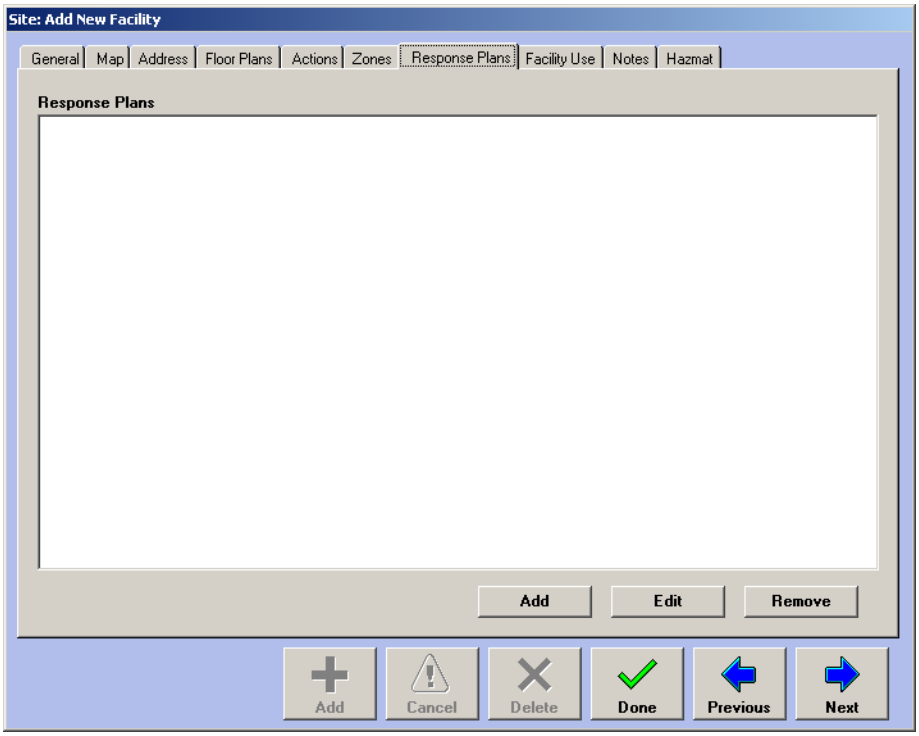
Actions associated with facilities appear under **Run Actions** on the pop-up menu that appears when the operator right-clicks a facility in the D-21 Incident Client. They also appear in the Actions viewer for an incident located at that facility. See "Using Actions" on page 3-27 and "Attaching Actions to Status Changes" on page 3-37 for more information on creating and using actions.

15 Click **Next** to advance to the Zones tab.



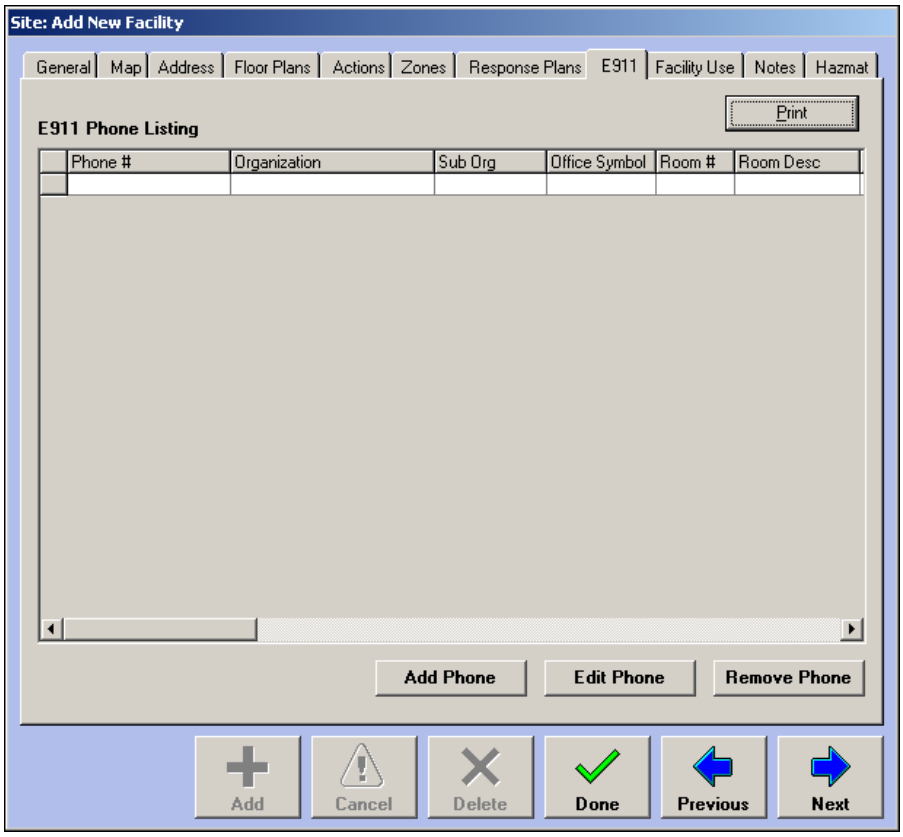
16 If you want to add a zone now, click **Add Zone.** Before a zone can be added, the unit and RID through which it is monitored must be defined in the D-21 database. For information on using the Add New Zone dialog box, see "To add a zone" on page 2-65.

17 Click **Next** to advance to the Response Plans tab.



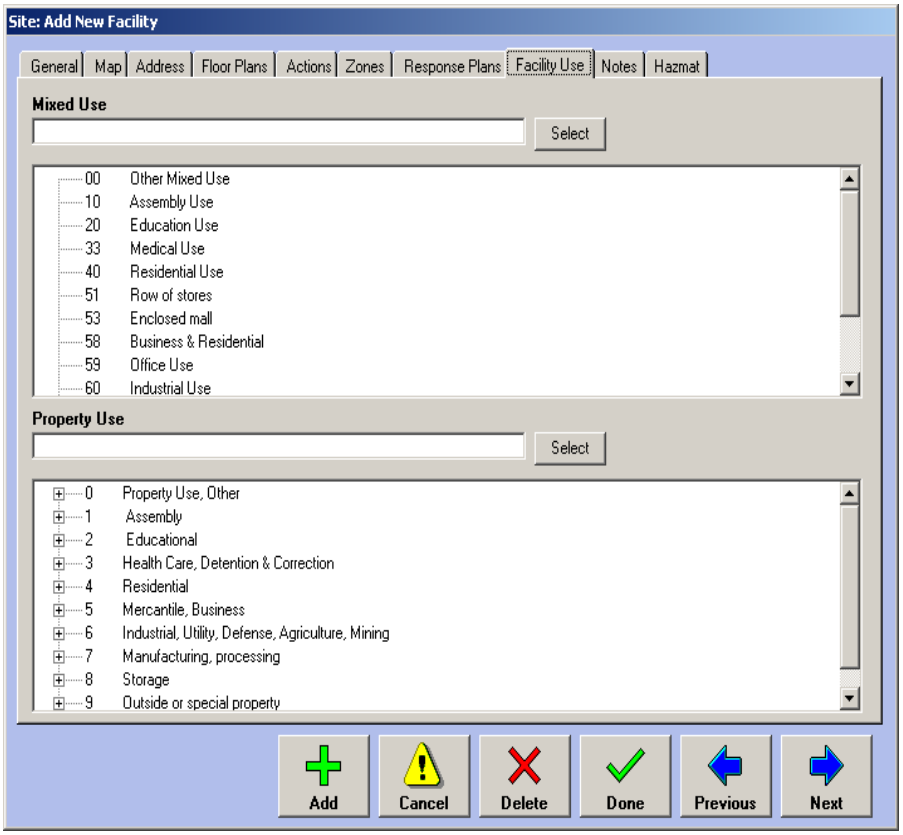
18 Click **Add** to add a response plan for the facility; or select the response plan you want to edit or delete and click the appropriate button. For information on adding and editing response plans, see "Response Plans" on page 3-2.

19 Click **Next** to advance to the E911 tab. (This tab is only available when an E911 system is installed for use with the D-21.)



20 To add the facility's phone number or numbers to the D-21 E911 phone listing, click **Add Phone**. For more information on the D-21 E911 database, see "Creating an E-911 Phone Number Database" on page 10-8.

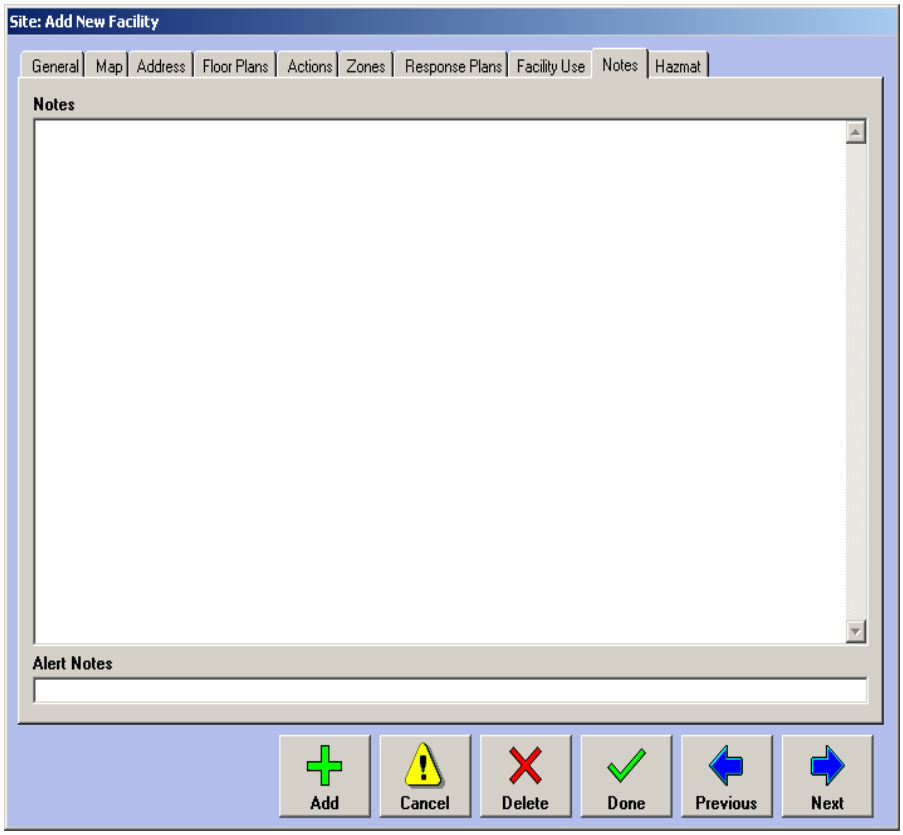
21 Click **Next** to advance to the Facility Use tab. Facility Use categories are NFIRS categories included when you export data from the D-21.



22 To assign a Mixed Use category, click on an item in the **Mixed Use** list and click **Select**. (You can also leave this blank.)

23 To assign a Property Use category, click the plus sign (+) next to the appropriate property category in the **Property Use** list, click the specific property type, and then click **Select**. (You can also leave this blank.)

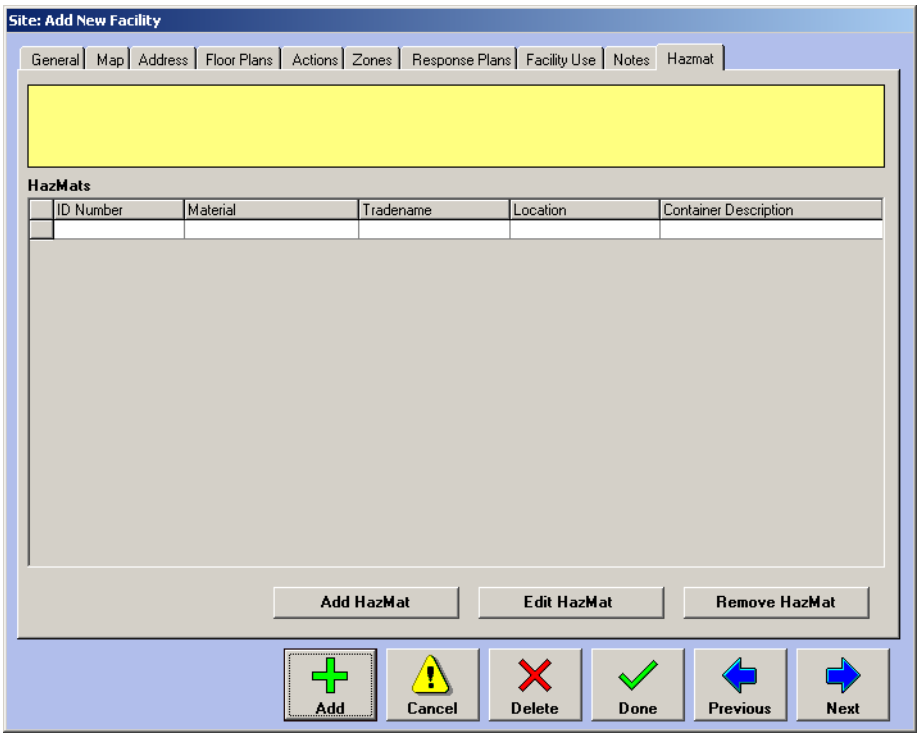
24 Click **Next** to advance to the Notes tab.



NOTE *Facility Notes and Alert Notes can be accessed in the D-21 Incident Client in many different viewers, including the Incident viewer and the Alert form.*

25 Enter the desired text in the Notes and Alert Notes textbox. Monaco recommends entering information into the Notes information section to help operators when handling an incident, such as remote unit information, location details, water supply locations, etc. The Alert Notes is a short (40 characters) textbox for information that is particularly essential for operators to know in the event of an alert in the facility.

26 Click next to proceed to the Hazmat tab.



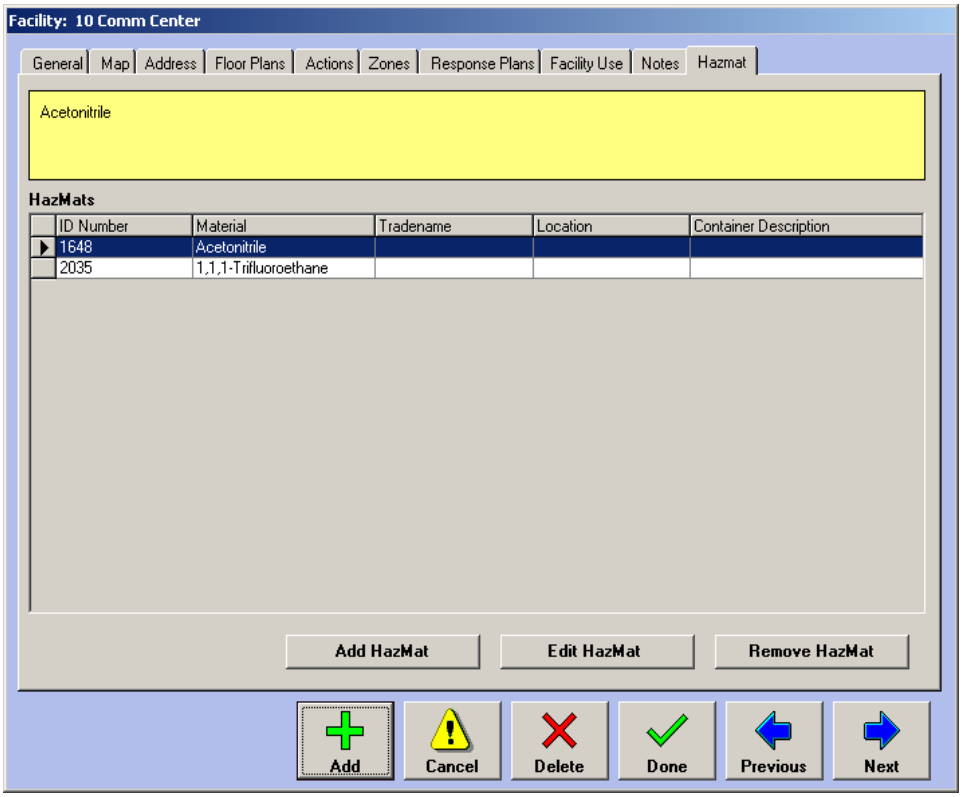
27 Use the **Add Hazmat** button to add a new Hazardous Material to the list. Use **Edit Hazmat** to change information in an existing hazardous material, or use **Remove Hazmat** to remove a hazardous material entry.

28 When you are done adding the facility, click **Done**.

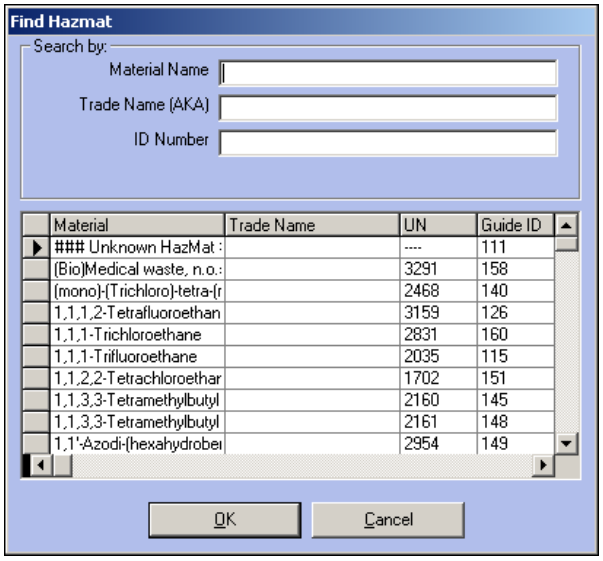
To add a Hazmat to a Facility

1 In the tree pane, right-click the facility to which you want to add the HazMat.

2 Click the Hazmat tab.



3 Click **Add HazMat**. The Find HazMat dialog box appears.

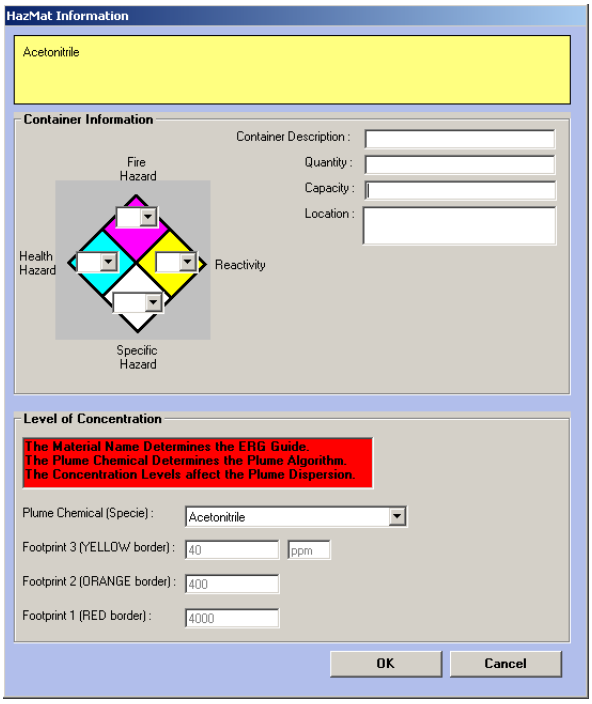


4 Select the hazardous material or materials in the list by clicking in the appropriate boxes on the left edge of the grid rows. You can quickly access specific rows by using the **Search by:** boxes. When you enter characters in one of the search boxes, the list of HazMat records

scrolls so the entry that begins with the same characters appears at the top. For example, if you enter “254” in the ID Number box, the first entry with an ID number that begins with “254” appears at the top of the list.

5 Click **OK**.

6 To enter specific information about how a HazMat is stored or used in the facility, select the hazardous material in the list and click **Edit HazMat**. The HazMat Information dialog box appears.



7 Enter information about the container holding the hazardous material in the container information fields: Container Description, Quantity, Capacity, and Location.

8 Use the drop-down lists on the diamond to specify the specific hazard and the numerical values for health, fire, and reactivity hazards.

9 If the hazardous material is already linked in the database with a chemical known to create a plume in the event of a spill, the Level of Concentration section will be automatically filled in with the Plume Chemical name and typical concentration levels. If plume information is not pre-populated, you can use the Plume Chemical drop-down list to identify the chemical stored at the facility. (This section is only available if the Plume feature is installed.)

10 Click **OK**.

To edit a facility Hazmat

1 In the tree pane, right-click the facility for which you want to edit HazMat information.

2 Click the Hazmat Tab.

3 Select the hazardous material you want to edit, and click the **Edit Hazmat** button.

4 In the Hazmat Information window change the information as needed.

5 Click **OK.**

To remove a facility Hazmat

1 In the tree pane, right-click the facility for which you want to remove a HazMat.

2 Click the Hazmat Tab.

3 Select the Hazmat entry you want to remove, and click **Remove Hazmat.**

4 Click **Yes** in the Delete Chemical dialog box.

To edit a facility

1 In the tree pane, right-click the facility you want to edit. The Facility dialog box appears.

2 Change dialog box entries and selections as desired. For more information on the tabs, boxes, and drop-down lists, see "To add a facility" on page 2-13.

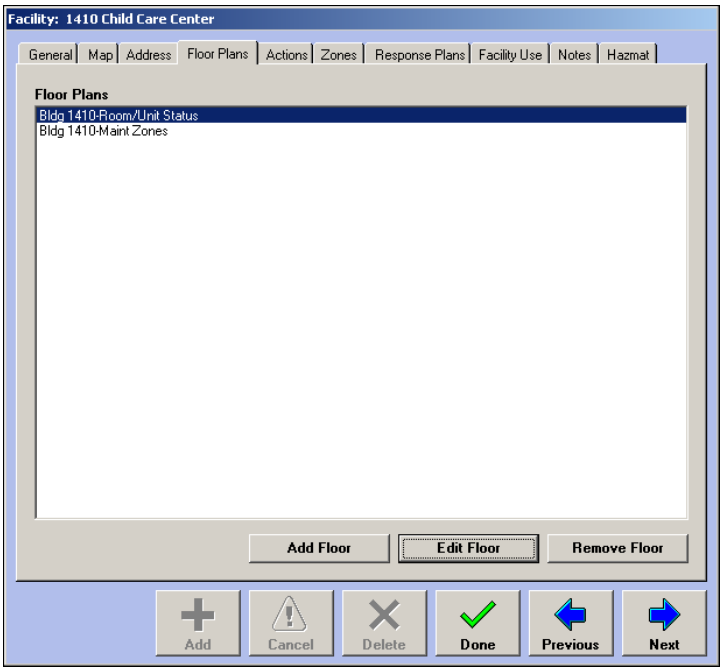
Adding Floor Plans

A D-21 Floor Plan is a line drawing or bitmap image associated with a facility record. Specific Floor Plans can be accessed by operators when there is an incident at the associated facility. You can also browse the collection of Floor Plans in the Floor Plans viewer in the D-21 Incident Client. See "Floor Plans, Pre-Plans, and Response Graphics" on page 5-3 for information on making files available for use as Floor Plans.

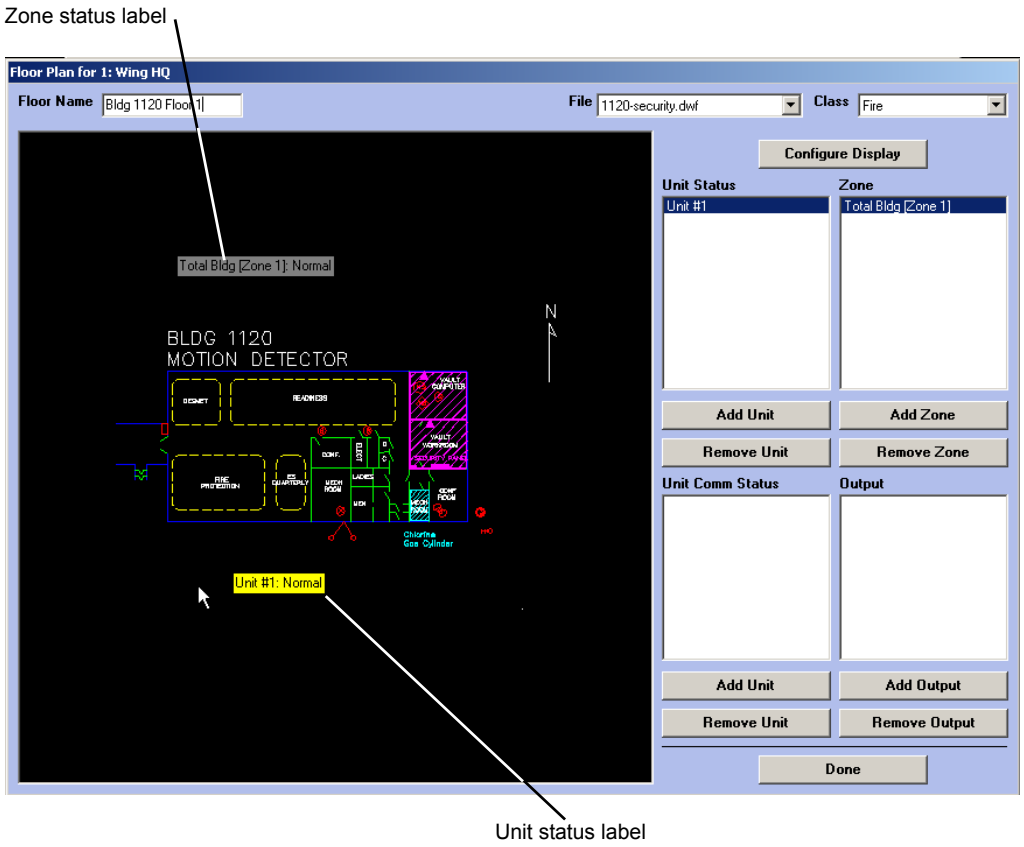
To add a floor plan to a facility

IMPORTANT *If you want to add a remote unit, output, or zone label to the floor plan, you must first create the remote unit, output, or zone.*

1. In the tree pane, right-click the existing facility to which you want to add a floor plan. The Facility dialog box appears.
2. Click the Floor Plans tab.



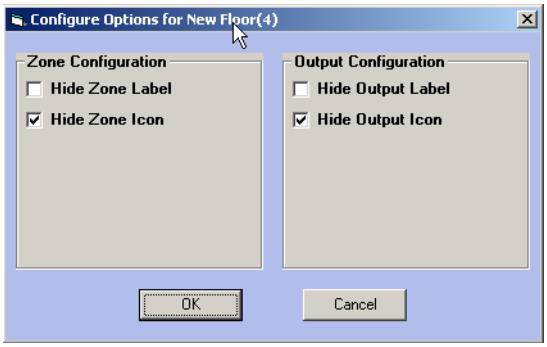
3 Click **Add Floor.** The Floor Plan dialog box appears, with the default Floor Name 'New Floor' entered.



- **Floor Name** Enter the name for the floor plan.
- **File** Select the floor plan image file. For more information on floor plan files, see "Floor Plans, Pre-Plans, and Response Graphics" on page 5-3.
- **Class** Select a class for the floor plan, if necessary. The class determines which workstations and user accounts can access the floor plan. By default, floor plans are available for all D-21 workstations and user accounts, but you can specify the floor plan be available only for Fire, Security, or Facility Management workstations and user accounts, or any combination of the three.

- **Configure Display** Allows the Administrator to configure how the labels and icons will be displayed on the floor plan graphic.

IMPORTANT *Labels and icons for a remote unit, output, or zone must be defined before they will be displayed on the floor plan.*



- **Unit Status** Click **Add Unit** to select a remote unit to place on the floor plan. Whenever the floor plan is displayed, the remote unit status label will indicate the current status condition of the remote unit. Only remote units associated with the facility are displayed in the list of units to add.
- **Unit Comm Status** Click **Add Unit** to select a dual comm remote unit to place on the floor plan. See "Configuring Dual Communication Channels" on page 6-4 for more information. When a dual comm unit is placed on a floor plan, the unit comm status label indicates whether the unit is communicating with the D-21 on the primary channel or the secondary channel, or is in a No Reply condition. Only remote units that have dual comm channels enabled and are associated with the facility are available to add to the floor plan.
- **Zone** Click **Add Zone** to select a zone to place on the floor plan. Whenever the floor plan is displayed, the zone status label will indicate the current status condition of the zone. Only zones associated with the facility are available to add to the floor plan.
- **Output** Click **Add Output** to select an output to place on the floor plan. Whenever the floor plan is displayed, the output status label will indicate the current status condition of the output. Only outputs that are associated with the facility are available to add to the floor plan.

4 Click **Done**.

Remote Interface Drivers (RIDs)

A remote interface driver (RID) is a software module that enables the D-21 server to communicate with a specific Monaco device, such as a radio frequency modem (RFM), or with a third-party product or service. The available D-21 RIDs are described in the table below.

IMPORTANT *The D-21 is pre-installed with the RIDs necessary for your system. Do not add or edit RIDs unless instructed to do so by a Monaco technical representative. If you are replacing a device with an identical device, you do not need to edit the associated RID.*

RID	Description
The RIDs listed below are documented in this manual.	
RFM 5000 (DTMF Radio Modem)	Use for communicating with a Monaco RFM 5000, a Dual-Tone Multi-Frequency (DTMF) radio modem. Remote units that communicate with the D-21 using the RFM 5000 include the BT2-3, BT2-4, and the M-1 conventional and addressable fire alarm control panels. See "Adding a RID for the RFM 5000" on page 2-31.
RFM 7000 (FSK Radio Modem)	Use for communicating with a Monaco RFM 7000, a Frequency Shift Keying (FSK) narrowband radio modem. Remote units that communicate with the D-21 using the RFM 7000 include the BT2-7, BT2-8, BT2-8S, BT-X, and M-2 conventional and addressable fire alarm control panels. See "Adding a RID for the RFM 7000 and RFM-X" on page 2-38.
ACU-1000 (Radio Switch)	Use for configuring an ACU-1000 Live Voice Input Radio Switch for live-voice mass notification messages. See "Adding a RID for the ACU-1000 Radio Switch" on page 7-13.
TCI E911	Use for receiving 911 call information from the TCI E-911 system. See "Configuring an E-911 System" on page 10-2.
Verizon E911	Use for receiving 911 call information from the Verizon E-911 system. See "Configuring an E-911 System" on page 10-2.
Zetron E911	Use for receiving 911 call information from the Zetron E-911 system. See "Configuring an E-911 System" on page 10-2.
Tone Alert (Tone Alert Panel Monitor)	Use in conjunction with the Tone Alert Unit for automatic and manual resource notification. See "Configuring Tone Alerting with a Tone Alert Unit" on page 11-6.
For information on the RIDs listed below, see the D-21 Remote Interface Driver Guide (P/N 001-399-01).	
Automatic Vehicle Location (Gemini, Placer)	Use for monitoring Monaco AVL units in vehicles.
CPS-484 (Power Supply Supervisor)	Use for monitoring the status of a Monaco CPS-484 backup power supply.
DIO (Dual Input/Output)	Use for monitoring the status of a Monaco Dual Input/Output Module (P/N 176-219-00). See the D-21 Dual Input Output Module I-O-M Manual (P/N 001-443-00) for more information.
DZI (Dual Zone Interface)	Use for communicating with a Monaco Dual Zone Interface, a two-zone input/output device connected locally to the D-21 Server.
General Status	Use for monitoring system-wide unacknowledged alarms and troubles and responding to them with actions and response plans.
GPIO (General Purpose Input/Output)	Use for communicating with a Monaco General Purpose Input/Output device.
iButton Analog Points	Use to monitor analog temperature values by reading the status of iButton temperature-sensing devices.

RID	Description
iButton Hub	Use to communicate with an HA7NetHub for IDS iButton enrollment. See"IDS iButton and PIN Assignments" on page 9-24 for more information.
NCD Relay (NCD Relay Control)	Use for communicating with the relays installed in a Monaco Automatic Control Output Panel.
RDU (Remote Display Unit)	Use for communicating with the a Monaco Remote Display Unit.
Remote Annunciator	Use for configuring custom LED display panels to show remote zone status.
Tone Generator (TGU) RID	Use in conjunction with the legacy Tone Alerting Panel for manually initiated resource notification.

Adding a RID for the RFM 5000

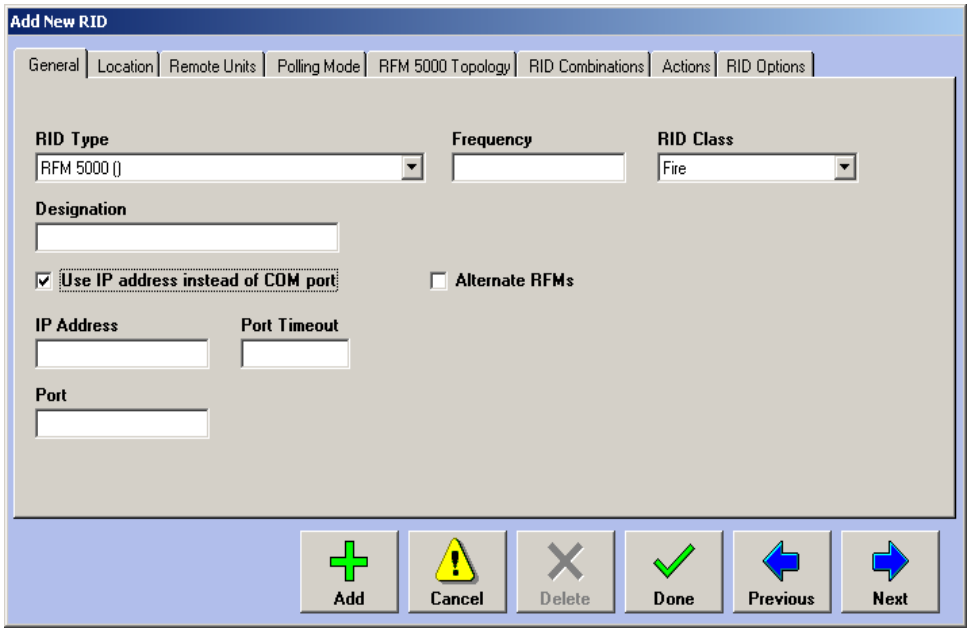
The RFM 5000 is a narrow-band, DTMF radio frequency modem. Configure an RFM 5000 RID for remote units reporting to the D-21 through an RFM 5000 device.

Before you begin

Add the facility where the RID device is located to the database so the facility information is available when you add the RID. See "Facilities" on page 2-13.

To add a RID for the RFM 5000

1 Select **Add > RID**.

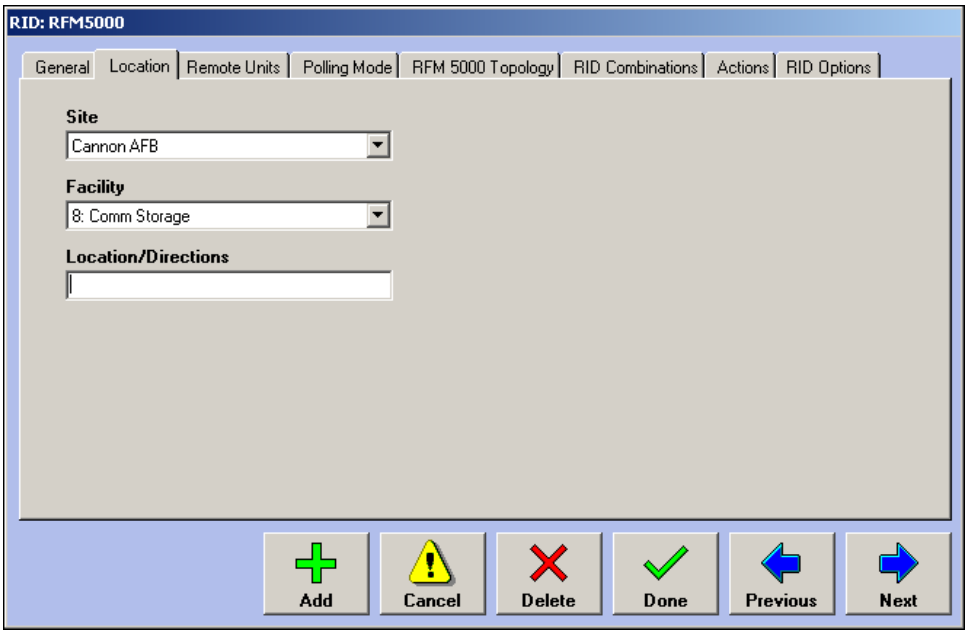


- **RID Type** Select RFM 5000 (DTMF Radio Modem).
- **Designation** Enter a name for the RID.
- **Frequency** Enter the frequency used by the RFM. (This box is for information purposes only and does not affect the frequency of the RFM 5000 device.)
- **Use IP address instead of COM port** Select this option if the RFM 5000 will communicate with the D-21 over an Ethernet network. When this checkbox is checked, text boxes appear for you to enter the Internet Protocol (IP) address, Port and

Port Time-out settings to be used by the RFM. An **Alternate RFMs** checkbox also appears, and an additional tab, labeled Alt RFM, will appear in the RID dialog box when the checkbox is checked. The new tab allows the administrator to add, edit, or remove alternate IP addresses and ports for alternate RFM 5000s on the same frequency.

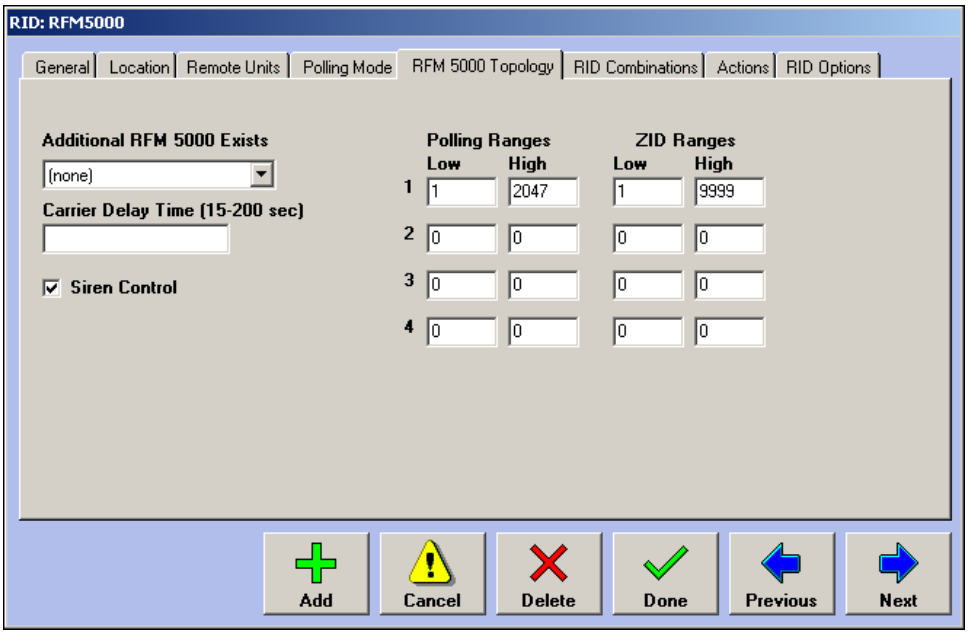
- **COM Port** Select the COM port by which the RFM 5000 is physically connected to the back of the D-21 computer.
- **RID Class** Select Fire, Security, or Facility Management to specify which workstations and operators can send commands to this RID and its remote units.

2 Click **Next** to advance to the Location tab.



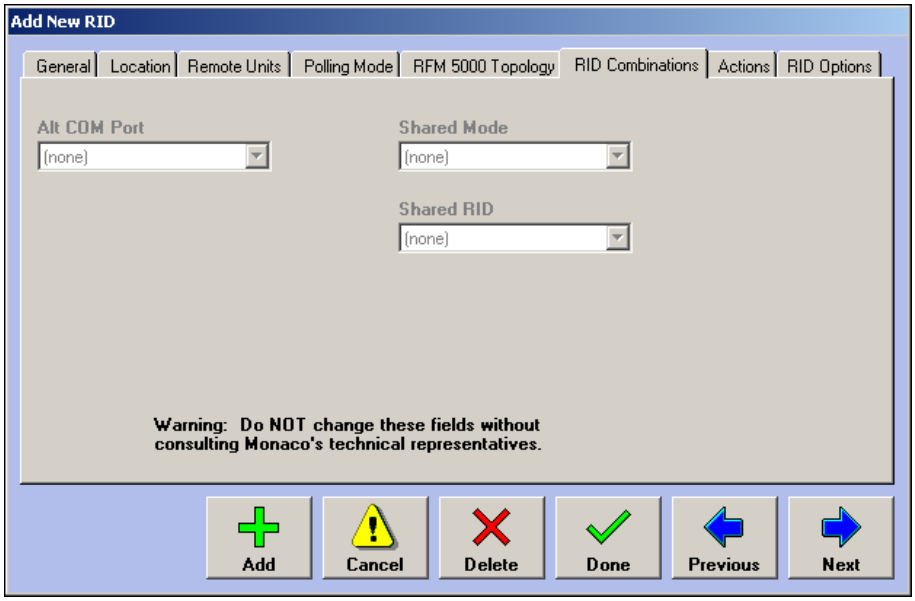
- **Site** Select the site where the RFM 5000 is located.
- **Facility** Select the facility where the RFM 5000 is located. If the appropriate facility does not appear in the drop-down list, make a note to return to this dialog box to specify the facility after it has been added to the database. See "To add a facility" on page 2-13.
- **Location/Directions** Enter descriptive information about the location.

3 Click the RFM 5000 Topology tab.



- **Additional RFM 5000 Exists** If this system includes another active or redundant (not alternate) RFM 5000 on the same frequency, select Yes.
- **Carrier Delay Time** Enter the amount of time in seconds during which the RFM 5000 is permitted to detect a continuous transmission before generating a carrier alarm. You can set the Carrier Delay from 15 to 200 seconds. To facilitate quick identification of potential problems, enter the smallest amount of time that lets you avoid nuisance alerts.
- **Siren Control** Select this option to enable the siren controller functionality in the RID. You must select this option if you want to add BT2-SC siren controllers to the database.
- **Polling Ranges** Enter the polling ranges for the remote unit numbers that communicate with this RFM 5000. You can enter up to four polling ranges for a single RFM 5000. The RFM 5000 only communicates with remote units with unit numbers included in these polling ranges.
- **ZID Ranges** Enter the ZID (zone identification) ranges for the zones associated with this RFM 5000. You can enter up to four ZID ranges for a single RFM 5000. The RFM 5000 only communicates with zones whose ZID numbers are included in these ranges.

4 Click the RID Combinations tab.



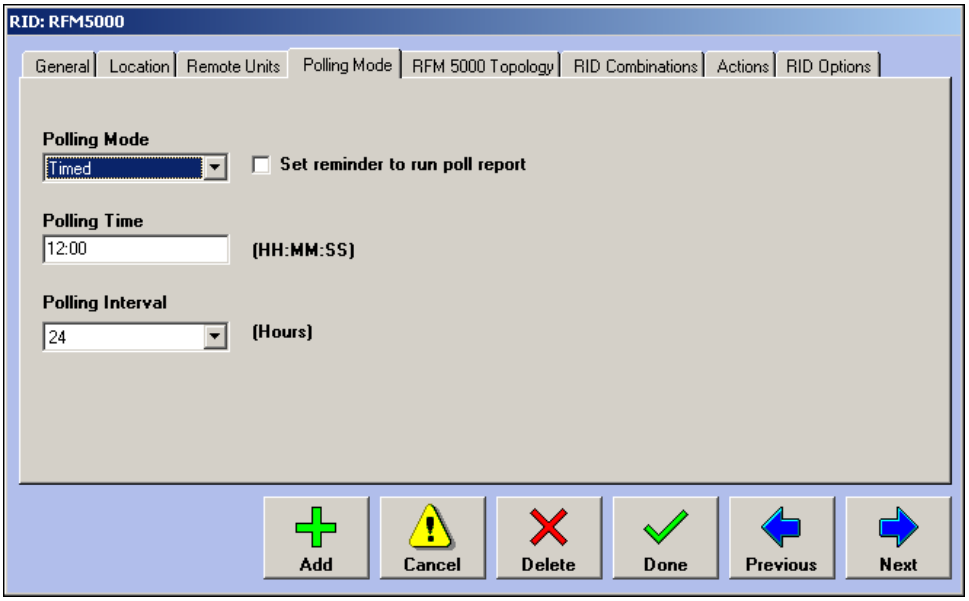
IMPORTANT *Do not change anything under the RID Combinations tab unless advised to do so by Monaco.*

- **Alt COM Port** Select the COM port to which a redundant RFM is attached. A redundant RFM is identical to the RFM associated with this RID, except that it is connected to a different COM port. If the main RFM fails, the D-21 switches to the RFM selected in the Alt COM Port drop-down list.
- **Shared Mode/RID** Select the RFM that shares this RFM's frequency. The D-21 is designed so that an RFM 5000 and RFM 7000 can share a single frequency. This feature is dongle-activated, and RIDS for both of the RFMs that share a frequency must be added before you can make Shared Mode and Shared RID selections. Select

Shared Frequency (transition) from the Shared Mode drop-down list, and then select the name of the RFM with the same frequency from the Shared RID drop-down list. *You must make these selections in the RID dialog boxes for both shared-frequency RFMs.*

NOTE *The Shared Frequency feature is designed for sites using a combination of the two RFM types. Because some advanced RFM 7000 features are not supported when the frequency is shared, it is important to consult a Monaco representative before sharing a frequency.*

5 Click the Polling Mode tab.



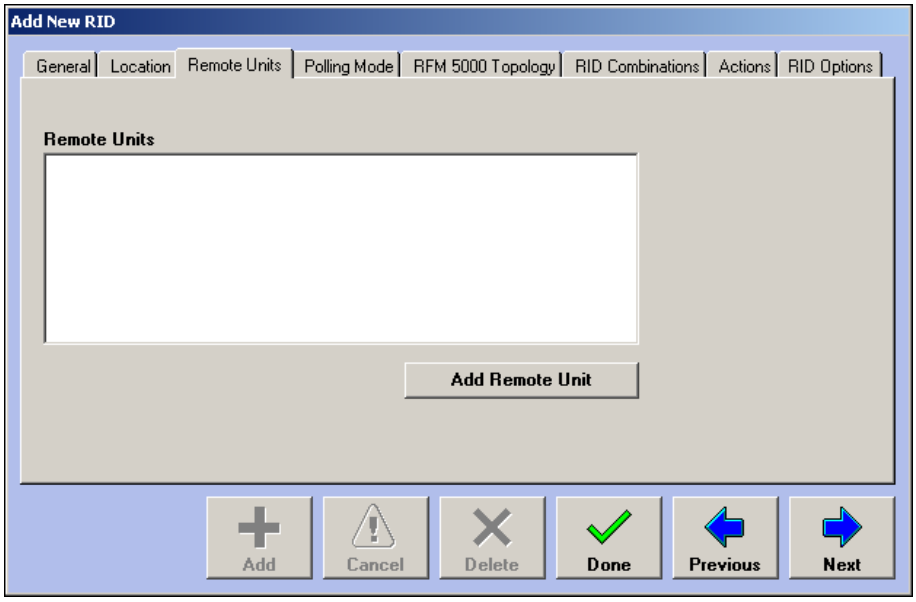
6 Select the polling mode:

- **Manual Poll Only** The RFM 5000 does not automatically request status from remote units on a regular basis.
- **Timed** The RFM 5000 automatically requests status from remote units at a specified interval starting at a designated time.

7 If the polling mode is Timed, enter the 24-hour clock time when you want polling to begin and select a polling interval.

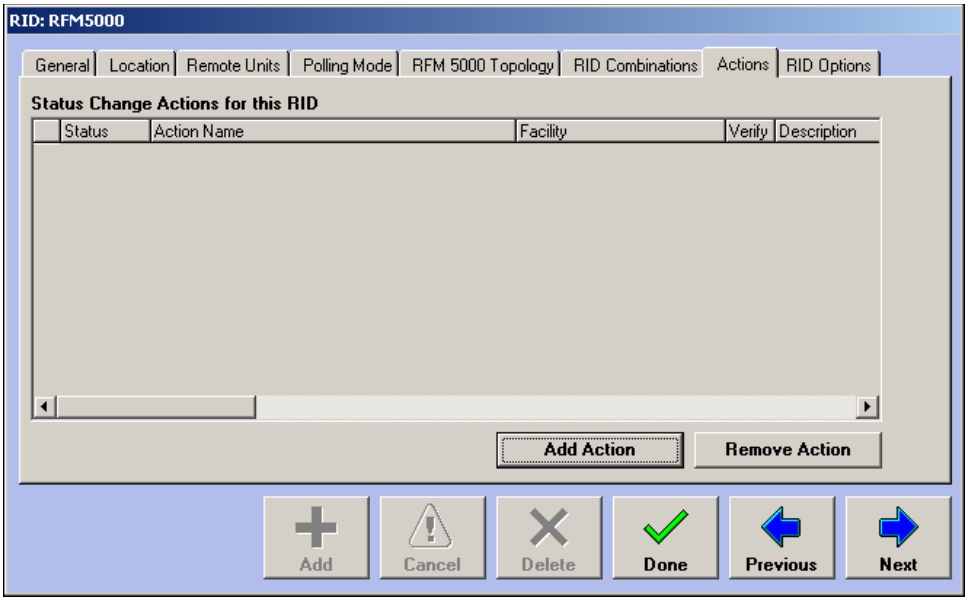
8 If the polling mode is Timed, check the **Set reminder to run poll report** option to display a pop-up reminder to print the polling report after a scheduled poll is complete.

9 Click the Remote Units tab.



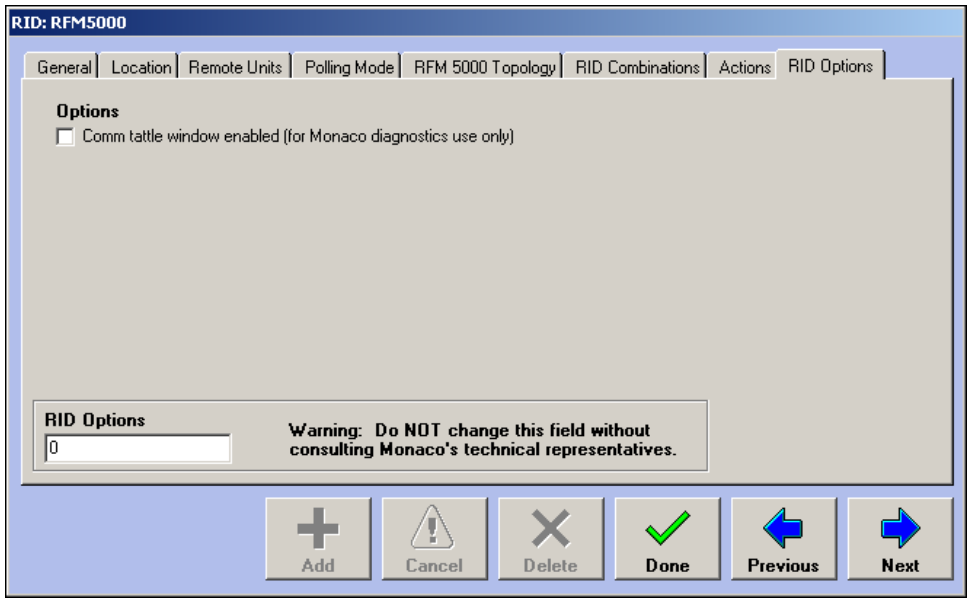
10 Click **Add Remote Unit** if you want to add remote units to this RID. For information on adding remote units, see "Remote Units" on page 2-51.

11 Click the Actions tab.



12 Click **Add Action** if you want to assign an action that will run when the RID changes status. See "Attaching Actions to Status Changes" on page 3-37 for more information.

13 Click the RID Options tab.



- **Comm tattle window enabled** Displays a floating window for troubleshooting purposes. Select this option only when directed to do so by Monaco personnel.

14 Click **Done**. A message appears to tell you the RID will be reloaded.

15 Click **OK**.

Adding a RID for the RFM 7000 and RFM-X

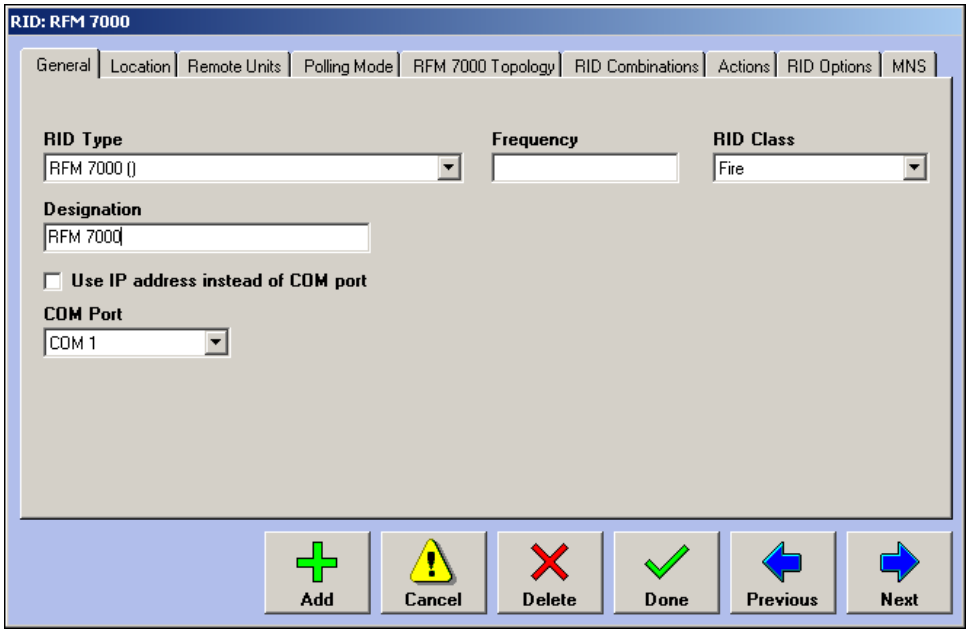
The RFM 7000 and the RFM-X are narrowband radio transceivers that use FSK (Frequency Shift Keying) radio protocol on UHF, VHF, or spread-spectrum frequencies to enable communication between the D-21 Central Receiving System and remote units. Create an RFM 7000 RID for remote units reporting to the D-21 using either an RFM 7000 or an RFM-X.

Before you begin

Add the facility where the transceiver device is located to the database so the facility information is available when you add the RID. See "Facilities" on page 2-13.

To add a RID for an RFM 7000 or an RFM-X

1 Select **Add > RID**.



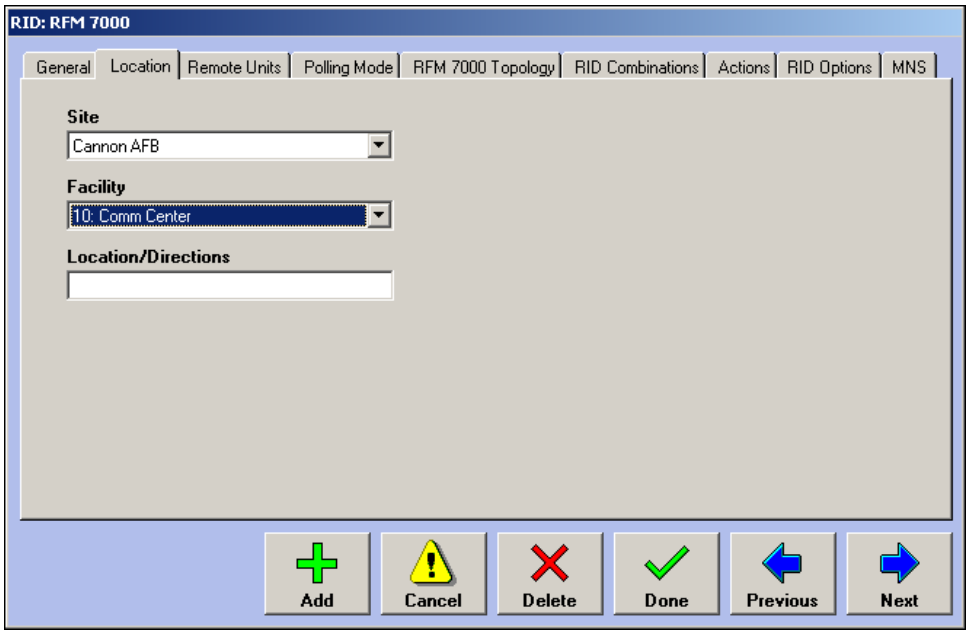
- **RID Type** Select RFM 7000 (FSK Radio Modem).
- **Designation** Enter a name for the RID.
- **Frequency** Enter the frequency used by the RFM. (This box is for information purposes only and does not affect the frequency of the RFM device.)
- **Use IP address instead of COM port** Select this option if the RFM will communicate with the D-21 over an Ethernet network. When this checkbox is checked, text boxes appear for you to enter the Internet Protocol (IP) address, Port and Port Time-out settings to be used by the RFM. An **Alternate RFMs** checkbox also appears, and an additional tab,

labeled Alt RFM, will appear in the RID dialog box when the checkbox is checked. The new tab allows the administrator to add, edit, or remove IP addresses and ports for alternate RFM 7000s or RFM-Xs on the same frequency.

NOTE *Use the IP address and port information listed on the label of the D-21 Remote Serial Port device that connects the RFM to the network.*

- **COM Port** Select the COM port where the RFM is physically connected to the back of the D-21 computer.
- **RID Class** Select Fire, Security, or Facility Management to specify which workstations and operators will be able to issue commands for this RID and its remote units.

2 Click **Next** to advance to the Location tab.

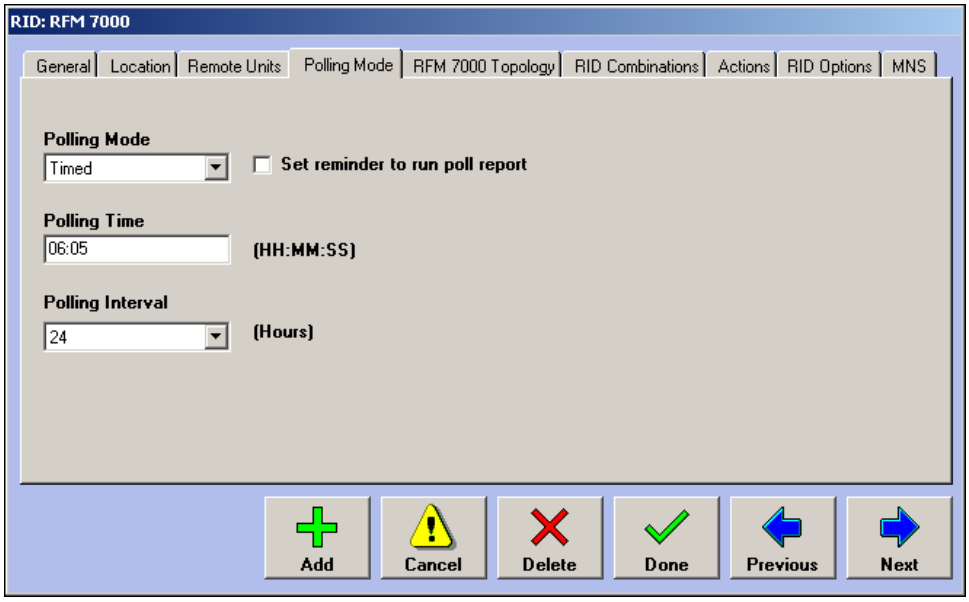


- **Site** Select the site where the RFM is located.
- **Facility** Select the facility where the RFM is located. If the appropriate facility does not appear in the drop-down list, make a note to return to this dialog box to specify the facility after it has been added to the database. See "To add a facility" on page 2-13.

NOTE *Site and Facility information is required for Mass Notification System applications.*

- **Location/Directions** Enter descriptive information about the location.

3 Click the Polling Mode tab.



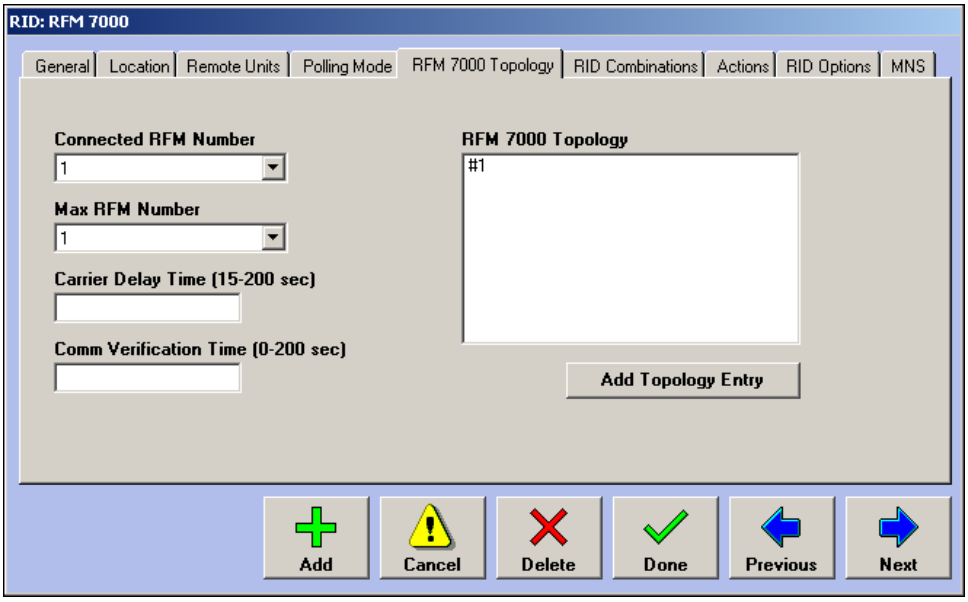
4 Select the polling mode:

- **Manual Poll Only** The RFM does not automatically request status from remote units on a regular basis.
- **Timed** The RFM automatically requests status from remote units at a specified interval starting at a designated time. Remote units respond with their current status.
- **Continuous** The RFM continuously polls remote units in sequence. Remote units respond to each poll and also send their status if it has changed since the last time they were polled.
- **Continuous/Timed** The RFM continuously polls remote units in sequence, and also automatically requests status from remote units at a specified interval starting at a designated time. Remote units respond to each continuous poll and also send their status if it has changed since the last time they were polled. Remote units respond to timed polls with their current status.

5 If the polling mode is timed or continuous/timed, enter the 24-hour clock time when you want polling to begin and a polling interval in hours.

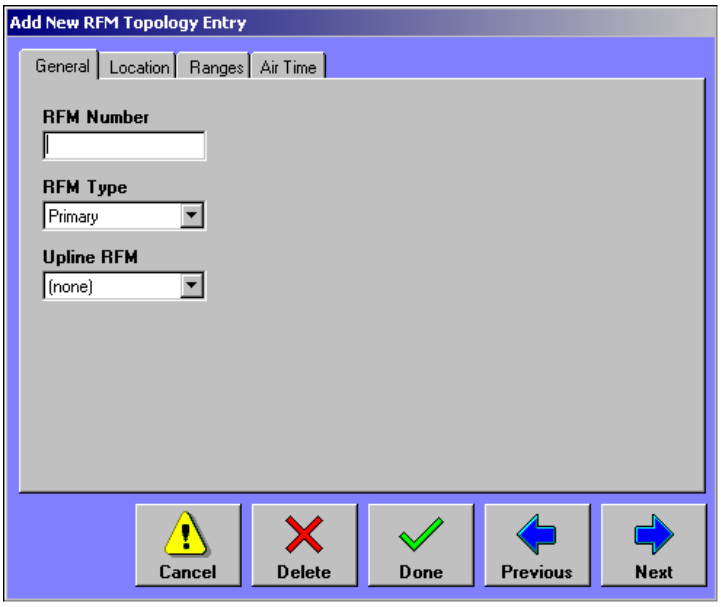
6 If the polling mode is timed or continuous/timed, check the **Set reminder to run poll report** option if you want to display a pop-up reminder message to print the poll report after a scheduled poll is complete.

7 Click the RFM 7000 Topology tab,



- **Connected RFM Number** This value defaults to 1, and identifies the RFM that is physically connected to the D-21. If you are adding a RID for a topology that includes primary, secondary, and repeater RFMs, you must add each RFM as a separate topology entry, then select the connected RFM number from the list.
- **Max RFM Number** Select the total number of RFMs that will communicate with the D-21 via this RID. (This number does not include RFM 7000s or RFM-Xs on a different frequency, alternate RFMs on the same frequency, or any RFM 5000s.)
- **Carrier Delay Time** Enter the amount of time in seconds during which the RFM is permitted to detect a continuous transmission before generating a carrier alarm. You can set the Carrier Delay from 15 to 200 seconds. To facilitate quick identification of potential problems, enter the smallest amount of time that lets you avoid nuisance alerts.
- **Comm Verification Time** Enter the amount of time the RFM must be offline before the D-21 generates an alert. You can set the Comm Verification from 0 to 200 seconds.

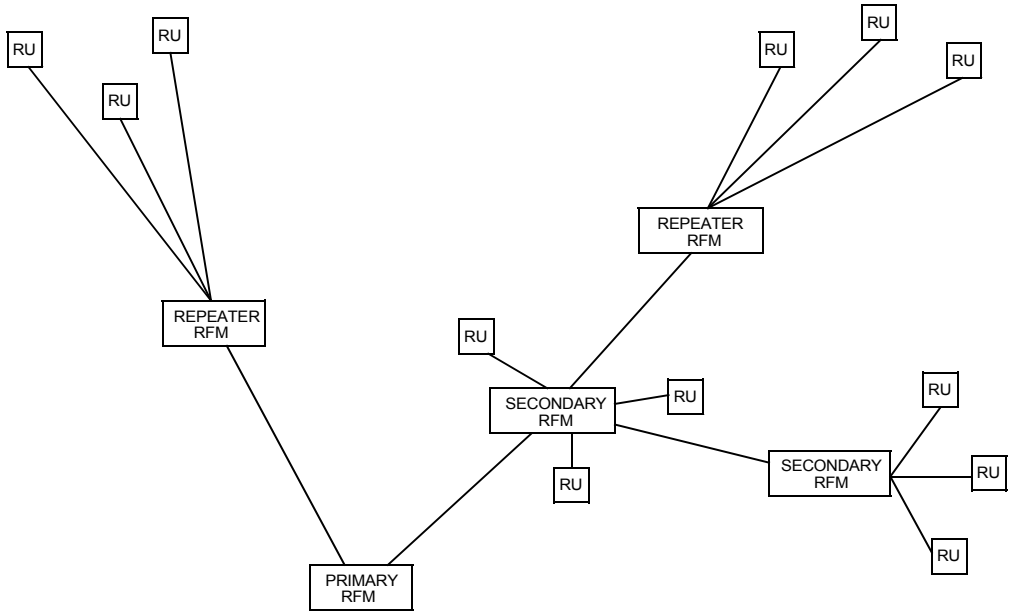
8 Click **Add Topology Entry**. The Add New RFM Topology Entry dialog box appears. You must add a topology entry for each RFM that will communicate with the D-21 via this RID.



9 Enter the number for the RFM topology entry you are adding. All RFM numbers must be lower than or equal to the Max RFM Number set under the 7000 Topology tab of the Add New RID dialog box.

10 Specify the RFM Type:

The following diagram shows how RFMs work together (RU = Remote Unit).



- **Primary** The primary RFM communicates with all other RFMs, as well as its own range of remote units. You can have only one primary RFM.

NOTE *The primary RFM must be set up before you can set up secondary or repeater RFMs.*

- **Secondary** A secondary RFM communicates with a range of remote units and may communicate with other secondary RFMs. Data from a secondary RFM is ultimately communicated to the primary RFM.
- **Repeater** A repeater RFM relays communications between remote units and a secondary or primary RFM.
- **Redundant Repeater** A redundant repeater shares a single RFM number with another repeater. Only one operates at a time, acting like a standard repeater. If the first fails, the second takes over.

11 If the RFM Type is other than Primary, select the number for the upline RFM from the Upline RFM drop-down list. A primary RFM does not have an upline RFM.

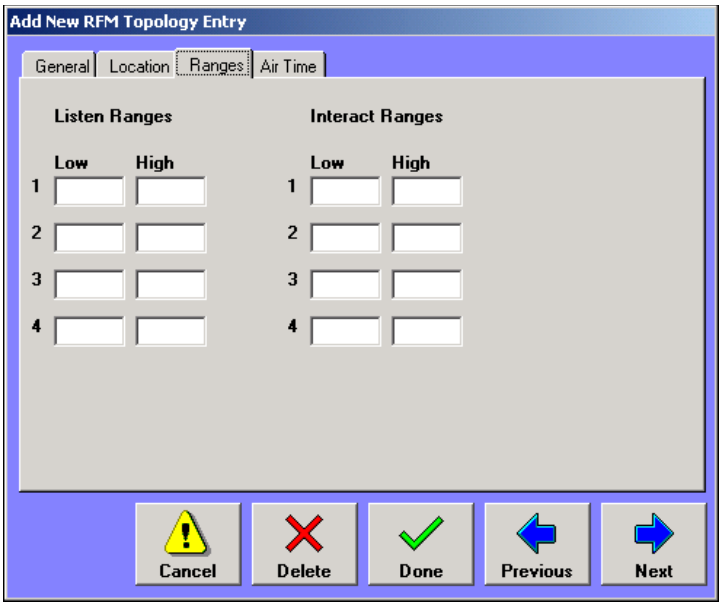
12 Click **Next** to advance to the Location tab.

13 Select the facility and enter a location for the RFM.

NOTE *If the desired facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See "To add a facility" on page 2-13.*

14 Click **Next** to advance to the Ranges tab.

NOTE *The following graphic is for a RID with two or more RFM 7000s. If there is only one RFM, instead of Listen Ranges and Interact Ranges the dialog box has "BT2 Ranges." If the RFM is a repeater, Listen Ranges is dimmed.*

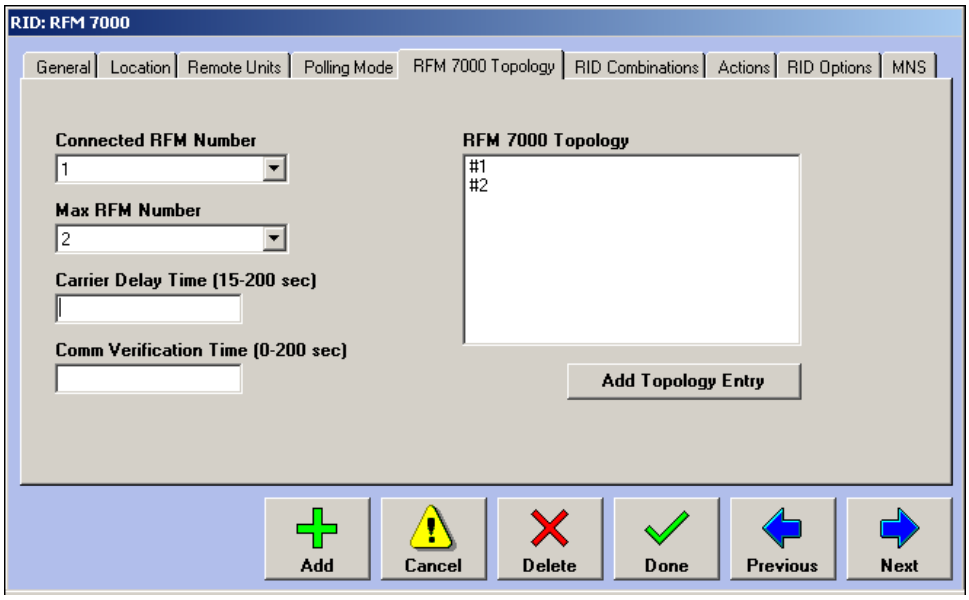


- **BT2 Ranges** If there is only one RFM in the topology, use the BT2 Ranges section to enter up to four ranges of unit numbers the RFM communicates with.
- **Listen Ranges** If there are two or more RFMs in the topology, use the Listen Ranges section to enter up to four ranges of unit numbers from which this RFM receives status information. Low values must be set to 1 or 1 plus a multiple of 4, and High values must be set to a multiple of four (1-64, 73-216, etc.). An RFM listens to transmissions from, but does not transmit to, remote units in its listen range. If the RFM is a Repeater, the Listen Ranges fields are not available.
- **Interact Ranges** If there are two or more RFMs in the topology, use the Interact Ranges section to enter up to four ranges of unit numbers the RFM communicates with. Low values must be set to 1 or 1 plus a multiple of 4, and High values must be set to a multiple of four (1-64, 73-216, etc.). Also make sure that all expansion unit numbers used by a

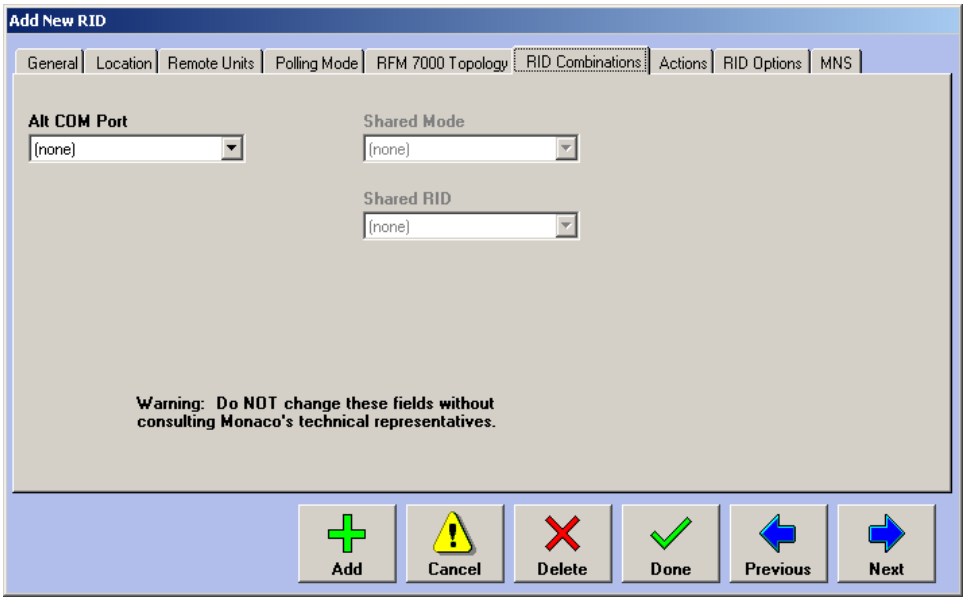
single remote unit, such as the four unit numbers used by a 64-zone M-2, are included in the same polling range. An RFM both transmits to and receives transmissions from remote units in its interact range.

IMPORTANT *Do not change anything under the Air Time tab unless advised to do so by a Monaco representative.*

15 If required, add another RFM to the same network; otherwise, click **Done**. The Add New RFM Topology Entry dialog box closes and you are returned to the RID dialog box.



16 Click **Next** to advance to the RID Combinations tab.

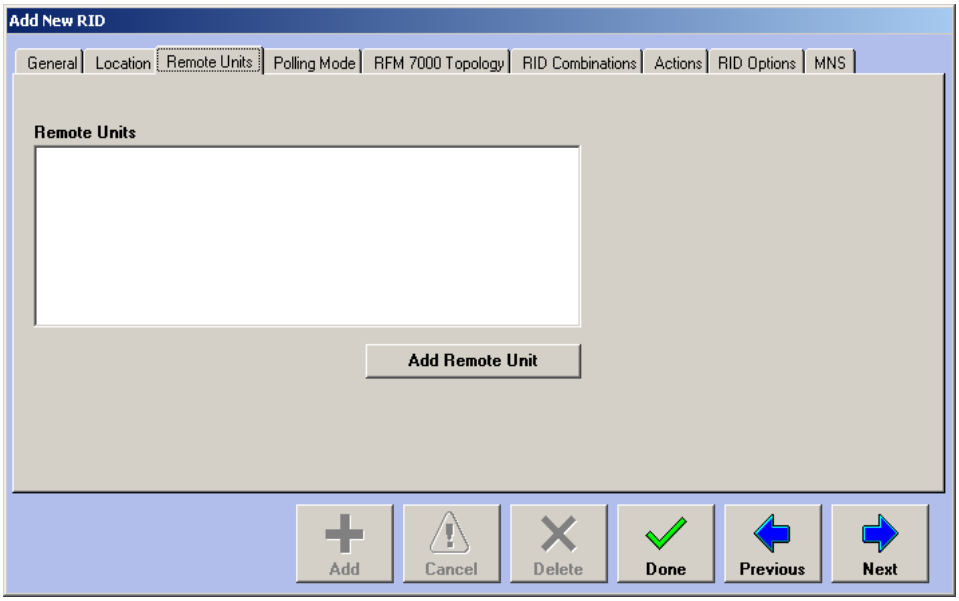


IMPORTANT *Do not change anything under the RID Combinations tab unless advised to do so by Monaco.*

- **Alt COM Port** Select the COM port to which a redundant RFM is attached. A redundant RFM is identical to the RFM associated with this RID, except it is connected to a different COM port. If the main RFM fails, the D-21 switches to the RFM selected in the Alt COM Port drop-down list.
- **Shared Mode/RID** Select the RID that shares this RFM's frequency. The D-21 is designed so an RFM 5000 and RFM 7000 can share a single frequency. This feature is dongle-activated, and RIDS for both of the RFMs that share a frequency must be added before you can make Shared Mode and Shared RID selections. Select **Shared Frequency (transition)** from the Shared Mode drop-down list, and then select the name of the RFM with the same frequency from the Shared RID drop-down list. *You must make these selections in the RID dialog boxes for both shared-frequency RFMs.*

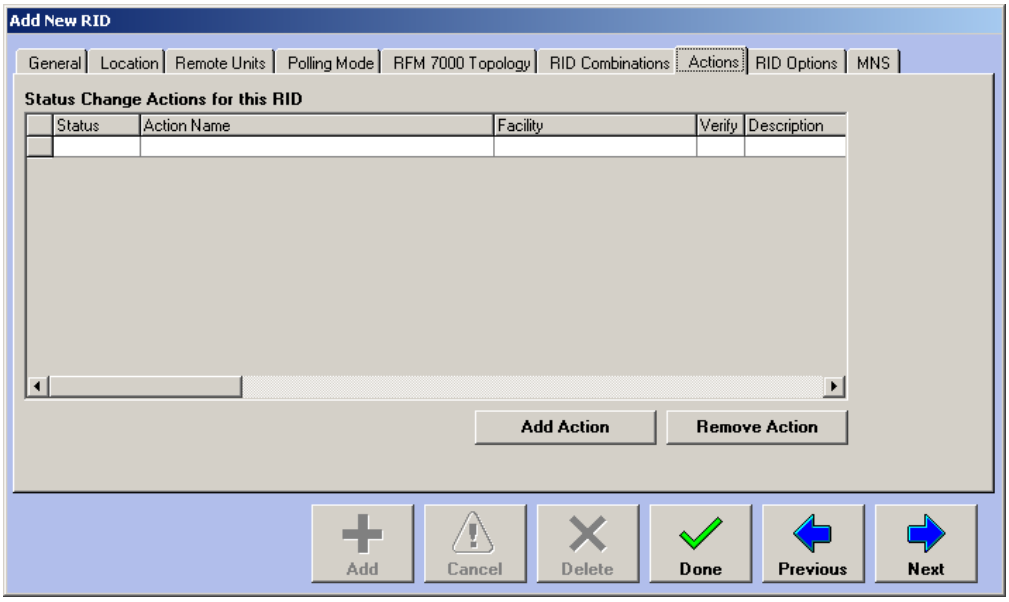
NOTE *The Shared Frequency feature is designed for sites using a combination of the two RFM types. Because some advanced RFM 7000 features are not supported when the frequency is shared, it is important to consult a Monaco representative before sharing a frequency.*

17 Click the Remote Units tab.



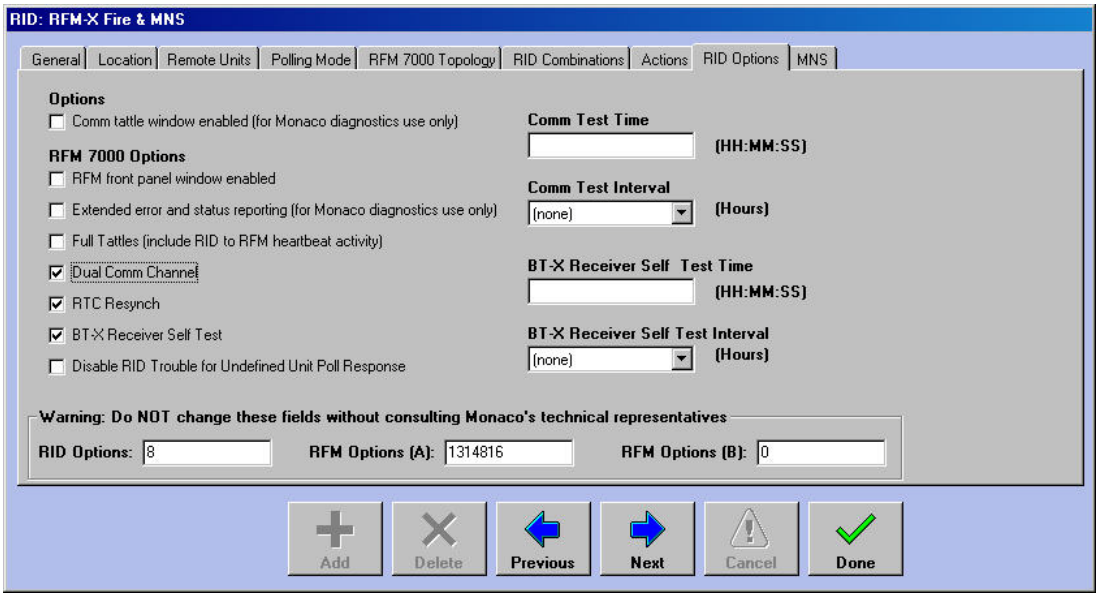
18 Click **Add Remote Unit**. The Add New Remote Unit dialog box appears. If you are ready to add remote units to this RID, see "Remote Units" on page 2-51 for more information.

19 Click the Actions tab.



20 Click **Add Action** to assign an action that will run when the RID changes status. The New Status Change Action dialog box appears. See "Attaching Actions to Status Changes" on page 3-37 for more information.

21 Click the RID Options tab.



- **Comm tattle window enabled** The tattle window is used for troubleshooting purposes. Select this option only when directed to do so by Monaco personnel.
- **RFM front panel window enabled** The RFM front panel window is a visual representation of the LEDs on the front panel of the RFM and is used for troubleshooting purposes. Select this option only when directed to do so by Monaco personnel.

- **Extended error and status reporting** When this option is enabled, an RFM-X will generate an AC Fail alert if it loses ac power or a Tamper alert if its tamper switch is tripped.
- **Full Tattles** For troubleshooting purposes only. Select this option only when directed to do so by Monaco personnel.
- **Dual Comm Channel** Enable this option when you are configuring the RID for Dual communication, which is only available with BT-X remote units which communicate with an RFM-X. Dual communication must also be enabled for each BT-X Communicator, BT-X Communicator Plus, or IDS Master unit that has primary and secondary communication modes. See "Configuring Dual Communication Channels" on page 6-4. After this checkbox is checked, the following two text boxes appear:

– **Comm Test Time** and **Comm Test Interval**. Use these text boxes to enter the 24-hour clock time for the initial and the interval for subsequent automatic Dual Comm Tests. Only schedule the Dual Comm Test if the RFM polling mode is set to Continuous or Timed/Continuous. Be sure the scheduled time does not overlap with other scheduled system operations such as extended polls or automatic database backups. See "Dual Communication Testing" on page 6-5 for more information.

- **RTC Resynch** When this option is enabled, the RID will synchronize the internal clocks of the BT-X remote units it with which it communicates with the D-21 clock every day at 3:15 am.
- **BT-X Receiver Self Test** Enable this option to schedule automatic communication status checks with any BT-X remote units with which the RID communicates. After this checkbox is checked, two additional text boxes appear, **BT-X Receiver Self Test Time** and **BT-X Receiver Self Test Interval**. Use these text boxes to enter the 24-hour clock time for the initial and the interval for subsequent automatic BT-X Receiver Self Tests.
- **Disable RID Trouble for Undefined Unit Poll Response** When this option is enabled, a RID Trouble alert will not be displayed if a unit that has not yet been entered in the D-21 database responds to an extended poll of the RID.

22 If the D-21 Mass Notification option is installed, the RFM 7000 RID dialog box also has an MNS tab. Use this tab to specify whether the RID supports pre-recorded and live-voice messages. For information on the MNS options, see "Enabling the RFM 7000 RID for Mass Notification" on page 7-4.

23 Click **Done**. An alert appears informing you the RID will be reloaded.

24 Click **OK**.

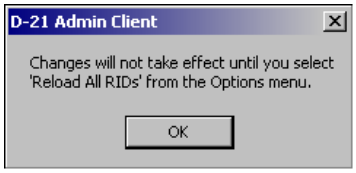
To delete a RID

IMPORTANT *You must delete remote units associated with the RID before you can delete the RID. For information on deleting a remote unit, see "To delete a remote unit" on page 2-61.*

1. In the tree pane, right-click the RID you want to delete. The RID dialog box appears.
2. Click **Delete**. A confirmation message appears.
3. Click **Yes**.

Reload All RIDs

The **Reload All RIDs** command on the Commands menu refreshes all RIDs with updated information, and should be issued after modifications have been made to remote unit data. The D-21 Admin Client may generate the following message to prompt you to select this menu item.



If you are making modifications to multiple remote units, you do not need to issue the **Reload All RIDs** command until after you've made all desired changes.

IMPORTANT *The Reload All RIDs command is only available if the operator who is logged in is assigned data entry level 2 or higher in the D-21 Admin Client. For more information on setting an operator's data entry level, see "To add an operator" on page 2-97.*

To reload all RIDs

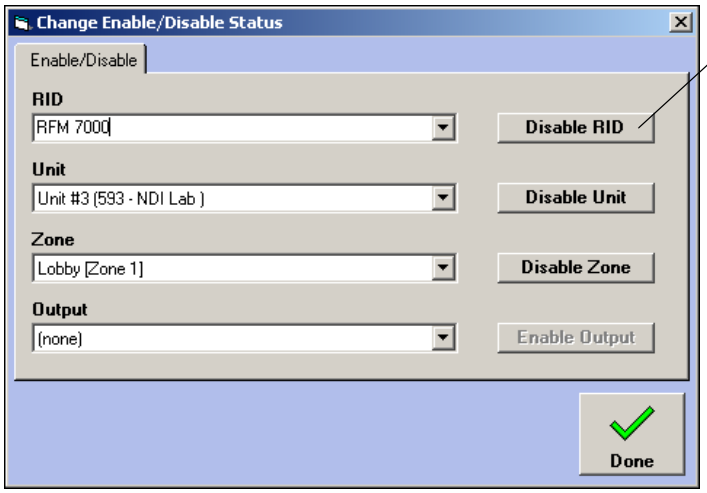
1. Select **Commands > Reload All RIDs**. A message appears, asking whether you are sure you want to reload all RIDs.
2. Click **Yes**.

Enabling and Disabling RIDs, Units, Zones, and Outputs

You can enable and disable RIDs, remote units, zones, and outputs from the D-21 Admin Client. Using the Enable/Disable command from the D-21 Admin Client is equivalent to changing the status of the device from the Device Status viewer in the D-21 Incident Client.

To enable or disable a RID, unit, zone, or output

1 Select **Commands > Enable/Disable Commands**. The Change Enable/Disable Status dialog box appears.



2 To enable or disable:

- **RID** Select the RID and click the button to the right of the RID drop-down list. If the RID is already enabled, clicking the RID button disables the RID. If the RID is disabled, clicking the RID button enables the RID.
- **Units** Select the RID that communicates with the unit you want, and then select the remote unit. Click the button to the right of the Unit drop-down list. If the unit is already enabled, clicking the Unit button disables the unit. If the unit is disabled, clicking the Unit button enables the unit.
- **Zone** Select the RID, unit, and zone. Click the button to the right of the Zone drop-down list. If the zone is already enabled, the Zone button disables the zone. If the zone is disabled, clicking the Zone button enables the zone.
- **Output** Select the RID, unit, and output. Click the button to the right of the Output drop-down list. If the output is already enabled, the Output button disables the output. If the output is disabled, clicking the Output button enables the output.

NOTE *You can only change the status of one device at a time.*

3 Click **Done**.

Remote Units

'Remote unit' is the term used in the D-21 to refer to the physical devices that communicate status to the D-21 through an RFM and its associated remote interface driver (RID). For more information on RIDs, see "Remote Interface Drivers (RIDs)" on page 2-30. The table below lists Monaco and third-party remote units which can be used with the D-21, along with the unit type and RID to use when you add the remote unit to the database, the possible unit class, and a source for information on configuring the remote unit.

Unit Class

Each remote unit must be classified as either a Fire, Security, or Facility Management unit. Commands to a Fire unit can only be issued on D-21 workstations where the Fire Client is enabled. Similarly, commands to Security units can only be issued on Security Client workstations, and commands to Facility Management units can only be issued on Facility Management Client workstations. If a workstation has all three clients enabled, you can issue commands to all three types of units. The class of some remote unit types is predefined as Fire or Security and cannot be changed.

Remote Unit	RID Type	Unit Type	Unit Class	Notes
Monaco Building Transceivers				
BT2, BT2-1, BT2-2	RFM 5000 (DTMF)	BT2-0/1/2	Fire	See "To add a remote unit" on page 2-55.
BT2-3	RFM 5000 (DTMF)	BT2-3	Fire or Fac Mgmt	See "To add a remote unit" on page 2-55.
BT2-SC (Siren Controller)	RFM 5000 (DTMF)	BT2-SC	Fire	The Siren Controller option must be enabled in the RFM 5000 Topology tab. See "To add a RID for the RFM 5000" on page 2-31. Valid unit addresses for a BT2-SC are 1024-1279. Add a zone at position 5 to supervise the siren controller. See "To add a remote unit" on page 2-55.
BT2-4	RFM 5000 (DTMF)	BT2-4(16) BT2-4(32)	Fire or Fac Mgmt	Use the BT2-4(16) unit type for a 16-zone unit. Use BT2-4(32) for a BT2-4 with more than 16 zones. See "To add a remote unit" on page 2-55.
BT2-R	RFM 5000 (DTMF)	BT2-R	Fire	See "To add a remote unit" on page 2-55.
BT2-7	RFM 7000 (FSK)	BT2-7(16)	Fire or Fac Mgmt	See "To add a remote unit" on page 2-55; if using the BT2-7with relays, add the remote unit and then see "To add an output" on page 2-74 for information on adding the relays to the database.
BT2-8	RFM 7000 (FSK)	BT2-8(16) BT2-8(32)	Fire or Fac Mgmt	Use the BT2-8(16) for a BT2-8 with up to 16 zones. Use the BT2-8(32) for a BT2-8 master and slave unit with up to 32 zones. See "To add a remote unit" on page 2-55.
BT2-8S	RFM 7000 (FSK)	BT2-8S(16)	Security	See "Setting Up the BT2-8S Security Unit" on page 9-2.
BT2-8S with Master zones	RFM 7000 (FSK)	BT2-8S-MC	Security	See "Setting Up the BT2-8S Security Unit" on page 9-2.

Remote Unit	RID Type	Unit Type	Unit Class	Notes
BT-XF (legacy program chip P/N 326-305-00 A.9)	RFM 7000 (FSK)	BT-XF(16): Add one for the 4 onboard zones and the first 2 fire zone cards. Add another for each additional group of 16 zones. BT-XF(32), BT-XF(48), BT-XF(64): Do not use these BT types.	Fire	When used for mass notification, see "Adding a BT-X with Mass Notification" on page 7-18; otherwise, see "To add a remote unit" on page 2-55.
BT-XS (legacy)	RFM 7000 (FSK)	BT-XS	Security	See "Setting Up the BT-X Security Unit" on page 9-11.
BT-X with Fire (program chip P/N 326-304-00 revision B.9 or higher)	RFM 7000 (FSK)	BT-X Communicator or Communicator Plus (Add one) *and* BT-XF(M) (Add one for each group of 16 fire zones after the 4 onboard zones)	Fire, Fac Mgmt, or Security Fire	See "To add the BT-X Communicator unit" on page 6-6. See "To add a remote unit" on page 2-55.
BT-X with Intrusion Detection (program chip P/N 326-304-00 revision B9 or higher)	RFM 7000 (FSK)	BT-X Communicator or Communicator Plus (Add one) *and* BT-XS(M) with IDS Master unit option selected (Add one. Provides up to 12 Master zones and 4 reserved status reporting zones.) *and* BT-XS(M) (Add one for each group of 16 IDS zones)	Fire, Fac Mgmt, or Security Security Security	See "To add the BT-X Communicator unit" on page 6-6. For more information on adding the IDS Master unit, see "Master Zones on the BT-XS" on page 9-12. See "Setting Up the BT-X Security Unit" on page 9-11.
BT-X with Access Control (program chip P/N 326-304-00 revision B.9 or higher)	RFM 7000 (FSK)	BT-X Communicator or Communicator Plus (Add one) *and* BT-X/ACS(M) (Add one for each group of four readers)	Fire, Fac Mgmt, or Security Security	See "To add the BT-X Communicator unit" on page 6-6. See "Adding a BT-X with Access Control" on page 8-10.
BT-X with Mass Notification (program chip P/N 326-304-00 revision B.9 or higher)	RFM 7000 (FSK)	BT-X Communicator or Communicator Plus (Add one)	Fire, Fac Mgmt, or Security	See "Adding a BT-X with Mass Notification" on page 7-18.

Remote Unit	RID Type	Unit Type	Unit Class	Notes
BT-X Wide Area Communicator	RFM 7000 (FSK)	BT-X/WAC+	Fire, Fac Mgmt, or Security	See "Adding a BT-X with Mass Notification" on page 7-18.
Monaco Fire Alarm Control Panels (FACP)				
M-1 FACP	RFM 5000 (DTMF)	M-1	Fire	See "To add a remote unit" on page 2-55.
M-1 Addressable FACP	RFM 5000 (DTMF)	MA-1	Fire	See "To add a remote unit" on page 2-55.
M-2 FACP	RFM 7000 (FSK)	M-2 (16)	Fire	See "To add a remote unit" on page 2-55.
M-2 Addressable FACP	RFM 7000 (FSK)	MA-2 (16)	Fire	See "To add a remote unit" on page 2-55.
Monaco Analog Addressable Plus FACP	RFM 7000 (FSK)	MAAP(+)	Fire	See the Monaco Addressable Plus Planner Guide (P/N 001-359-01).
Other Remote Unit Devices				
Dual Input/Output Module	DIO (Dual Input/Output)	DIO	Fire, Fac Mgmt, or Security	See the D-21 Remote Interface Driver Guide (P/N 001-399-01).
Dual Zone Input Module	DZI (Dual Zone Interface)	DZI	Fire, Fac Mgmt, or Security	See the D-21 Remote Interface Driver Guide (P/N 001-399-01).
iButton Network Hub	iButton Hub (iButton Enrollment)	HA7NetHub	Fire, Fac Mgmt, or Security	See the D-21 Remote Interface Driver Guide (P/N 001-399-01).
General Status	General Status	General Status	Fire, Fac Mgmt, or Security	See the D-21 Remote Interface Driver Guide (P/N 001-399-01).
Tone Alerting Panel	TGU (Tone Generator)	TG-1	Fire, Fac Mgmt, or Security	See the Tone Alerting section of the D-21 Remote Interface Driver Guide (P/N 001-399-01) and the D-21 Admin Client User Guide "Configuring Tone Alerting with a Tone Generator" on page 11-2.

Numbering Remote Units

The D-21 identifies each remote unit by its unit address. If the unit is a building transceiver or FACP, the unit address is programmed during the hardware installation and must match the unit address that is specified when the unit is added to the D-21 database. Remote units that

communicate with the D-21 via RFM are associated in the D-21 database with the remote interface driver (RID) for the RFM. Each unit address associated with an RFM RID must be unique for the RID.

IMPORTANT *A remote unit cannot report status to the D-21 if the unit address is not included in one of the polling ranges of its associated RFM.*

Each building transceiver or FACP remote unit is limited to 16 zones in the D-21 database. If a unit has more than 16 zones because of the addition of expansion equipment, multiple remote units with the same unit type and with contiguous unit addresses must be added to the D-21 database (one unit is required for each group of 16 zones).

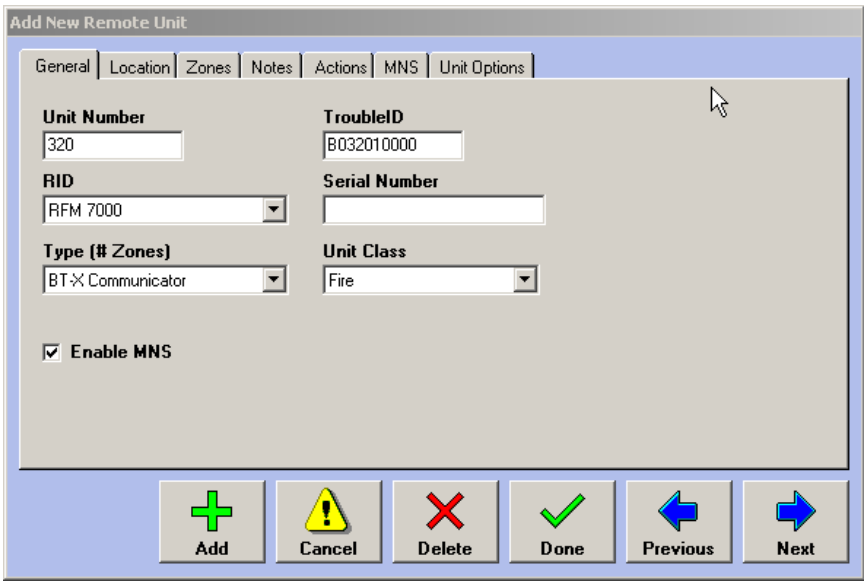
When a single device, such as a Dual Input/Output Module or Tone Alerting Panel, communicates directly with the D-21 via a network connection or COM port on the back of the D-21 server computer, the unit address is generally "1." For more information on configuring RIDs and remote units other than Monaco building transceivers and FACPs, see the D-21 Remote Interface Driver Guide (P/N 001-399-01).

For information on the unit addresses required by the multi-application BT-X, see "Adding the Multi-Application BT-X" on page 6-2.

Before you begin Be sure you previously added the remote interface driver (RID) that will communicate with the remote unit. See "Remote Interface Drivers (RIDs)" on page 2-30.

To add a remote unit

1 Select **Add > Remote Unit**.



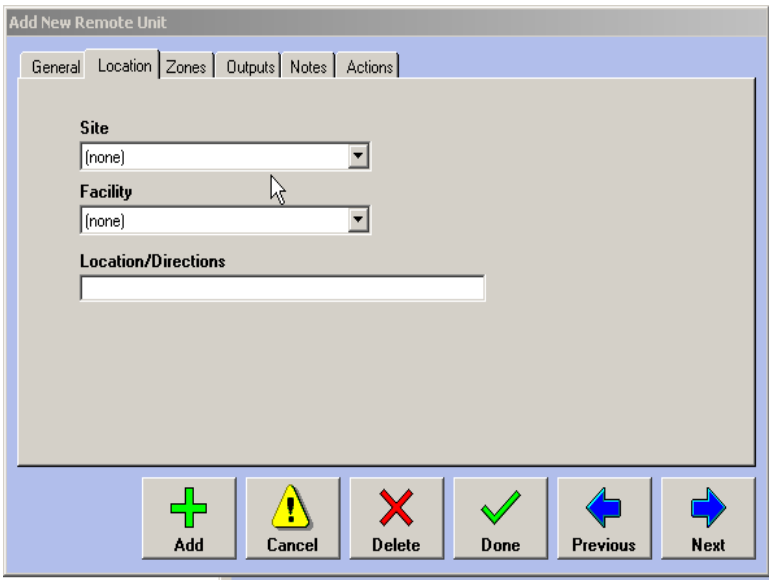
- **Unit Number** Enter the number that identifies the remote unit. See "Numbering Remote Units" on page 2-54 for more information on how units are numbered in the D-21. If you are configuring a BT-X, see "Adding the Multi-Application BT-X" on page 6-2.

- **RID** Select the RID to which you want to add the unit. Remote units must be added to the RIDs they will use to communicate with the D-21.

NOTE *You cannot add a remote unit without selecting a RID. If the RID you need for this remote unit has not been configured, click the Cancel button and see "Remote Interface Drivers (RIDs)" on page 2-30.*

- **Type (# Zones)** Select the remote unit type. Only remote unit types compatible with the selected RID are listed. See "Remote Units" on page 2-51 to determine which remote unit type to select.
- **TroubleID** Reserved for use by Monaco Enterprises.
- **Serial Number** Enter the serial number for the remote unit hardware. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class for the remote unit type. If the unit class field is enabled, you can select either Fire, Security, or Facility Management. If the unit class field is disabled, you cannot change the unit class. See "Unit Class" on page 2-52 for more information.

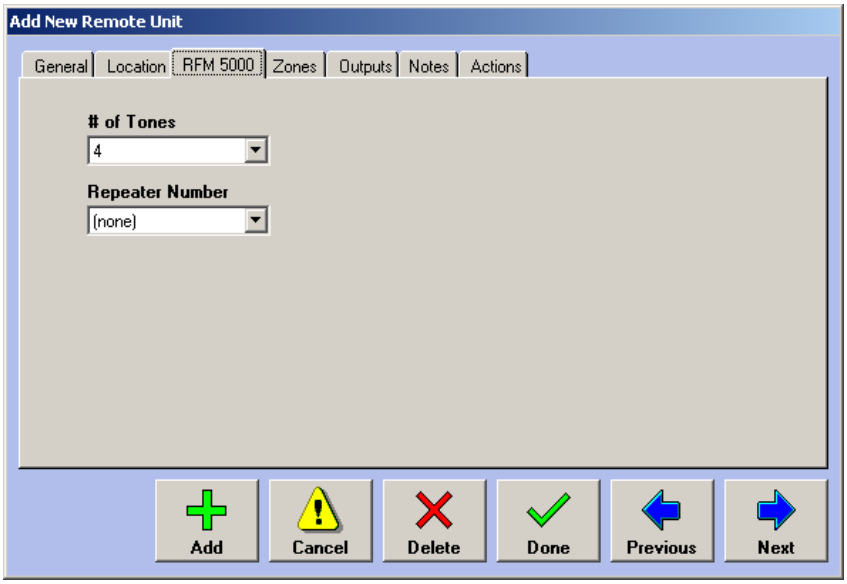
2 Click **Next** to advance to the Location tab.



3 Select the facility where the remote unit is located from the Facility drop-down list. If desired, enter more specific information in the Location/Directions box.

NOTE *Location information is required for MNS applications. If the facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See* *"To add a facility" on page 2-13.*

4 If the RID selected under the General tab is for an RFM 5000, click **Next** to advance to the RFM 5000 tab and follow the lettered steps below; otherwise, skip this step.



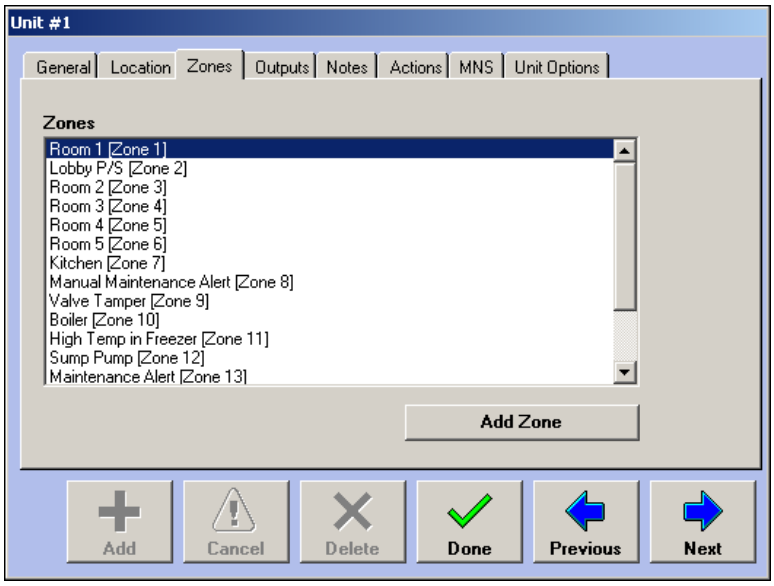
- **# of Tones** Select the number of tones the remote unit uses for communicating with the RFM 5000: 4 or 5.

NOTE *If you are configuring a BT2-SC remote unit for use as a siren controller (DTMF), you must use a unit address between 1024 and 1279 and set the # of Tones option to 5.*

- **Repeater Number** If the remote unit communicates via a remote unit repeater, select the repeater number. The remote unit repeater must be added to the database before it is available in this list.

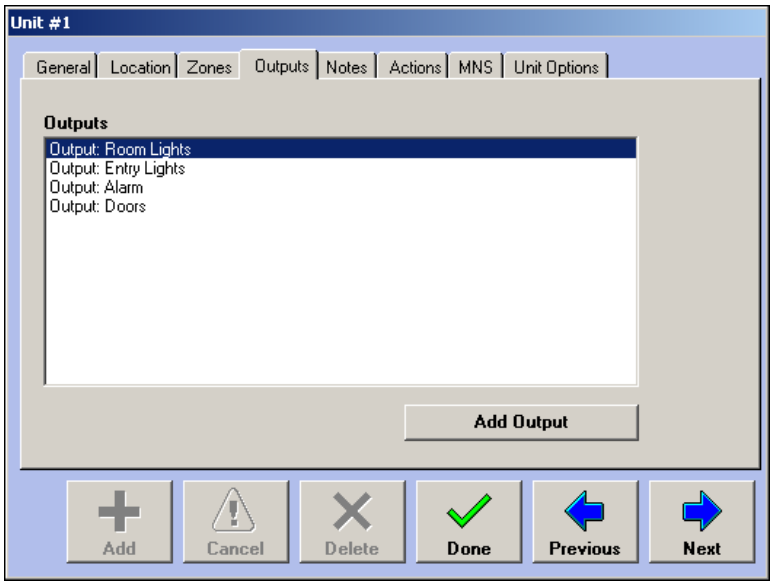
NOTE *A remote unit repeater repeats transmissions for a single remote unit. It is not the same as an RFM repeater.*

5 Click **Next** to advance to the Zones tab.



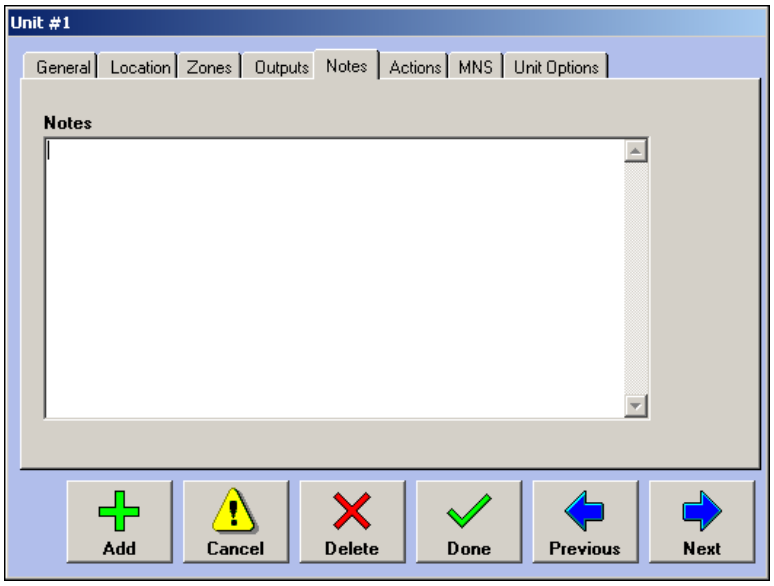
6 Click **Add Zone**. The Add New Zone dialog box appears. For information on using the Add New Zone dialog box to add fire reporting zones, see "To add a zone" on page 2-65.

7 When you have finished adding zones, click **Next** to advance to the Outputs tab.



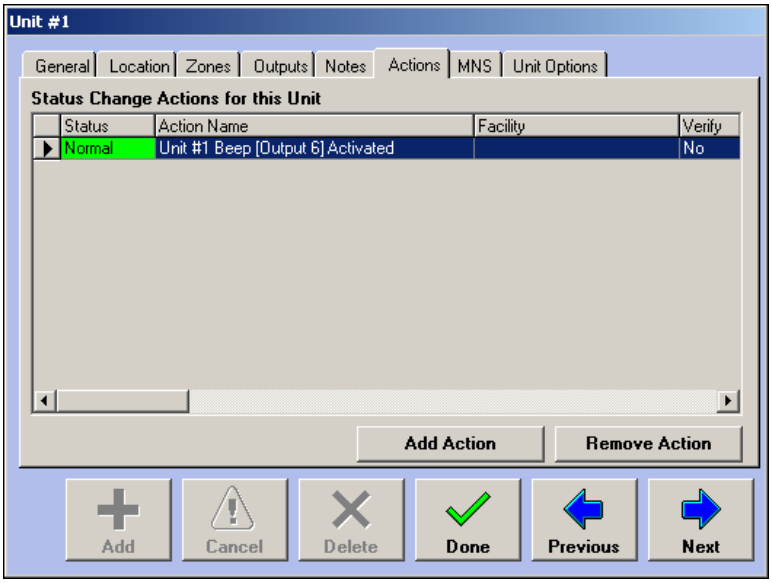
8 Click **Add Output.** The Add New Output dialog box appears. For information on adding outputs, see "Outputs" on page 2-74.

9 When you have finished adding outputs in the Add New Remote Unit dialog box, click **Next** to advance to the Notes dialog box.



10 Enter text in the Notes box as desired.

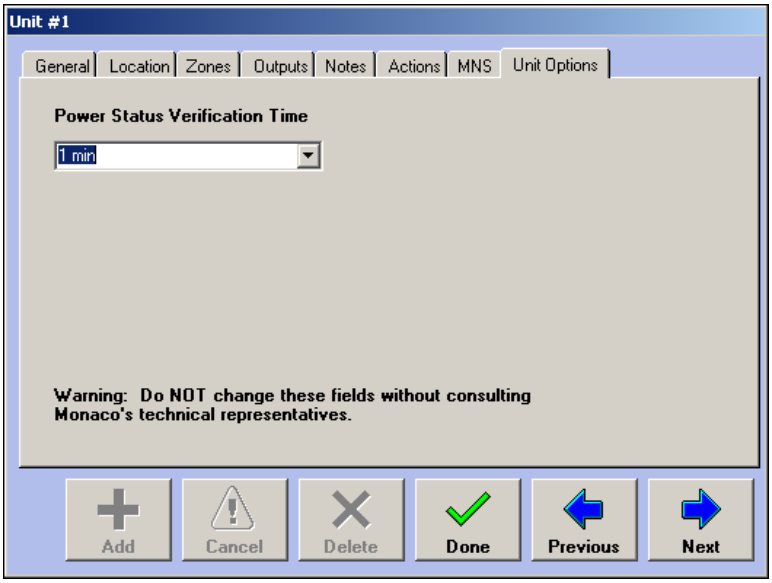
11 Click **Next** to advance to the Actions tab.



12 Click **Add Action** to assign an action that will run when the remote unit changes status. The New Status Change Action dialog box appears. See "Attaching Actions to Status Changes" on page 3-37 for more information.

NOTE *The MNS tab is only available when the RFM 7000 RID has mass notification (MNS) enabled. If you are configuring this remote unit for MNS, see "Configuring Mass Notification" on page 7-1 for more information.*

13 Click **Next** to advance to the Unit Options tab. The Unit Options tab is only available for the BT-XF (16), BT-XS, BT-XS (M), BT-X Communicator, and BT-X Communicator Plus.



- **Power Status Verification Time** Select the length of time for the D-21 to wait before displaying a Battery Fault alert from the unit. The default selection is none. Do not change this setting unless instructed to do so by a Monaco Help Desk representative.

14 Click **Done**.

To edit a remote unit

1 In the tree pane, right-click the remote unit you want to edit. The Remote Unit dialog box appears.

2 Change dialog box entries and selections as desired. For more information on the tabs, boxes, and drop-down lists, see "To add a remote unit" on page 2-55.

To delete a remote unit

IMPORTANT *You must delete zones and outputs associated with the remote unit before you can delete the remote unit. For information on deleting a zone, see "To delete a zone" on page 2-70; for information on deleting an output, see"To delete an output" on page 2-78.*

1 In the tree pane, right-click the remote unit you want to delete. The Remote Unit dialog box appears.

2 Click **Delete**. A confirmation message appears.

3 Click **Yes**.

Creating Remote Unit Groups

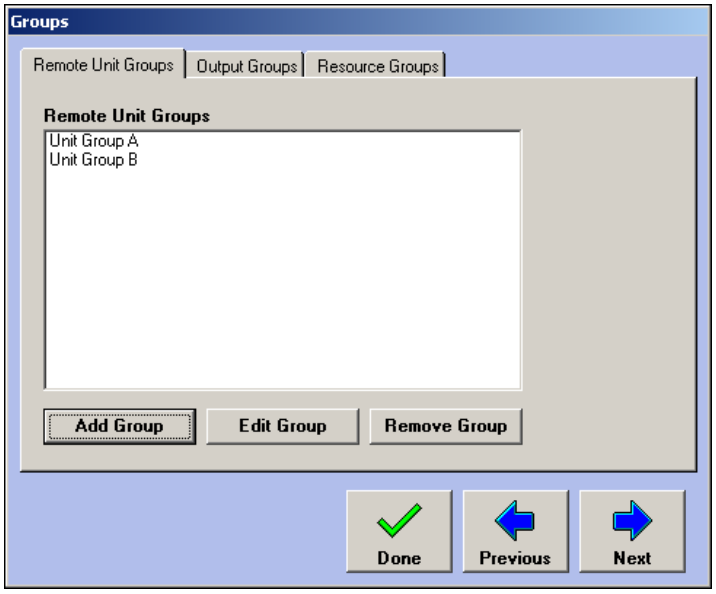
You can communicate with groups of remote units through the D-21 Incident Client, and you can create actions that can send commands to these groups. For instance, you may want to group all fire remote units and then poll them as a group. See "Using Actions" on page 3-27.

Before you begin

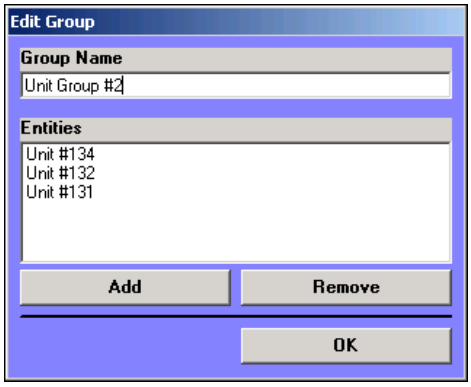
Add all of the remote units that you want to group together. For information on adding remote units, see "Remote Units" on page 2-51.

To create a remote unit group

1 Select **Options > Groups**. The Groups dialog box appears.

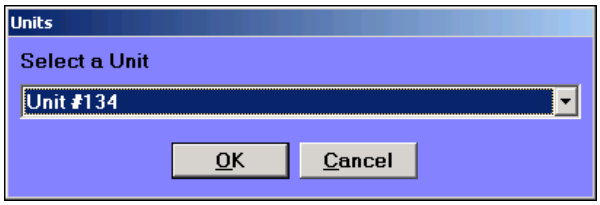


2 Click **Add Group**. The Edit Group dialog box appears.



3 Enter a name in the Group Name box.

4 Click **Add**.



5 Select the remote unit you want to add to the group.

6 Click **OK**. The remote unit appears in the Entities list in the Edit Group dialog box.

7 Repeat these steps for each item you want to add to the group.

8 In the Edit Group dialog box, click **OK**.

9 In the Groups dialog box, click **Done**.

To edit a remote unit group

1 Select **Options > Groups**. If necessary, click the Remote Unit Groups tab.

2 Select the desired group, then click **Edit Group.** The Edit Group dialog box appears.

3 If you want to change the name, edit the text in the Group Name box.

OR

- If you want to add a remote unit, click **Add.** A dialog box appears, from which you can choose the item you want to add to the group. For more information, see "Creating Remote Unit Groups" on page 2-62.

OR

- If you want to remove an item from the group, select it and click **Remove**.

4 In the Edit Group dialog box, click **OK**.

5 In the Groups dialog box, click **Done**.

To remove a remote unit group

1 Select **Options > Groups**. If necessary, click the Remote Unit Groups tab.

2 Select the desired group, then click **Remove Group.** A message asks you to confirm that you want to delete the group.

3 Click **Yes**.

4 In the Groups dialog box, click **Done**.

Zones

Use the Add New Zone dialog box to add and configure the zones attached to a remote unit. To report status to the D-21, each zone input must be entered into the D-21 database.

Zone Class

Each zone has a class. Class is used throughout the D-21 to categorize remote units, zones, outputs, and incidents.

Zone Class	Description
Fire	Fire zones report Alarm, Trouble, and Normal status to the D-21 Incident Client, and you can view their status in the Fire Status View. Incidents created from Fire alarms or troubles are classed as Fire by default.
Security	Security zones report Alarm, Access, and Secure status to the D-21 Incident Client, and you can view their status in the Security Status View. Incidents created from Security alarms are classed as Security by default.
EMS	The EMS class is a subset of the Fire class. An EMS zone reports Alarm, Trouble, and Normal status. You can view their status in the Fire Status View. Incidents created from EMS zone alarms or troubles are classed as EMS by default. The Emergency Medical Dispatch Guide is third-party software that must be purchased separately. When installed with the D-21, the Emergency Medical Dispatch Guide is available whenever you are working with EMS incidents.
Aircraft	The Aircraft class is a subset of the Fire class. An Aircraft zone reports Alarm, Trouble, and Normal status. You can view their status in the Fire Status View. Incidents created from Aircraft zone alarms or troubles are classed as Aircraft by default. The index of aircraft diagrams is available whenever you are working with Aircraft incidents.
HazMat	The HazMat class is a subset of the Fire class. A HazMat zone reports Alarm, Trouble, and Normal status. You can view their status in the Fire Status View. Incidents created from HazMat zone alarms or troubles are classed as HazMat by default. The HazMat guide is available whenever you are working with HazMat incidents.
Fire Auxiliary	Use Fire Auxiliary zones to report the status of zones that monitor Fire system equipment. A Fire Auxiliary zone reports Alarm, Trouble, and Normal status conditions.
Security Auxiliary	Use Security Auxiliary zones to report the status of zones that monitor Security system equipment. A Security Auxiliary zone reports Alarm, Tamper, and Normal status conditions.

A D-21 workstation only displays zones that match the class of the clients enabled on that workstation. For example, in a D-21 workstation that has Fire, Security, and Facility Management Clients installed shows all remote units, zones, and incidents on all workstations regardless of their class. A Fire-only workstation shows units, zones, and incidents classified as Fire. For more information on configuring workstations, see “Setting Workstation Options” on page 4-49.

Zone Priority

Zone priority determines the order in which a buffered alert is presented to the operator by the D-21 Incident Client.

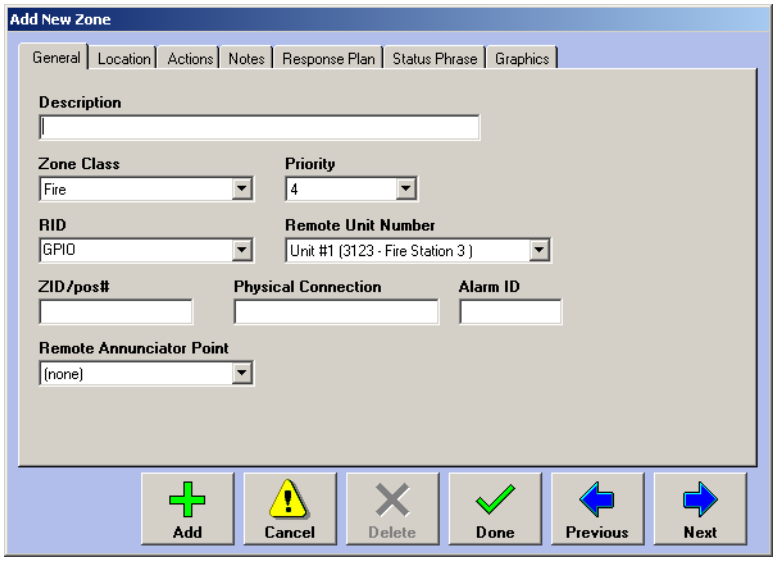
Priority	Description
1–8	Numbered rankings that determine the order in which alarms are displayed at the D-21 Incident Client. For example, alerts with a priority of 1 are presented before alerts with a priority of 2, even if the priority 2 alerts occurred before to the priority 1 alerts.
Supervisory	Zones assigned a Supervisory priority report alarms to the D-21 Incident Client as supervisory alarms, which are prioritized lower than alarms from zones that are ranked 1-8.
Trouble	Zones assigned a Trouble priority report alarms to the D-21 Incident Client as non-alarm troubles. The Trouble priority is not available for Security zones.
No Alert	This zone priority is only available for Fire and Security Auxiliary class zones. Alarms occurring on zones assigned with a No Alert priority are not displayed at the D-21 Incident Client, but the zone status changes are recorded in the D-21 log as Supervisory zone events.
No Log	This zone priority is only available for Fire and Security Auxiliary class zones. Alarms occurring on zones assigned with a No Log priority are not displayed at the D-21 Incident Client and the zone status changes are not recorded in the D-21 log. All events from zones that are assigned the No Log priority are handled by the D-21 as Supervisory zone events.
Log MNS Alarms	This zone priority is only available for Fire Auxiliary zone classes. It controls the alert behavior of MNS monitoring zones. During an alarm event or a normal event no alert will be displayed, but the event will be logged. During a trouble event an alert will be displayed and the event will be logged.

Before you begin

Be sure you have added the RID and remote unit to which the zone is attached before attempting to add the zone to the database. See "Remote Interface Drivers (RIDs)" on page 2-30 and "Remote Units" on page 2-51 for more information.

To add a zone

1 Select **Add > Zone**.



2 Enter descriptive information about the zone in the Description box. The description identifies the zone throughout the D-21 system.

3 Select a Zone Class from the drop-down list. See "Zone Class" on page 2-64.

4 Select a Priority from the drop-down list. See "Zone Priority" on page 2-65.

5 Select the RID from the drop-down list.

6 Select the Remote Unit Number from the drop-down list. Only remote units associated with the selected RID appear in the drop-down list.

7 Enter the zone position number by doing one of the following:

- If the unit is attached to an RFM 5000, enter a ZID or ZID position number. This is the number the system uses to identify the source of an alert associated with a zone. The ZID number must be a number between 0 and 9999 and unique to the RFM.

OR

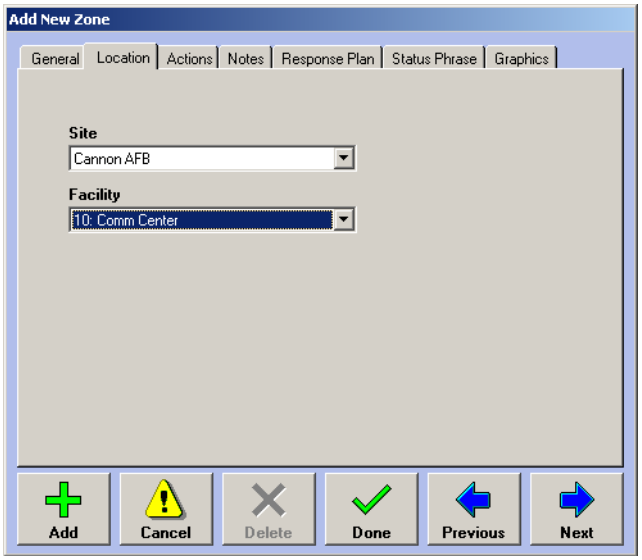
- If the zone is associated with an RFM 7000, enter the Logical Position number. This is the number of the remote unit terminal to which the zone is connected.

8 Enter a description of the zone's physical connection in the Physical Connection box, if desired. This textbox is for informational purposes only.

NOTE *The Alarm ID option is used for communication with 3rd-party equipment.*

9 If the zone will be attached to a remote annunciator, enter the point name in the Remote Annunciator Point box. See the D-21 Remote Interface Driver Guide (P/N 001-399-01) for more information.

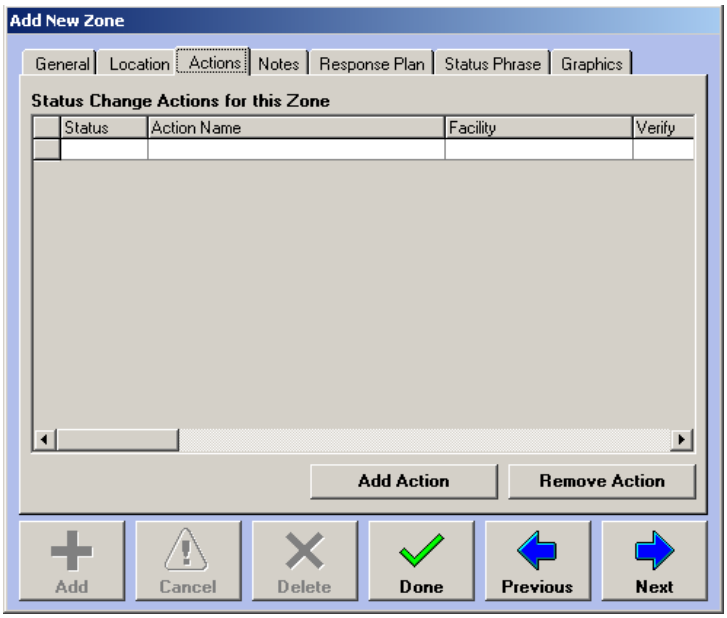
10 Click Next to advance to the Location tab



11 Select the site and the facility where the zone is located.

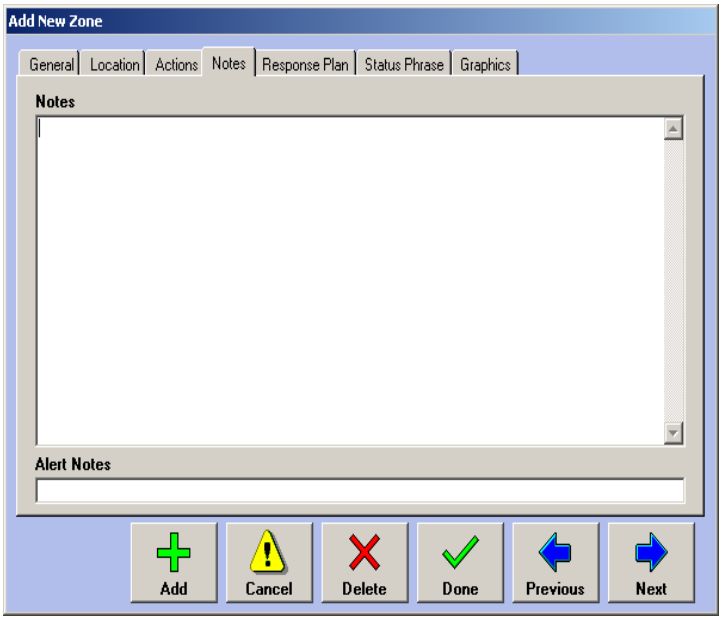
NOTE *If the desired facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See "To add a facility" on page 2-13.*

12 Click **Next** to advance to the Actions tab.



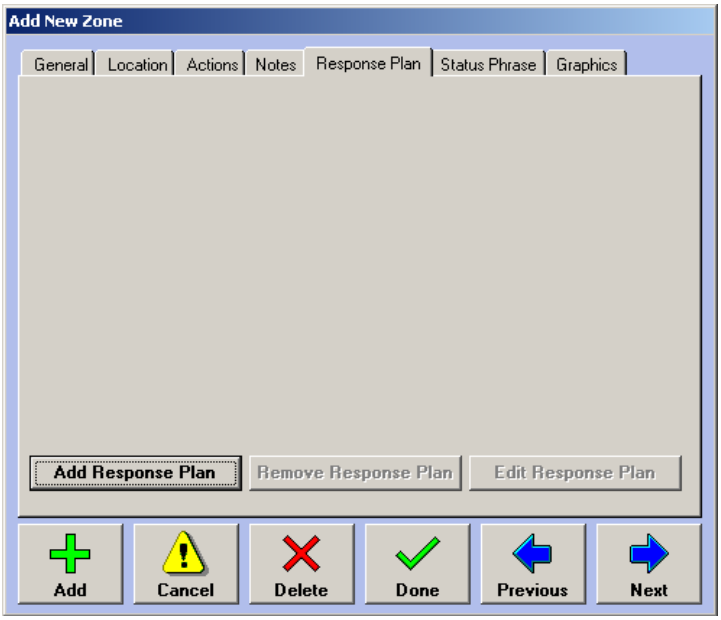
13 Click **Add Action** if you want an action to run when this zone changes status. For information on adding status change actions, see "Attaching Actions to Status Changes" on page 3-37.

14 Click **Next** to advance to the Notes tab.



15 Enter the desired text in the Notes and Alert Notes text box. Monaco recommends entering the Notes information operators may need when handling an incident related to this zone, such as remote unit information, location details, water supply locations, etc. The Alert Notes is a short (40 characters) text box for information that is particularly essential for operators to know in the event of an alert on this zone. For Hot Zones, the Alert Notes text box is pre-populated with 'Hot Zone'.

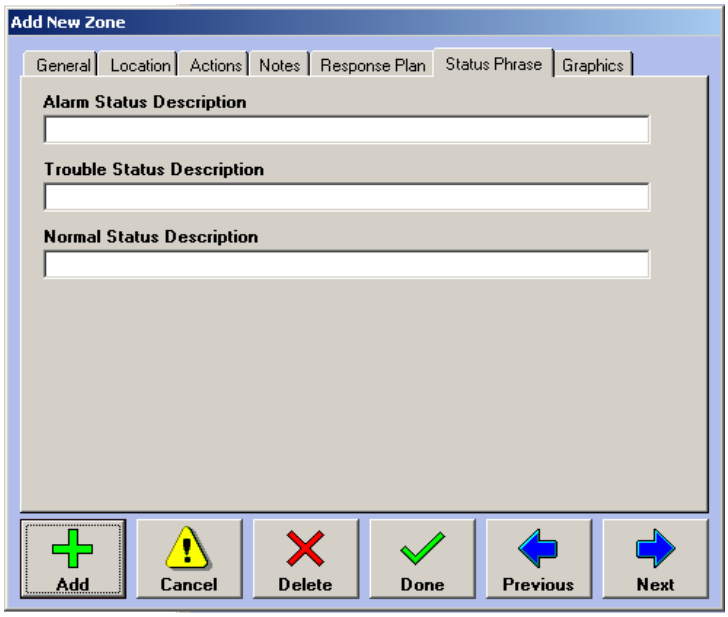
16 Click **Next** to advance to the Response Plan tab.



17 Click **Add Response Plan** to enter the Response dialog box for this zone. For information on adding response plans to a zone, see "Response Plans" on page 3-2.

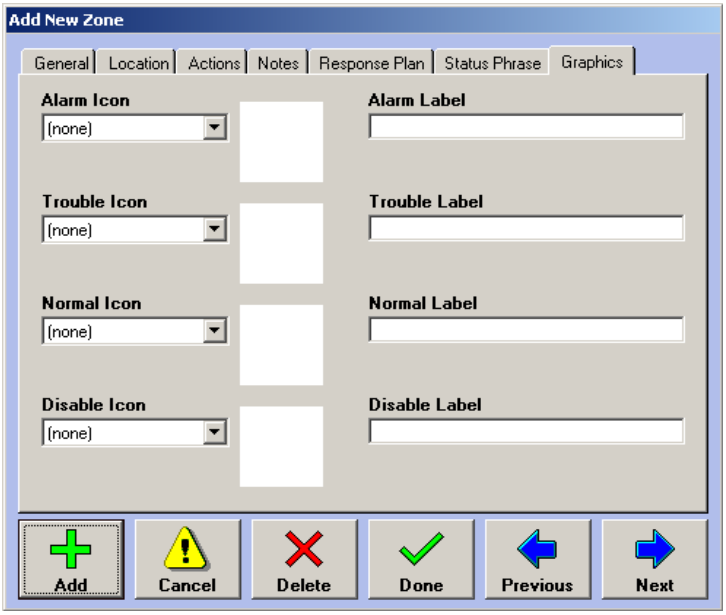
NOTE *You can only add one response plan to a zone. Once the zone has a response plan, the Add Response Plan button is dimmed, and the Remove Response Plan and Edit Response Plan buttons are enabled.*

18 Click **Next** to advance to the Status Phrase tab.



19 Enter the status description you want to appear when alerts for the new zone are sent to the D-21 Incident Client.

20 Click Next to move to the Graphics tab.



21 Use the drop-down lists to select an icon for each condition (Alarm, Trouble, Normal, and Disable) and give it a label. Icon graphics must be saved in the folder `C:\Program Files\D21\Media\Icons`

NOTE *If you want to add an icon and/or label representing this zone to the facility's floor plan, you must fill in the Graphics tab.*

22 Click **Done** to add the new zone to the database.

To edit a zone

1 In the tree pane, click the plus sign (+) next to the RID and then click the plus sign (+) next to the unit that contains the zone you want to edit.

2 Right-click the zone you want to edit. The Zone dialog box appears.

3 Change dialog box entries and selections as desired. For more information on the tabs, boxes, and drop-down lists, see "To add a zone" on page 2-65.

To delete a zone

1 In the tree pane, click the plus sign (+) next to the RID and then click the plus sign (+) next to the unit that contains the zone you want to delete.

2 Right-click the zone you want to delete. The Zone dialog box appears.

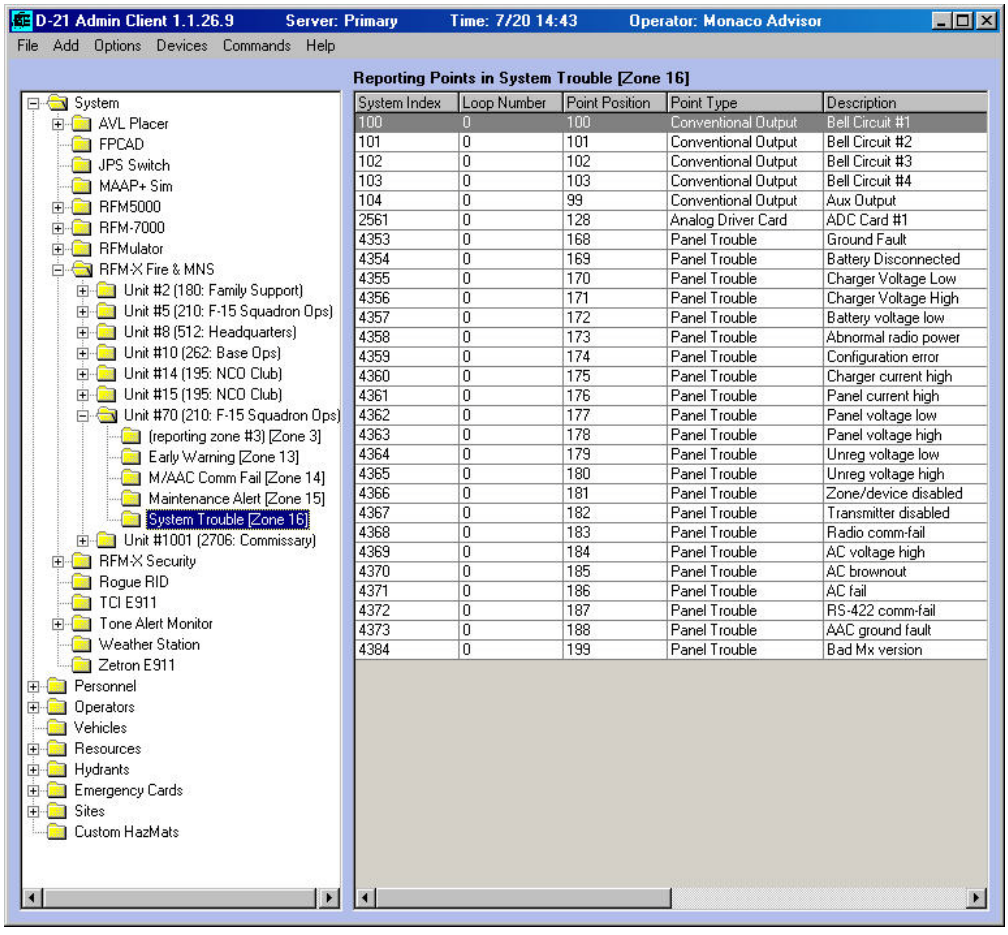
3 Click **Delete.** A confirmation message appears.

4 Click **Yes**.

Point Reporting Zones

If the D-21 system includes one or more MAAP(+) remote units with point reporting enabled, then the zones for those units will be associated in the D-21 database with individual detectors, or *points*. These zones cannot be manually added to the database in the D-21 Admin Client in the way described previously. Instead, the entire configuration of the MAAP(+) remote unit must be imported. Consult the Monaco Addressable Plus Planner Guide (P/N 001-359-01) for instructions on the MAAP(+) import process.

Once the import has been completed, the properties of individual points can be accessed in the D-21 Admin Client system tree by selecting the point reporting zone.



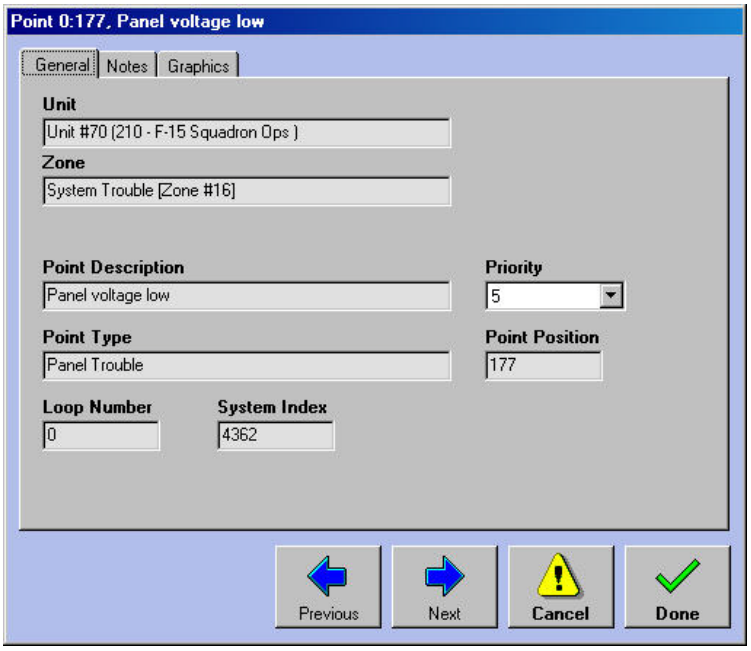
System Index	Loop Number	Point Position	Point Type	Description
100	0	100	Conventional Output	Bell Circuit #1
101	0	101	Conventional Output	Bell Circuit #2
102	0	102	Conventional Output	Bell Circuit #3
103	0	103	Conventional Output	Bell Circuit #4
104	0	99	Conventional Output	Aux Output
2561	0	128	Analog Driver Card	ADC Card #1
4353	0	168	Panel Trouble	Ground Fault
4354	0	169	Panel Trouble	Battery Disconnected
4355	0	170	Panel Trouble	Charger Voltage Low
4356	0	171	Panel Trouble	Charger Voltage High
4357	0	172	Panel Trouble	Battery voltage low
4358	0	173	Panel Trouble	Abnormal radio power
4359	0	174	Panel Trouble	Configuration error
4360	0	175	Panel Trouble	Charger current high
4361	0	176	Panel Trouble	Panel current high
4362	0	177	Panel Trouble	Panel voltage low
4363	0	178	Panel Trouble	Panel voltage high
4364	0	179	Panel Trouble	Unreg voltage low
4365	0	180	Panel Trouble	Unreg voltage high
4366	0	181	Panel Trouble	Zone/device disabled
4367	0	182	Panel Trouble	Transmitter disabled
4368	0	183	Panel Trouble	Radio comm-fail
4369	0	184	Panel Trouble	AC voltage high
4370	0	185	Panel Trouble	AC brownout
4371	0	186	Panel Trouble	AC fail
4372	0	187	Panel Trouble	RS-422 comm-fail
4373	0	188	Panel Trouble	AAC ground fault
4384	0	199	Panel Trouble	Bad Mx version

When a point reporting zone is selected in the left pane, the right pane displays the points that report via the zone in a grid in the right pane, as shown in the figure above. To view the properties of an individual point, double-click it in the right pane grid.

To view point properties

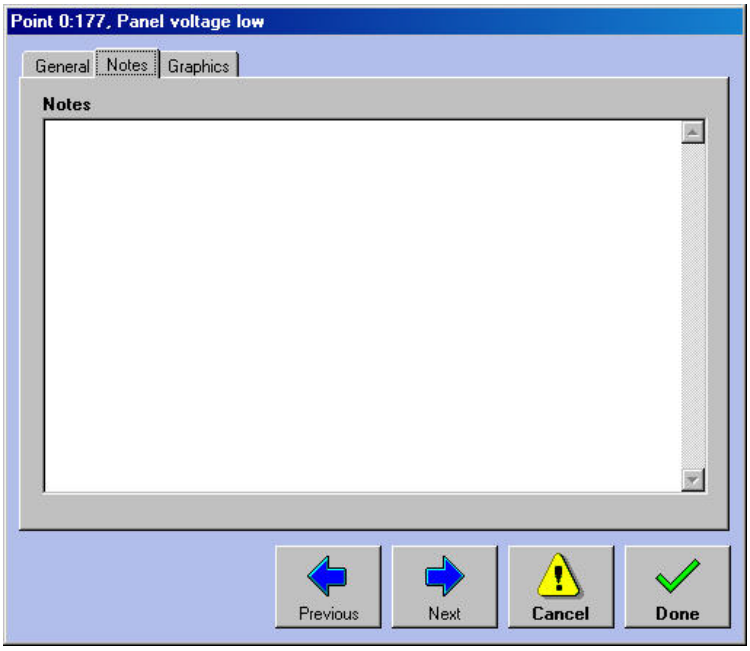
1 Select the point reporting zone in the system tree. The zone's points are displayed in the grid in the right pane.

2 Double-click the desired point in the grid in the right pane. The Point dialog box opens with the General tab displayed.



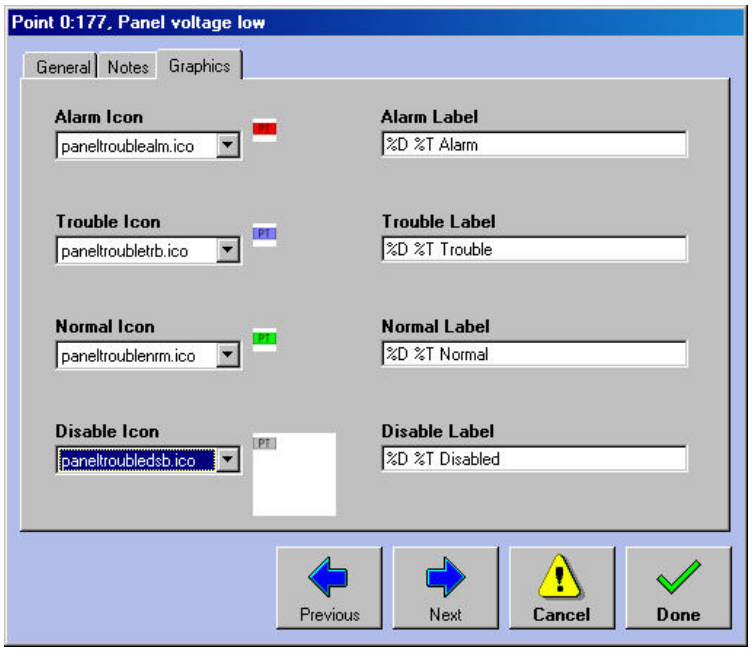
3 The point's **Priority** can be modified by selecting it from the drop-down list, while all other values on the General tab are set through the import process.

4 Click the Notes tab.



5 Enter additional information in the **Notes** text box as desired. This information will be displayed in the D-21 Incident Client's Device Status viewer for the point.

6 Click the Graphics tab.



7 During the import process, icons and labels can be automatically assigned for display on floor plans, and icons and labels can be modified on the Graphics tab. The '%D %T' notation in the labels signifies the date and time of the last status update received from the point will be included in the label.

Outputs

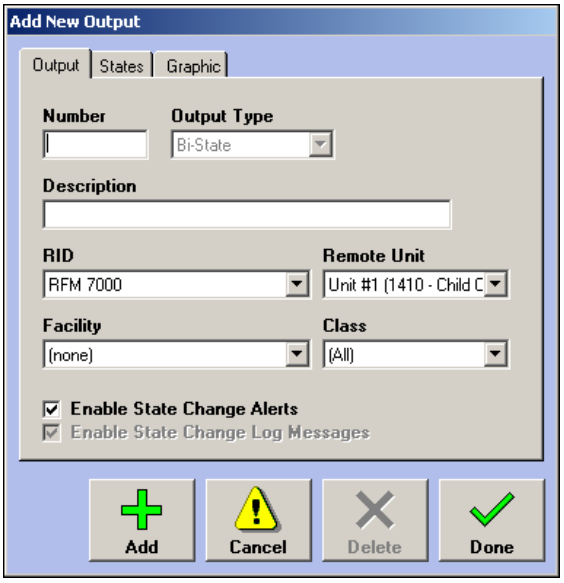
Outputs are used in the D-21 database to represent the relays connected to remote units to provide control of auxiliary devices, such as door releases or emergency lights. The D-21 can control relays connected to the following types of remote units:

- **Building Transceivers (BTs) and Fire Alarm Control Panels (FACPs)** The number and type of outputs available depends on the type of remote unit and expansion options that have been installed. See the documentation provided with the equipment for relay specifications.
- **D-21 Automatic Control Output Panel** Up to fourteen output relays can be controlled from each D-21 Output Panel. The relays on the D-21 Output Panel can be configured as bi-state (on/off) or momentary (on). The NCD RID must be configured before you can add the remote unit and outputs to the D-21 database. See the D-21 Remote Interface Driver Guide (P/N 001-399-01).
- **D-21 General Purpose Input/Output (GPIO) Zone Cards** GPIO Zone Cards communicate directly with the D-21 via the COM port on the back of the D-21 server or through a network connection. The GPIO Zone Cards can be configured for standard zone monitoring, feedback reporting, or relay outputs. The GPIO RID must be configured before you can add the remote unit and outputs to the D-21 database. See the D-21 Remote Interface Driver Guide (P/N 001-399-01).

Outputs can also be grouped according to location or type, placed on graphics (D-21G or D-21M required), and activated and deactivated from the D-21 Incident Client. When you are finished adding individual outputs, see "Creating Output Groups" on page 2-78 for more information.

To add an output

1 Select **Add > Output**.



2 Select the appropriate RID and Remote Unit from the drop-down lists.

3 Enter the output number in the Number box. For the onboard remote signal activation (RSA) relay output on a Monaco remote unit, enter 0 (zero). For other kinds of outputs, consult the documentation for the remote unit to determine the output number.

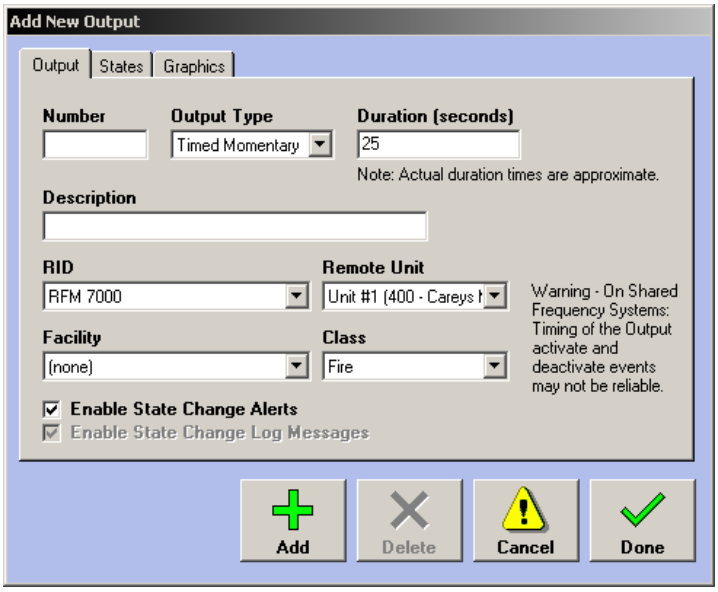
NOTE *RSA is available only on BT2-3, BT2-4, BT2-7, and BT2-8 transceivers; M-1 and M-2 Fire Alarm Control Panels, and General Purpose Input/Output (GPIO) Zone Card panels.*

4 Specify the output type:

- **Bi-State** A bi-state output toggles between powered and unpowered. This output type is available with the BT2-7 and BT-X transceivers, the D-21 Automatic Output Control Panel, and GPIO Zone Cards. Bi-state outputs report Off and On status to the D-21 Incident Client.
- **Momentary/Timed Momentary** A momentary output activates a relay for a configurable and brief period (typically 25 seconds). Momentary outputs report Inactive and Activated status to the D-21 Incident Client.

NOTE *The momentary output type is required for RSA outputs.*

5 If you specified the Momentary type, the Duration box appears and RSA relays default to 25 seconds and cannot be changed. Other momentary outputs, such as those that control the relays on the D-21 Control Output Panel, can use durations that range from 1 to 254 seconds. Depending on the remote unit type, advisory messages about output duration may appear on the dialog box.



6 Enter a description in the Description box. Without a meaningful description, it is difficult to distinguish among outputs, especially if your system has many outputs or outputs that are launched automatically.

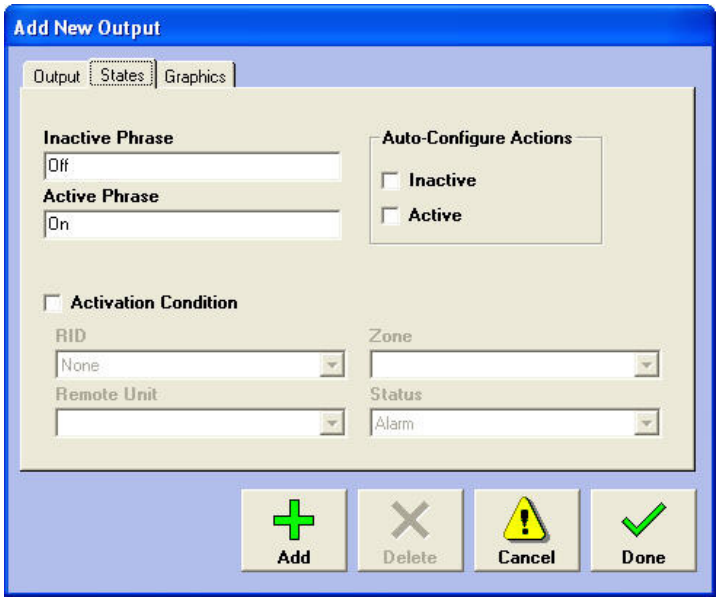
7 Select Fire, Facility Management, Security, or any combination of the three, in the Class list, depending on the operation the output performs.

- **Fire** Output commands can be issued on workstations where the Fire Client is enabled by operators with Fire permissions.
- **Facility Management** Output commands can be issued on workstations where the Facility Management Client is enabled by operators with Facility Management permissions.
- **Security** Output commands can be issued on workstations where the Security Client is enabled by operators with Security permissions.

8 Specify how you want the D-21 to process the output's status changes.

- **Display alerts and log activity** If you want the D-21 to display an alert when the output's status changes, select the Enable Status Change Alerts option. When this option is selected, status changes are also entered in the log.
- **Do not display alerts but log activity** If you do not want status change alerts but want the D-21 to record the status change in the log, clear the Enable Status Change Alerts check box and select the Enable State Change Log Messages option.
- **Do not display alerts and do not log activity** If you do not want to receive alerts for the output and you do not want the D-21 to log the status changes, clear both check boxes.

9 Click the States tab.



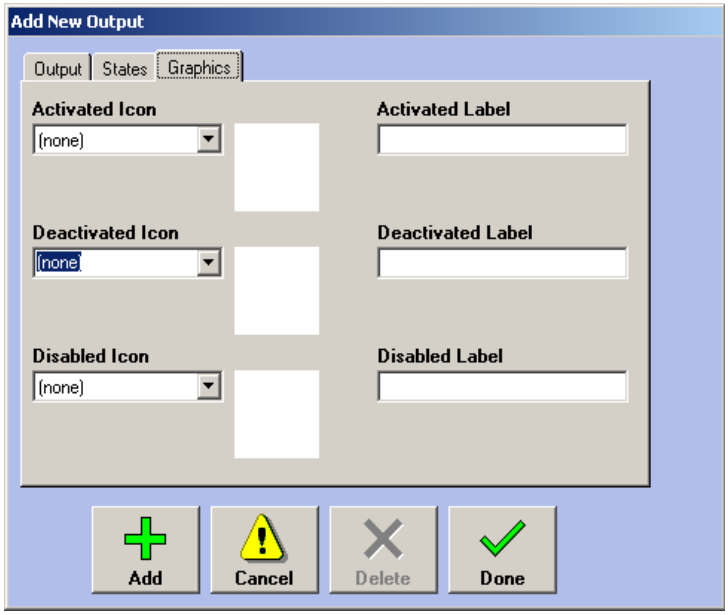
- **Inactive Phrase** Enter custom text for the inactive state of the output. The D-21 uses these phrases when displaying the status of the output in the D-21 Incident Client.
- **Active Phrase** Enter custom text for the active state of the output. The default phrase for bi-state outputs is "On." The default phrase for momentary outputs is "Activated."

- **Auto Configure Actions** Select the check boxes for the output actions you want the D-21 to create. For example, clicking the Active check box creates an action for activating the output. This action can then be assigned to status change actions for RIDs, remote units, and zones throughout the D-21. When you auto-configure an action for an output, the D-21 names the action using the following format:

  `UnitNumber Description OutputNumber Phrase`

  For more information on using actions, see "Actions" on page 3-27.
- **Activation Condition** Check this box to define a zone status which will automatically activate this output. Once this box is checked, the **RID**, **Remote Unit**, **Zone**, and **Status** drop-down lists are enabled, allowing you to define the activation condition.

10 Click the Graphic tab.



11 If the output will be placed on a floor plan or used in an output group in the D-21 Incident Client, type a caption for the label and select a graphic in the Icon drop-down list for each of the output's possible states. For more information, see "Creating Output Groups" on page 2-78.

NOTE *If you want to add an icon and/or label representing this output to the facility's floor plan, you must fill in the Graphics tab.*

12 Click **Done**.

To edit an output

1 In the tree pane, click the plus sign (+) next to the RID and then click the plus sign (+) next to the unit that contains the output you want to edit.

2 Right-click the output you want to edit. The Output dialog box appears.

3 Change dialog box entries and selections as desired. For more information on the boxes and drop-down lists, see "To add an output" on page 2-74.

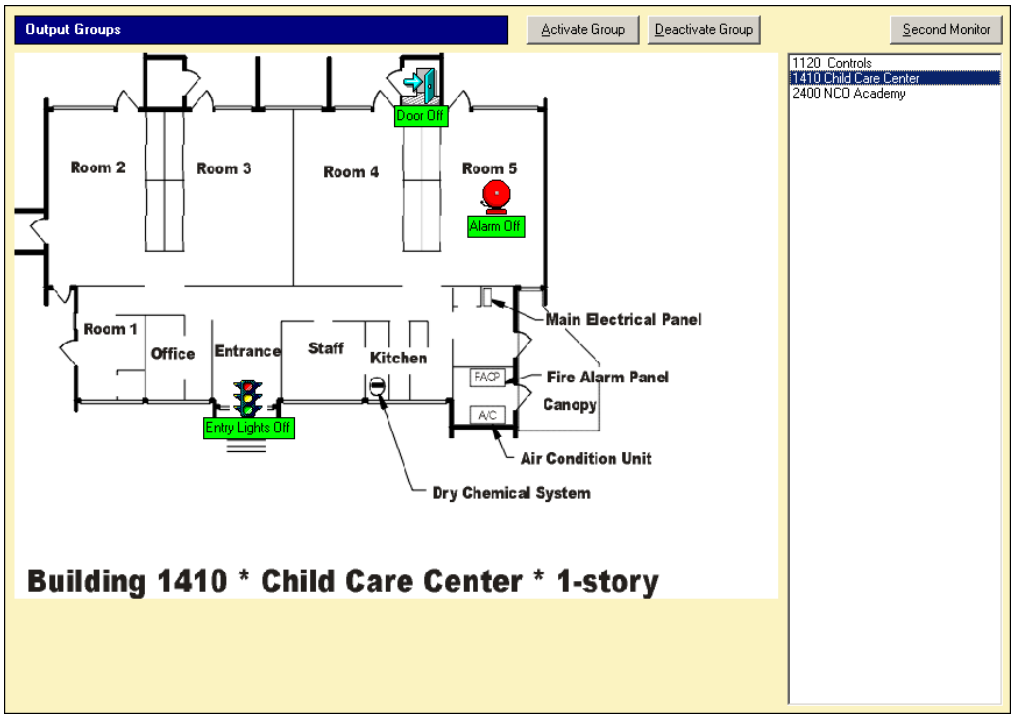
To delete an output

1. In the tree pane, click the plus sign (+) next to the RID and then click the plus sign (+) next to the unit that contains the output you want to edit.
2. Right-click the output you want to edit. The Output dialog box appears.
3. Click **Delete**. A confirmation message appears.
4. Click **Yes**.

Creating Output Groups

Outputs attached to different remote units can be grouped together to make it easier to turn them on and off and view their status in the D-21 Incident Client. For example, you can put all of the gates on a site in the same group and then raise, lower, and monitor their status from a single window in the D-21 Incident Client. With the graphics and map versions of the D-21 (D-21G and D-21M), you can place the output icons on a graphic, usually a floor plan or other line drawing of one or more facilities.

Figure 2-1
Output group on a floor plan in the D-21 Incident Client



For more information on using output groups, see the D-21 Incident Client User Guide (P/N 001-392-00).

Before you begin

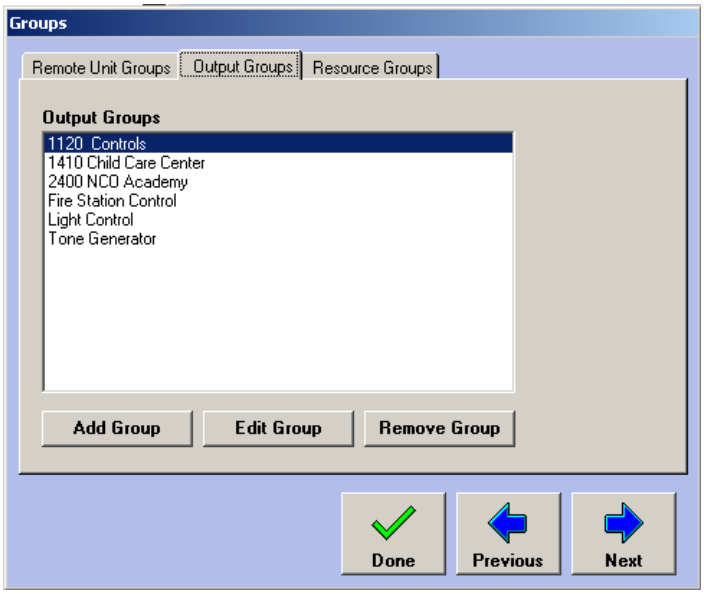
Add the individual relay outputs to the database. See "Outputs" on page 2-74 for more information. Add the floor plans or graphics to the database. See "Floor Plans, Pre-Plans, and Response Graphics" on page 5-3.

To create an output group (D-21)

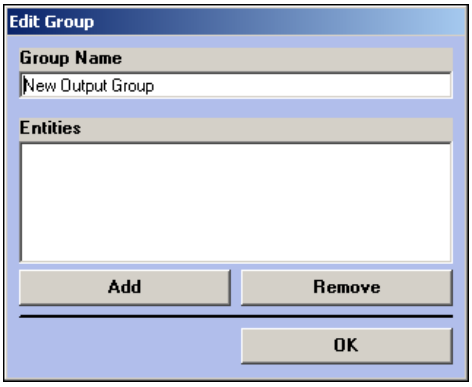
NOTE *The standard D-21 does not support floor plans or graphics. You can activate and deactivate output groups created in the standard D-21 from the Fire Commands pane in the D-21 Incident Client.*

1 Select **Options > Groups**.

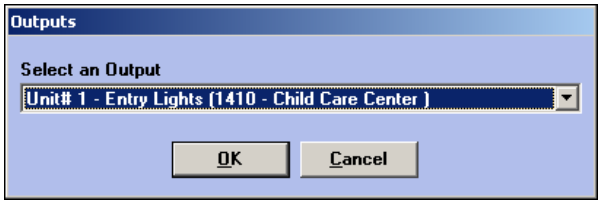
2 Click the Output Groups tab.



3 Click **Add Group**. The Edit Group dialog box appears.



4 Click **Add**. The Outputs dialog box appears.



5 Select an output from the drop-down list. The list displays all outputs that have been added to the D-21 database.

6 Click **OK**.

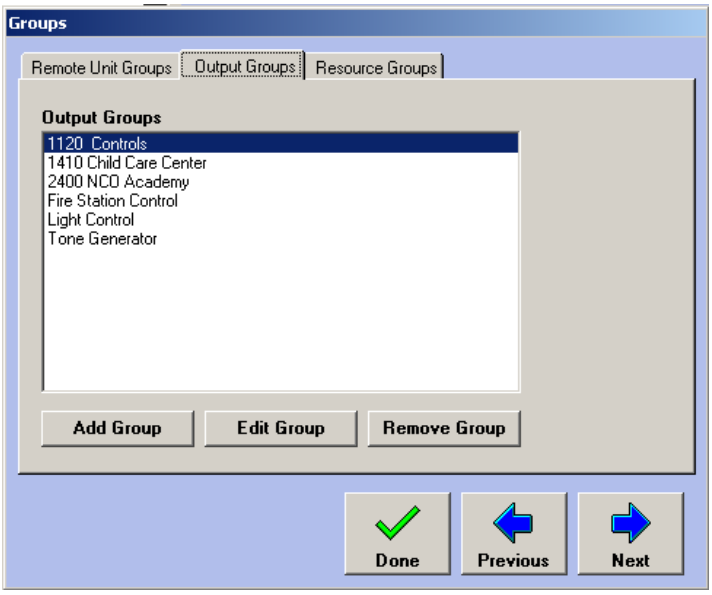
7 Add all the outputs you want to include in the output group.

8 When you are done adding outputs to the group, click **OK** in the Edit Group dialog box.

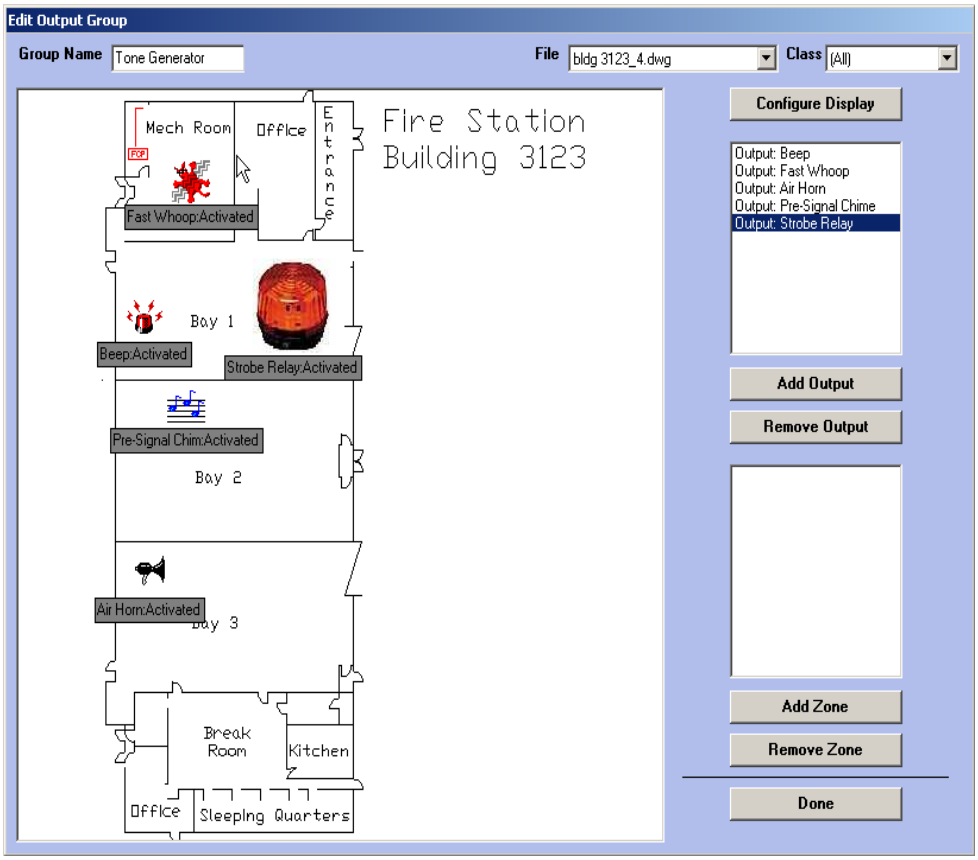
To create an output group (D-21G or D-21M)

1 Select **Options > Groups**.

2 Click the Output Groups tab.



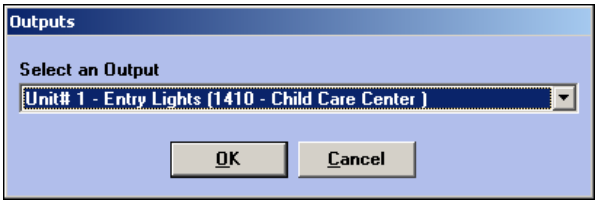
3 Click **Add Group**. The Edit Output Group dialog box appears.



4 Enter a name in the Group Name box. This is the name that identifies the group in Output Groups in the D-21 Incident Client.

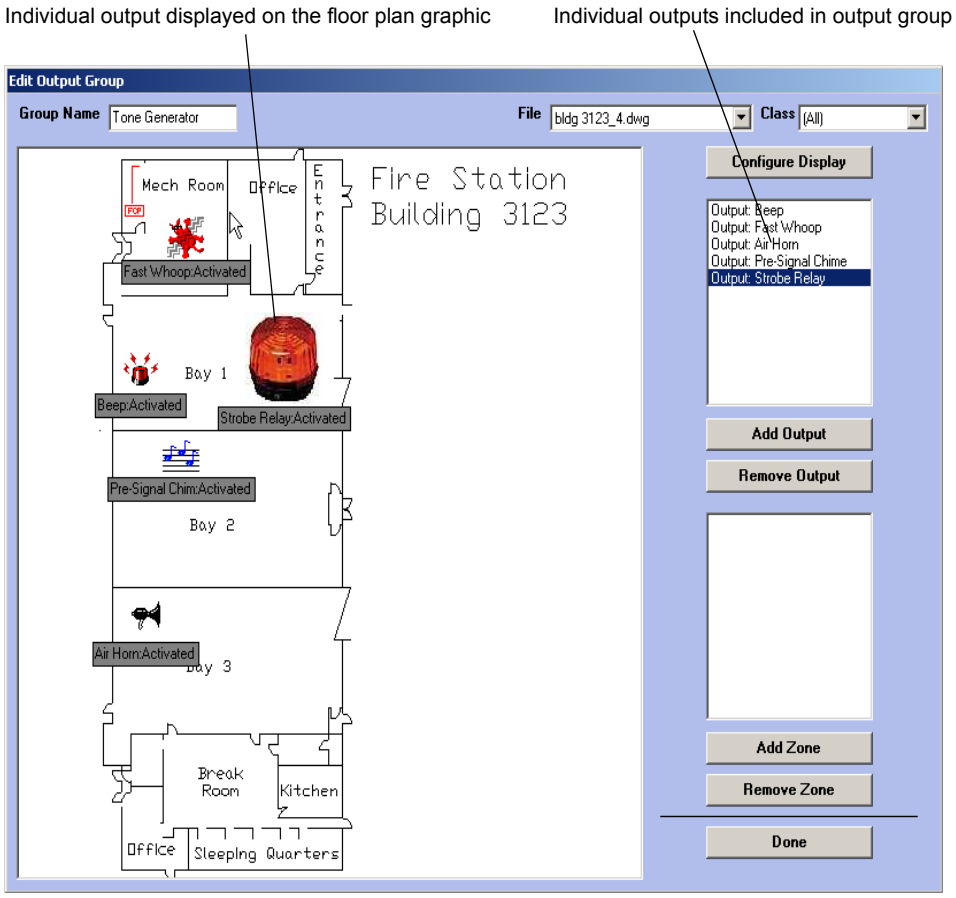
5 Select a floor plan graphic from the file drop-down list.

6 Click **Add Output**. The Outputs dialog box appears.



7 Select the desired output from the drop-down list.

8 Click **OK**. The output icon and icon caption appear on the graphic.

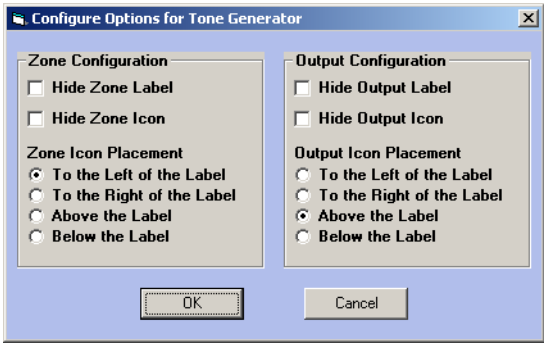


If an icon and caption were not entered in the Graphics tab in the Outputs dialog box, the output will not be displayed on the output group in the Incident Client. See "To add an output" on page 2-74.

9 Position the output icon and caption on the graphic using the mouse.

10 Repeat these steps for each output you want to add to the group.

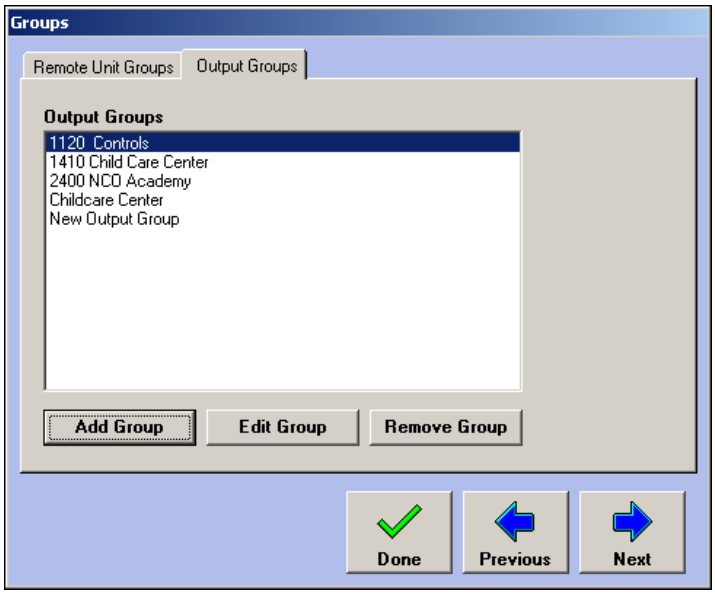
11 Use the Configure Display button to customize how icons and labels for zones and outputs are displayed.



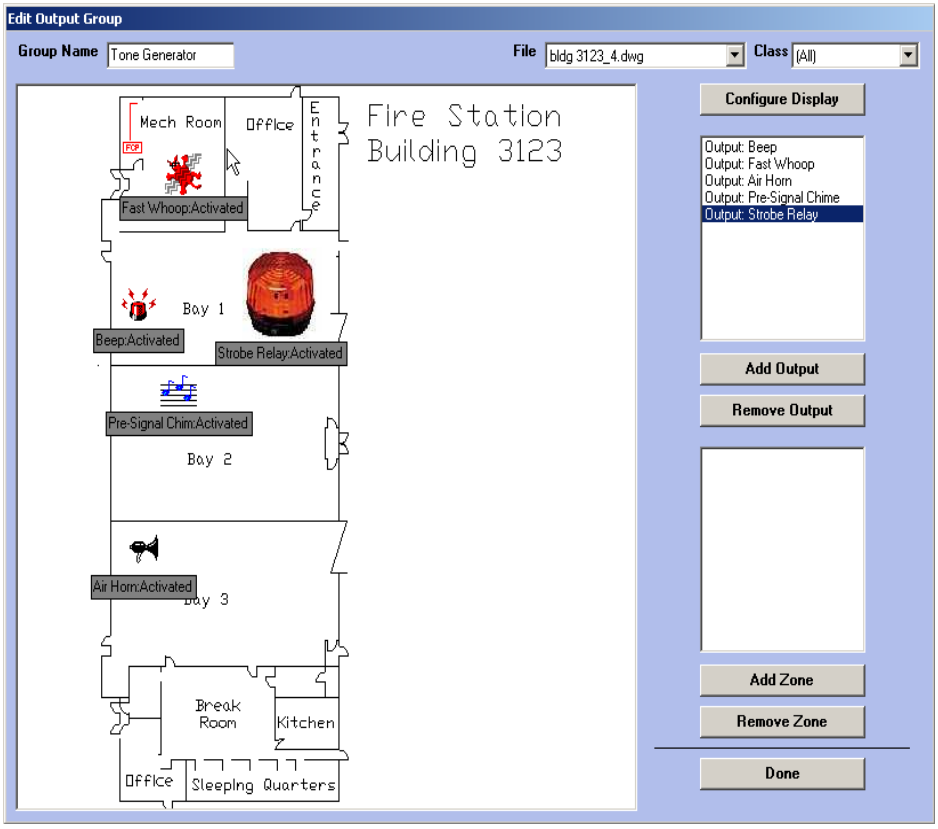
12 When you are finished adding outputs to the graphic, click **Done**.

To add a zone to an output group (D-21G or D-21M)

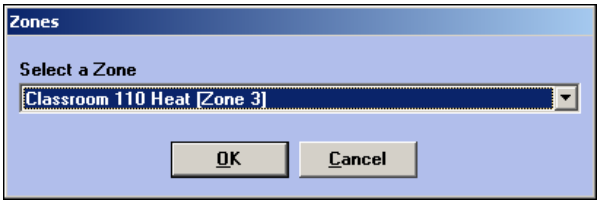
1. Select **Options > Groups**.
2. Click the Output Groups tab.



3. Select the output group to which you want to add a zone.
4. Click **Edit Group**. The Edit Output Group dialog box appears.



5 Click **Add Zone**. The Zones dialog box appears.



6 Select the zone you want to add from the drop-down list. The list includes all zones in the D-21 database.

NOTE *Be sure to select a zone which has been configured with an icon and caption. For more information, see "To add a zone" on page 2-65.*

7 Click **OK**. The zone icon and caption appear on the graphic.

8 Position the zone icon and caption on the graphic using the mouse.

9 Repeat these steps for each zone you want to add to the group.

10 When you are finished adding zones to the graphic, click **Done**.

To edit an output group (D-21G or D-21M)

1 Select **Options > Groups**.

2 Click the Output Groups tab.

3 Select the desired group, then click **Edit Group**. The Edit Group dialog box appears.

4 If you want to change the name, edit the text in the Group Name box.

If you want to add an output, click **Add Output**. A dialog box appears, from which you can choose the item you want to add to the group. For more information, see "Creating Output Groups" on page 2-78.

If you want to remove an item from the group, select it and click **Remove**.

5 In the Edit Group dialog box, click **OK**.

6 In the Groups dialog box, click **Done**.

To remove an output group

1 Select **Options > Groups**.

2 Click the Output Groups tab.

3 Select the desired group, then click **Remove Group**. A message asks you to confirm that you want to delete the group.

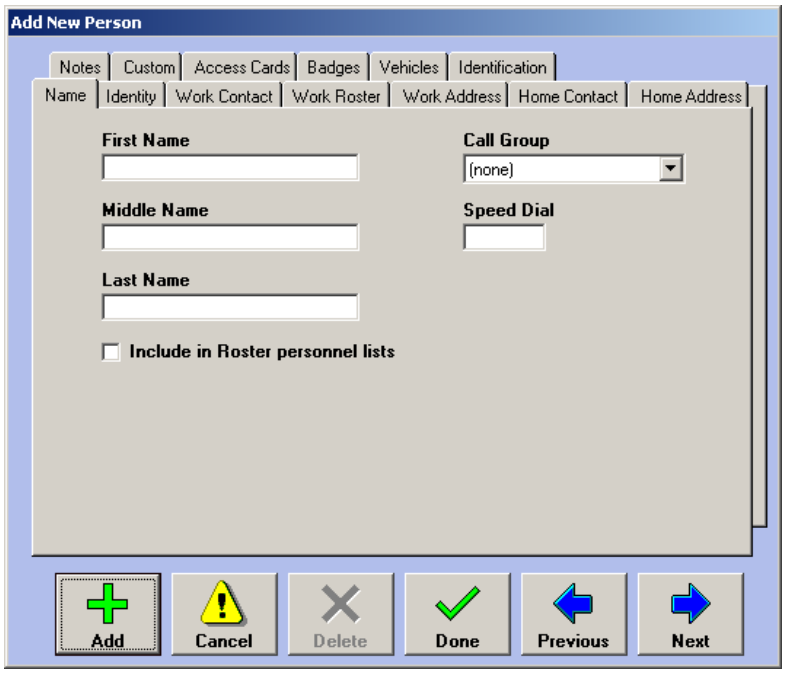
4 Click **Yes**.

5 In the Groups dialog box, click **Done**.

Personnel

Use the Add New Person dialog box to create a record for each person who is a resource, operator, or for whom you need easy access to their contact information. All D-21 Admin Client and D-21 Incident Client operators must be associated with a Person record. Only those people for whom a Person record exists are available in the drop-down lists in the Response and Operator dialog boxes.

Figure 2-2 *Add New Person dialog box*



Before you begin

If the person is associated with a certain facility, be sure to add the facility before adding the person. See "Facilities" on page 2-13. If you use job titles and call groups, add them first so they are available when adding the person. See "Personnel Lists" on page 4-23.

Standard Personnel Information

This section describes how to enter personnel information into the database for a standard D-21 system. For information on custom personnel features, see "Custom Personnel Information" on page 2-93.

To add a person

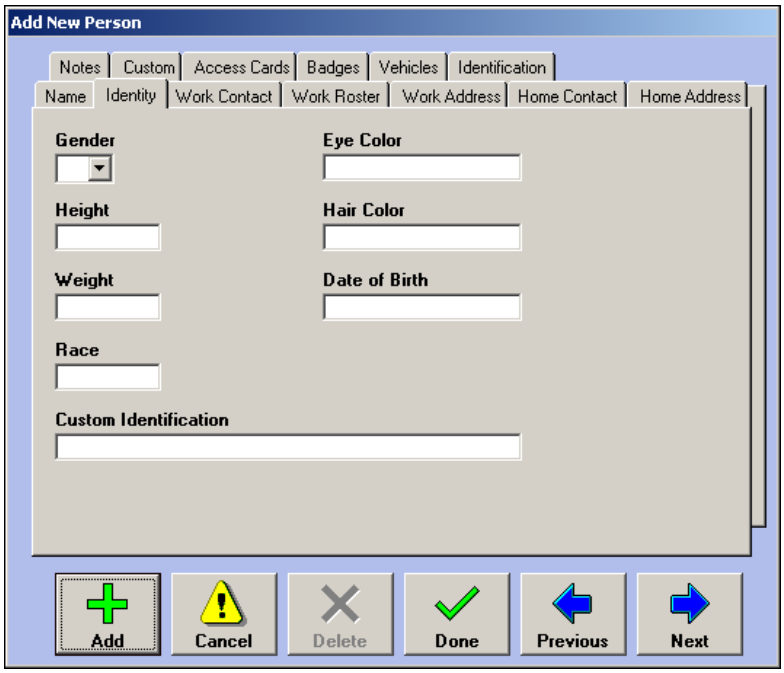
1 Select **Add > Person**.

2 Enter the name in the designated boxes.

NOTE *If the name includes an apostrophe, see "To enter a single quotation mark or apostrophe" on page 1-11.*

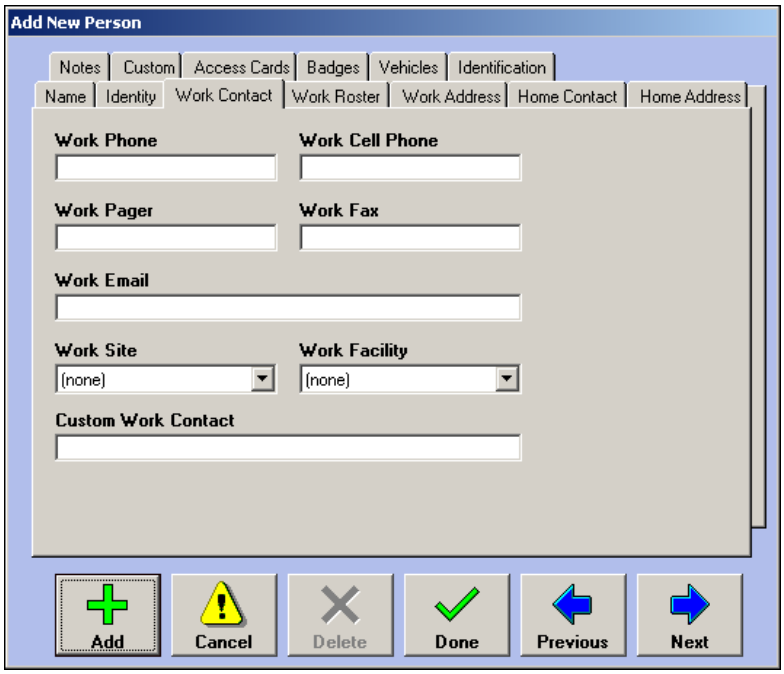
3 Place a checkmark in the Include in Roster personnel lists checkbox if you want the person's name to be available for Roster shift assignments. For more information, see "Creating Rosters" on page 4-38.

4 Click **Next** to advance to the Identity tab.



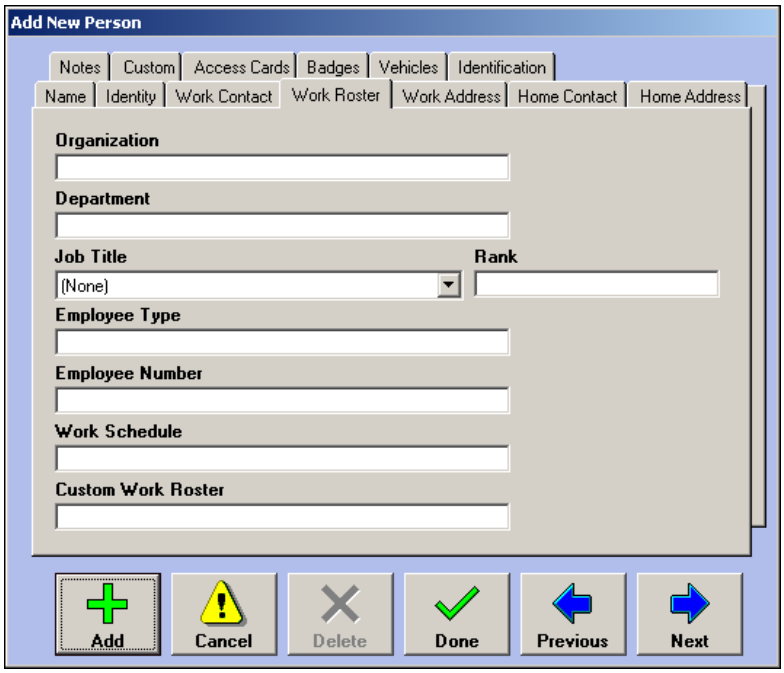
5 Enter the physical characteristics of the new person.

6 Click **Next** to advance to the Work Contact tab.



7 Enter the person's phone, pager, fax, and email information, and choose the site and facility where they work from the drop-down lists.

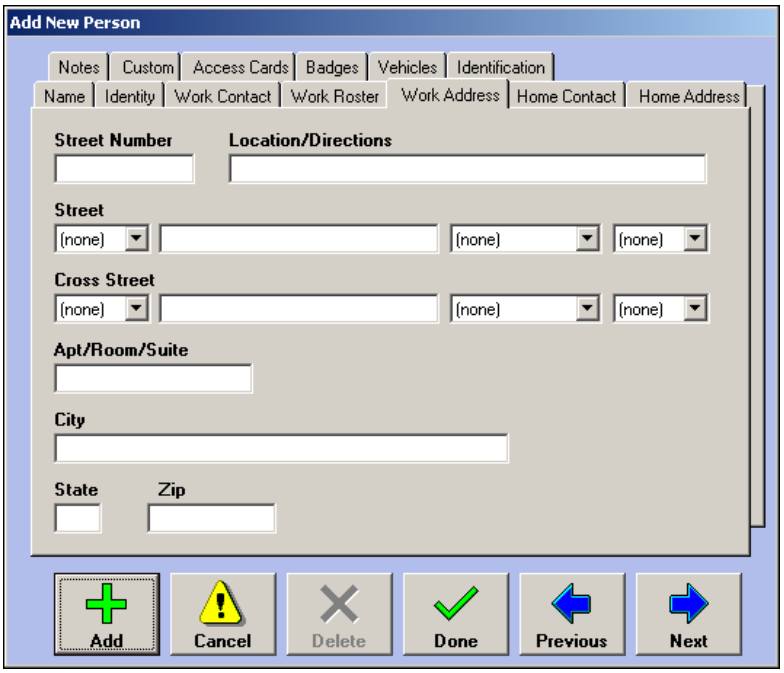
8 Click **Next** to advance to the Work Roster tab.



9 Enter the organization, department, job title and rank, employee type and number, and work schedule information for the new person.

NOTE *You can add to, delete from, and edit the items that appear in the Job Title drop-down list via the Roster tab of the Personnel Lists dialog box. See "Personnel Lists" on page 4-23.*

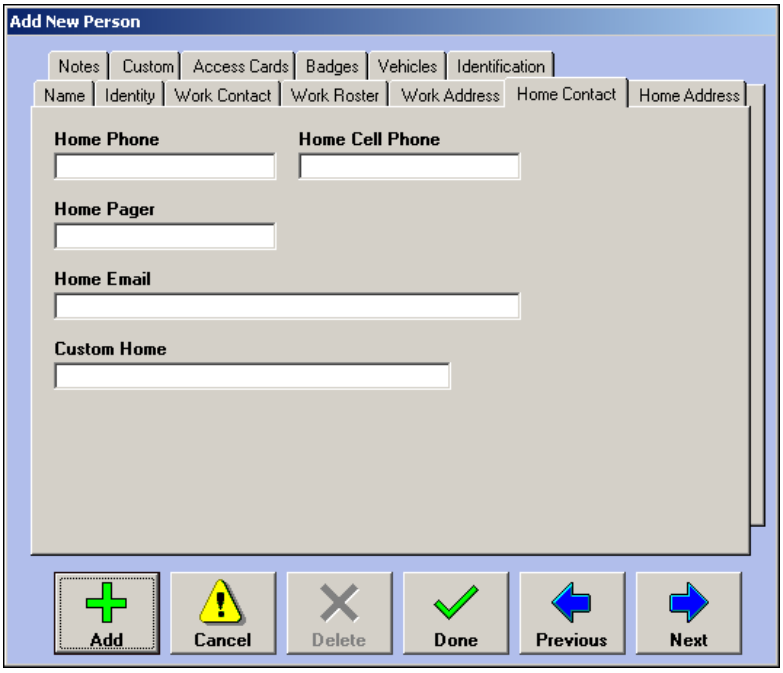
10 Click **Next** to advance to the Work Address tab.



11 Enter the person's work address, choosing the directional prefix/suffix (N, NW, etc.) and street types (Ave, St, etc.) from the drop-down lists.

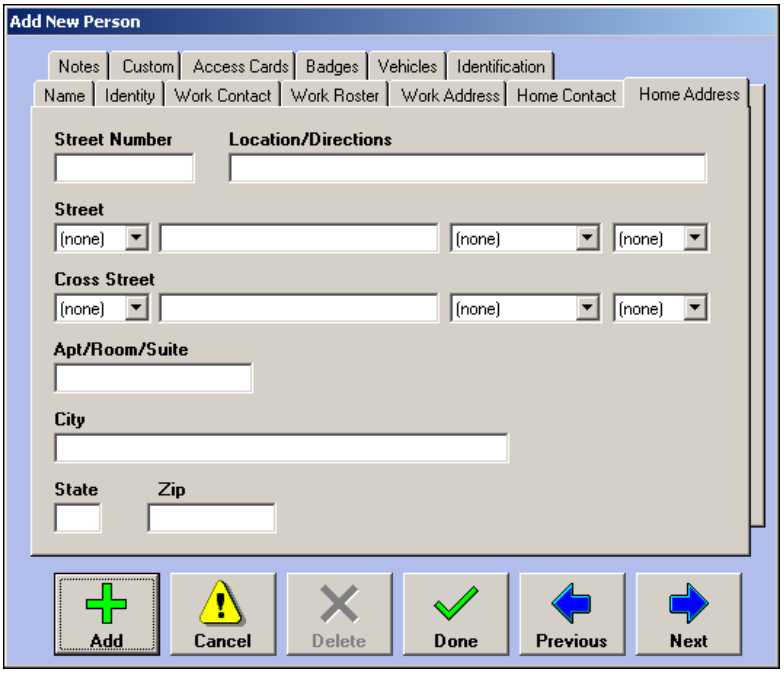
NOTE *You can add to, delete from, and edit the items that appear in the directional prefix/suffix list and street types list in the General Lists dialog box. See* *"Customizing Lists" on page 4-2.*

12 Click **Next** to advance to the Home Contact tab.



13 Enter phone, pager, and email information for the new person.

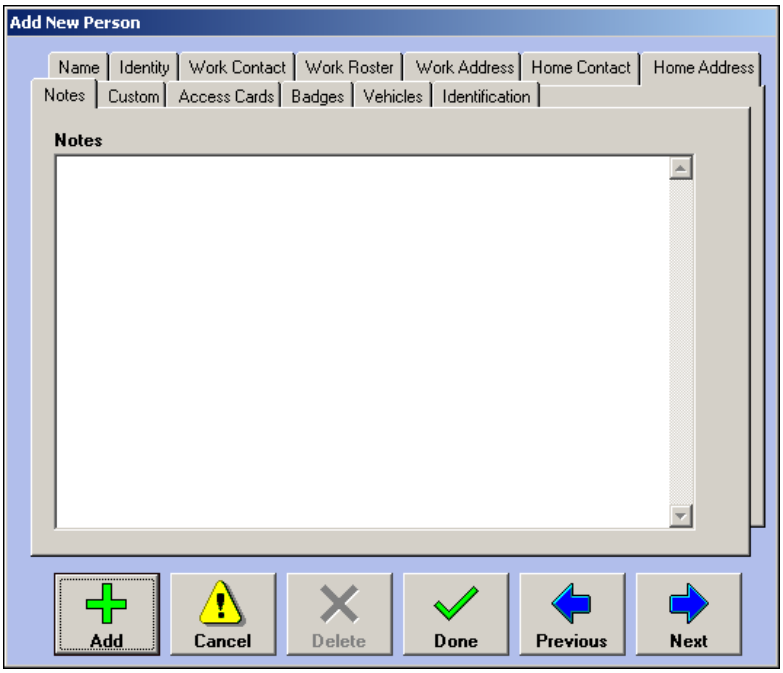
14 Click **Next** to advance to the Home Address tab.



15 Enter the person's home address, choosing the directional prefix/suffix (N, NW, etc.) and street types (Ave, St, etc.) from the drop-down lists.

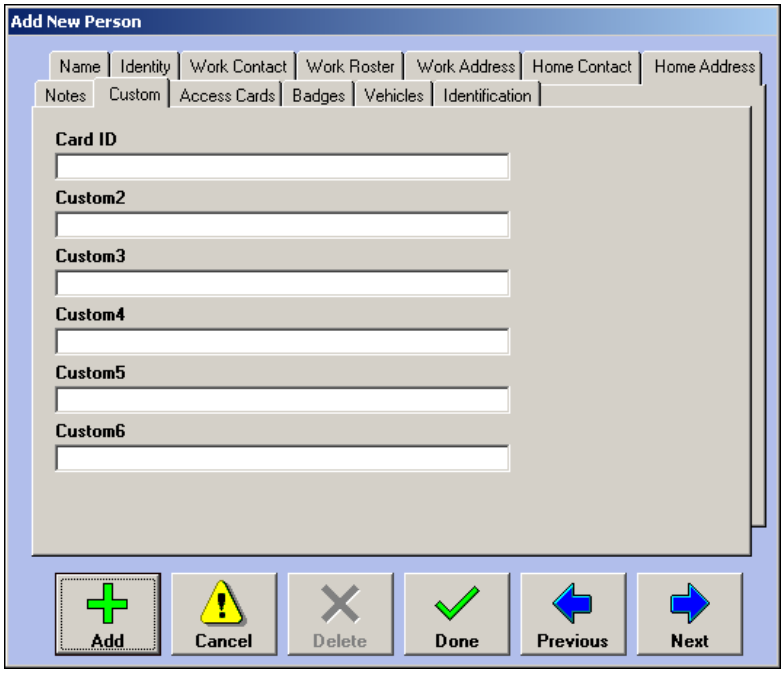
NOTE *You can add to, delete from, and edit the items that appear in the directional prefix/suffix list and street types list in the General Lists dialog box. See "Customizing Lists" on page 4-2.*

16 Click **Next** to advance to the Notes tab.



17 Enter the desired text in the Notes box.

18 Click **Next** to advance to the Custom tab.



19 Use the text boxes in this tab to enter custom personnel information. To add customized personnel fields, see "To create custom personnel fields" on page 4-24.

20 Click **Done**.

To edit a person record

1 In the tree pane, right-click the name of the person whose record you want to edit. The Person dialog box appears.

2 Change dialog box entries and selections as desired. For more information on the boxes and drop-down lists, see "To add a person" on page 2-86.

To delete a person record

1 In the tree pane, right-click the name of the person whose record you want to edit. The Person dialog box appears.

2 Click **Delete**. A confirmation message appears.

3 Click **Yes**.

Custom Personnel Information

The tabs included in this section appear in the Person dialog box when custom features are purchased and installed in addition to the standard D-21.

Access Cards

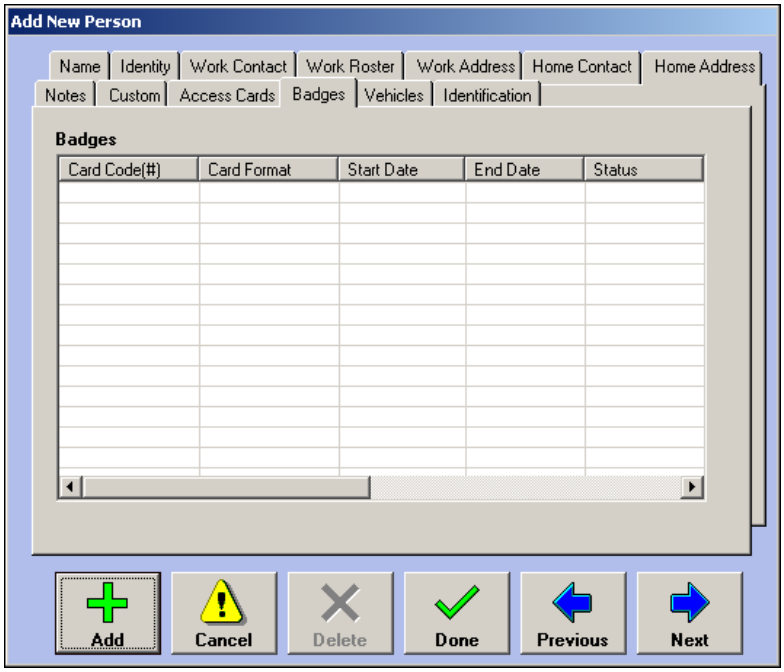
Access cards can be maintained using the Access Card tab. See "Assigning Cards and PINs" on page 8-23 for more information.

Badges

The Badges tab is available in the Person dialog box when you purchase and install the D-21 Badging System (P/N 192-851-00).

To add badging information to personnel

1. In the tree pane, click the plus sign (+) next to Personnel.
2. Right-click the person to receive a badge.
3. Click the Badges tab in the Person dialog box.



Badge information on the Badge tab is made available to the D-21 by GuardCard, a software product that lets you create badge formats, store personnel image files, and print badges. For more information on using GuardCard, see D-21 Badging System Set Up and Operation Manual (P/N 001-412-00).

Use the scrollbar to view more information.

Vehicles

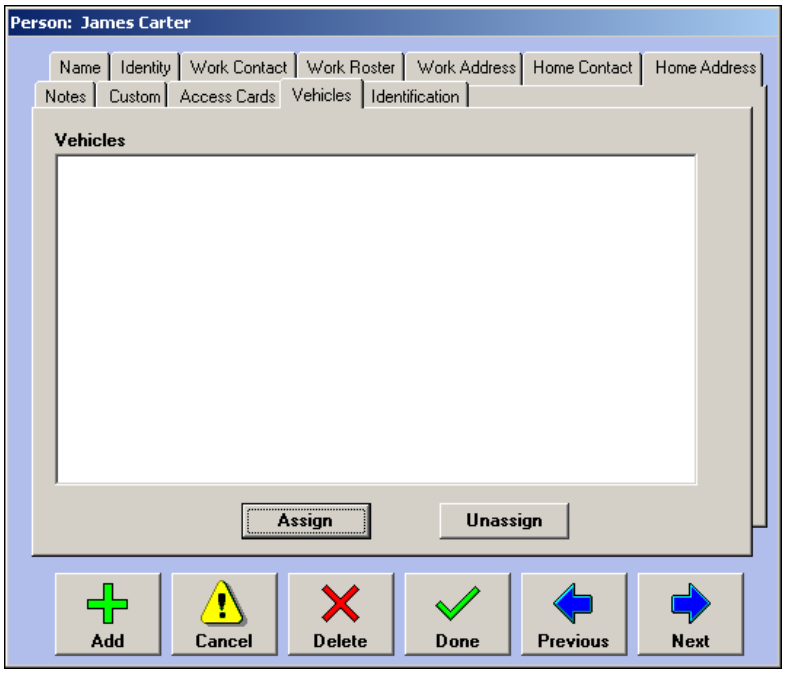
The Vehicles tab is available when you purchase and install the D-21 Security Client. Use the Vehicles tab to assign a vehicle in the database to a person.

Before you begin

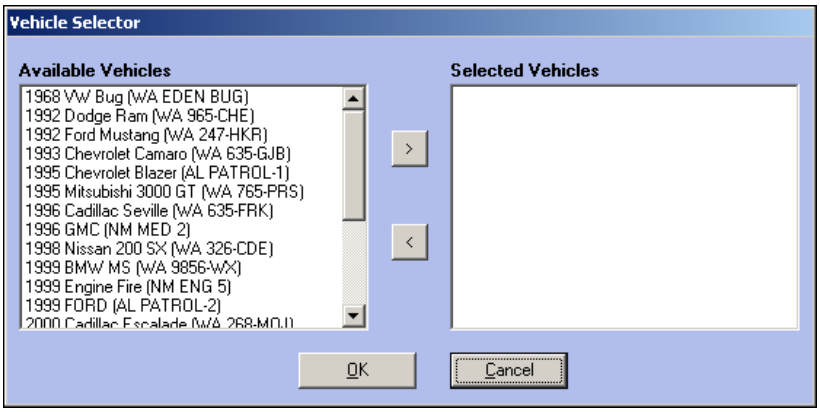
You must add the vehicle to the D-21 database before it is available for assignment to a person. For information on adding vehicles to the database, see "Vehicles" on page 2-101.

To assign a vehicle to a person

1. In the tree pane, click the plus sign (+) next to Personnel to display the personnel list.
2. Right-click the name of the person to whom you want to assign a vehicle.
3. In the Person dialog box, click the Vehicles tab.



4. Click **Assign**. The Vehicle Selector dialog box appears.



5. In the Available Vehicles list, click the name of the vehicle you want to assign.
6. Click **>** to move the vehicle from the Available Vehicles list to the Selected Vehicles list.

7 Click **OK**.

8 Click **Done**.

To unassign a vehicle to a person

1 In the tree pane, click the plus sign (+) next to Personnel.

2 Right-click the name of the person whose vehicle you want to unassign.

3 In the Person dialog box, click the Vehicles tab.

4 Click **Unassign**.

5 Click **Done**.

Identification

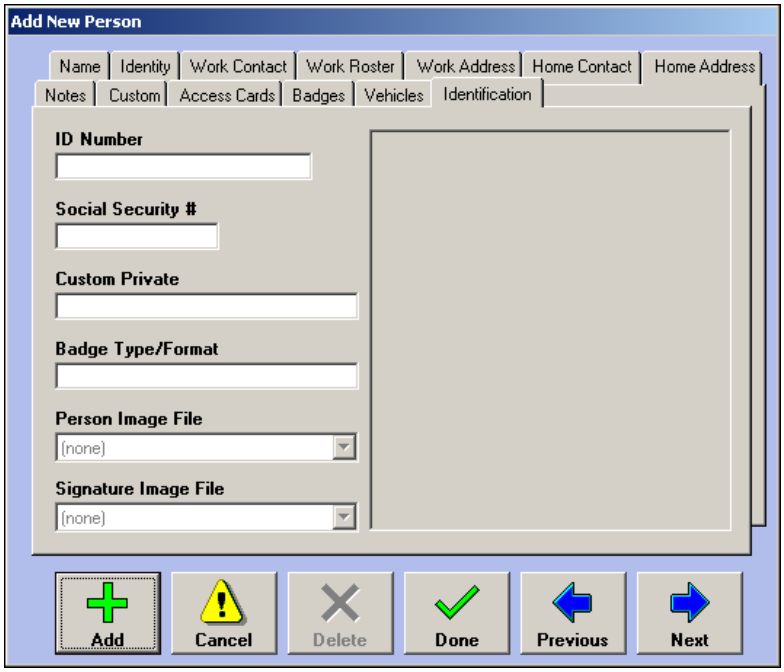
The Identification tab is available in the Person dialog box when you purchase and install the D-21 Security Client or the D-21 Badging System. Use the Identification tab to set up badge and identification tools for personnel.

IMPORTANT *You must make an entry in the ID Number field before the person's database record is available to the GuardCard software in the D-21 Badging System.*

To add security information to personnel

1 Click the Identification tab in the Person dialog box

NOTE *You must be logged into the Admin Client using the built-in Admin account to have access to the Identification tab.*



2 Enter a badge ID number, Social Security number, and badge type/format.

3 If you have set up person and signature images using the GuardCard badging system, the file names appear in the image file boxes. Person images are displayed in the area to the right and are stored at `C:\Program Files\D21\Media\PersonnelImages\[image name]`. Signature images are stored at `C:\Program Files\D21\Media\Signatures\[image name]` and can only be viewed using GuardCard. For more information on using GuardCard, see the D-21 Badging System Set Up and Operation Manual (P/N 001-412-00).

Operators

It is possible to add a new operator, specify personnel authorized to operate the D-21, and determine the portions of the D-21 they can access by using the Admin Client.

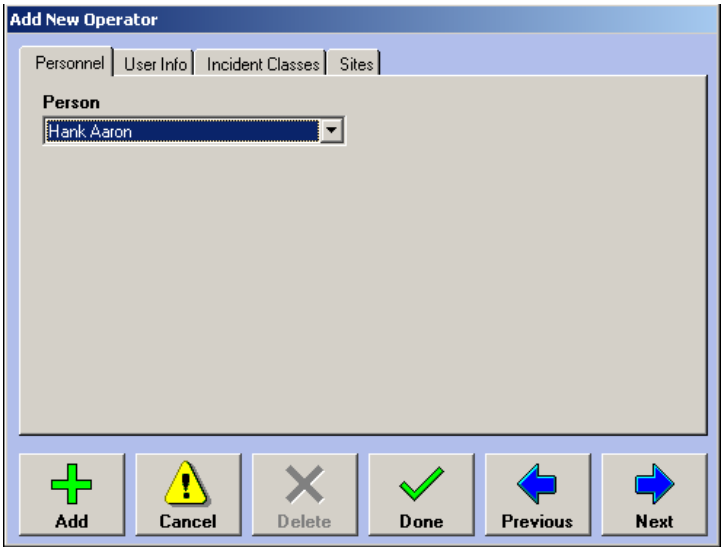


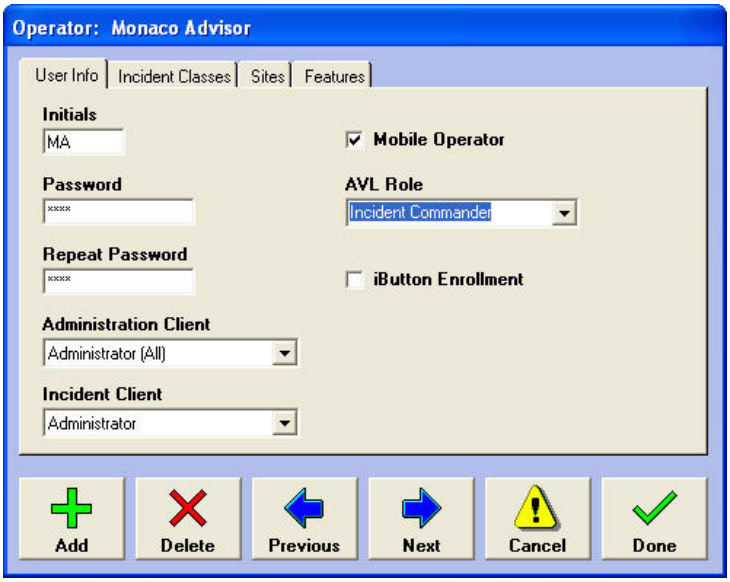
***Figure 2-3** Add New Operator dialog box*

Before you begin

The Add New Operator dialog box is accessible only if the database contains personnel who are not already operators. If you select **Add > Operator** when there are no personnel remaining who are not already operators, you will receive a message saying there are no personnel left to become operators.

To add an operator

1. Select **Add > Operator**.
2. Select the person you want to make an operator. Only persons who have been added to the database and are not already operators appear in this list.
3. Click **Next** to advance to the User Info tab.



4 Enter the operator initials as you would like them to appear in reports.

5 Enter the password in both the Password and Repeat Password boxes. The password must include at least four characters and is case sensitive.

6 Select the operator's security level when working in the D-21 Admin Client from the Administration Client drop-down list:

- **Administrator** Operators assigned the Administrator Admin Mode have full access to the D-21 Admin Client.
- **Data Entry1 (Expanded)** Operators assigned the Data Entry1 Admin Mode have the same access as Administrators except that they cannot add or delete operators, or view or edit operator records.
- **Data Entry2 (Standard)** Operators assigned the Data Entry2 Admin Mode cannot use the restore function. They cannot add or delete operators or view or edit operator records. They cannot add or delete RIDs or view or edit RID records. The following menu items are unavailable:

File	Add	Options	Commands
Restore	RID	Incident Processing	Reload All RIDs
	Operator	Workstation Options	Reset Edit Incident

- **Data Entry3 (Limited)** The only menu items available to operators assigned the Data Entry3 Admin Mode are under the File menu: Export, Backup, Compact, and Exit. The Restore function is disabled. Limited operators can view data and edit a subset of data by right-clicking the following in the tree pane: remote units, personnel, resources, hydrants, emergency cards, sites, facilities, and custom hazmats. Map locations cannot be set. No records can be deleted or added.
- **(none)** Operators assigned the (none) Admin Mode do not have access to the D-21 Admin Client.

7 Select the **Data Security Level**. Use the data security level to control the information displayed to the operator in the D-21 Incident Client personnel tabs.

Data Security Level	Displays information from the following D-21 Admin personnel tabs in the D-21 Incident Client
0-3	Reserved
4	Identity (only)
5	Identity, Work Roster, Work Contact, Home Contact, Notes, Custom
6	Identity, Work Roster, Work Contact, Home Contact, Notes, Custom, Identification, Badge
7-9	Reserved

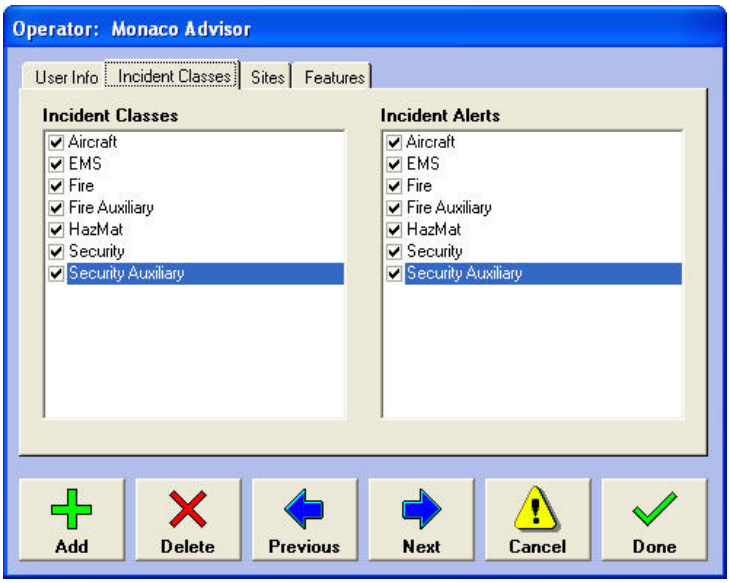
NOTE *You must be logged into the Admin Client using the built-in Admin account to view or set an Operator's Data Security Level.*

8 Select the operator's security level when working in the D-21 Incident Client in the Incident Client drop-down list:

- **Administrator** Operators assigned the Administrator Incident Mode have full access to the D-21 Incident Client.
- **Incident** Operators assigned the Incident Mode of Incident have the same access as Administrators except that they cannot enable or disable zones, RIDs, or remote units.
- **(none)** Operators assigned the (none) Incident Mode do not have access to the D-21 Incident Client.

9 Place a check mark in the iButton Enrollment check box if you want this operator to be able to assign IDS iButtons and PINs to personnel. For more information, see "IDS iButton and PIN Assignments" on page 9-24.

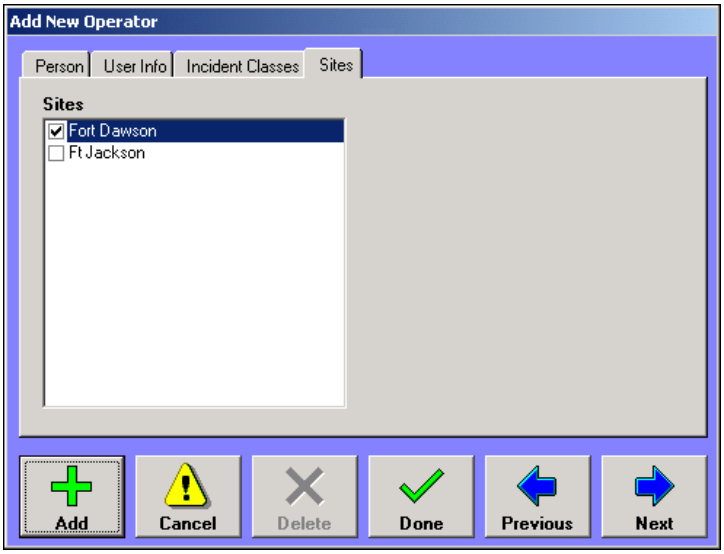
10 Click **Next** to advance to the Incident Classes tab.



11 Click to add a check in the box next to each class in the Incident Classes list to which this operator should have access. The D-21 Incident Client operator can create and manage incidents for the classes selected.

12 As checks are placed in the Incident Classes list, the corresponding boxes are also checked in the Incident Alerts list. Modify these defaults as necessary to add or remove classes for which the D-21 Incident Client operator will receive alerts from RIDs, units and zones.

13 Click **Next** to advance to the Sites tab.



14 Specify the sites for which you want this operator to receive alerts.

15 Click **Done**.

To edit an operator

1 In the tree pane, click the plus sign (+) next to Operators and then right-click the operator you want to edit. The Operator dialog box appears.

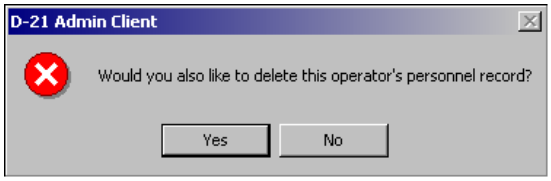
2 Change dialog box entries and selections as desired. For more information on the boxes and drop-down lists, see "To add an operator" on page 2-97.

To delete an operator

1 In the tree pane, click the plus sign (+) next to Operators and then right-click the operator you want to delete. The Operator dialog box appears.

2 Click **Delete**. A confirmation message appears.

3 Click **Yes**. The following alert appears:



4 If you want to delete the personnel record, click **Yes**. Otherwise, click **No**.

Vehicles

The Vehicles database is available with the D-21 Security Client, or when you purchase and install the separate vehicle database feature for the D-21. Vehicles can be entered in the D-21 system and tracked for repair and refueling, as well as gate entry identification, and they can be configured as dispatch resources. When the D-21G is installed, image files can be associated with vehicles in the database.

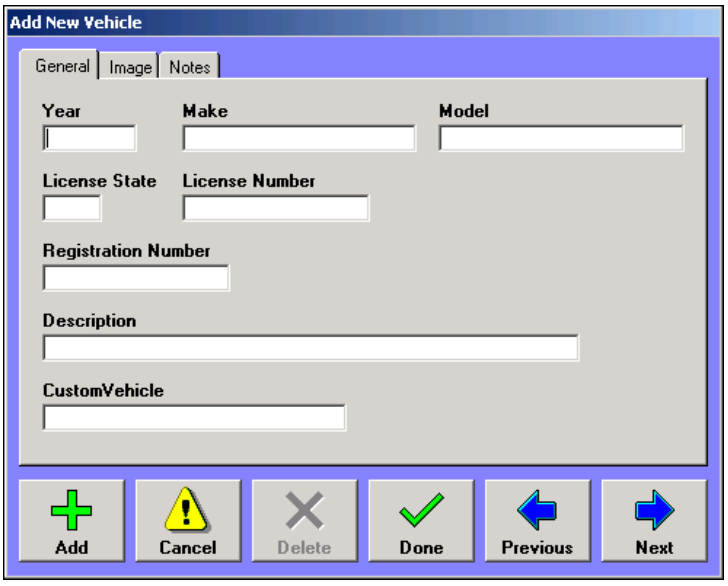
After you add a vehicle to the database, you can assign it to a person or resource. For more information, see:

- "To assign a vehicle to a person" on page 2-94.
- "To add a resource" on page 2-103.

To add a vehicle to the database

NOTE *Vehicle image files must be located in the D-21\Media\Vehicles folder. For more information on using image files, see "Media Files" on page 5-2.*

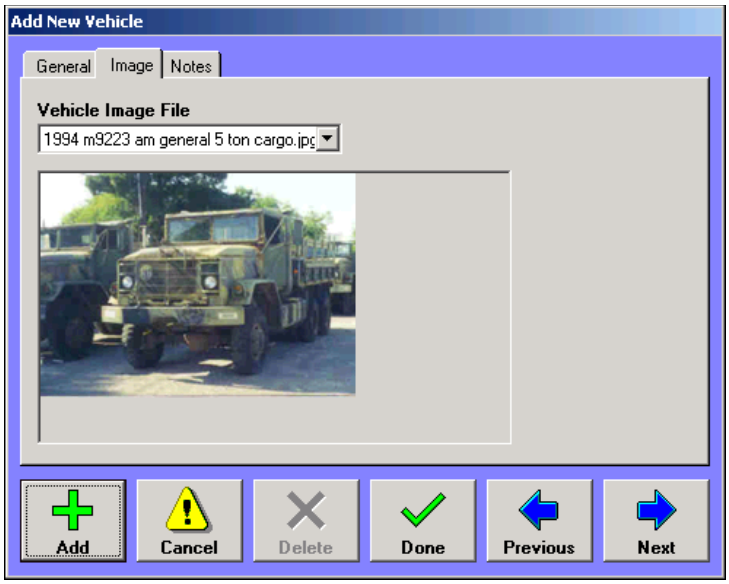
1 Select **Add > Vehicle**.



NOTE *The Image tab is only available with the D-21G.*

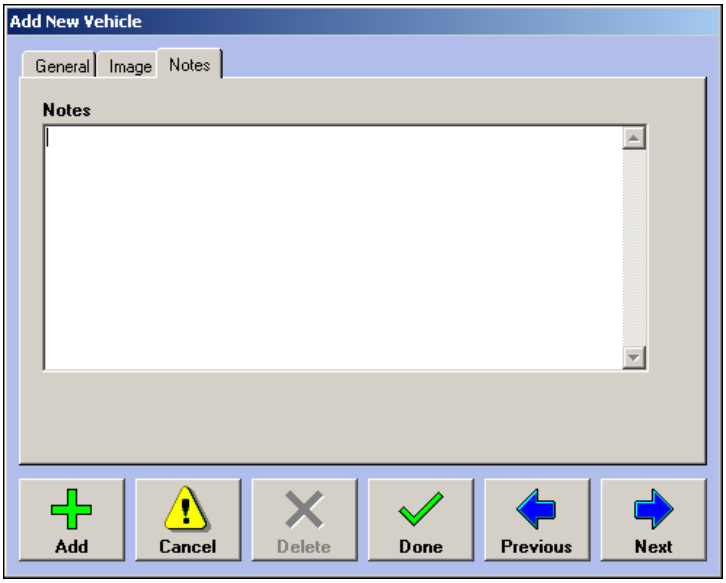
2 Enter vehicle information in the fields on the General tab.

3 Click the Image tab (only available with the D-21G).



4 If there is an image of the vehicle, select the name of the image file in the Vehicle Image File drop-down list.

5 Click the Notes tab.



6 Add notes for the vehicle, if desired.

7 Click **Done**.

To delete a vehicle

NOTE *A vehicle that is associated with a resource cannot be deleted from the database. You must first edit the resource to remove the vehicle association.*

1. In the tree pane, click the plus sign (+) next to Vehicles to display the list of vehicles.
2. Right-click the vehicle you want to delete. The Vehicle dialog box appears.
3. Click **Delete**.
   - If the vehicle is assigned to a resource, a message appears indicating the vehicle cannot be deleted. The message also displays the resource to which the vehicle is assigned.

   OR
   - If the vehicle is not assigned to a resource, a confirmation message appears. Click **OK**.

Resources

Use the Add New Resource dialog box to add a resource such as a fire truck, chief, or pump.

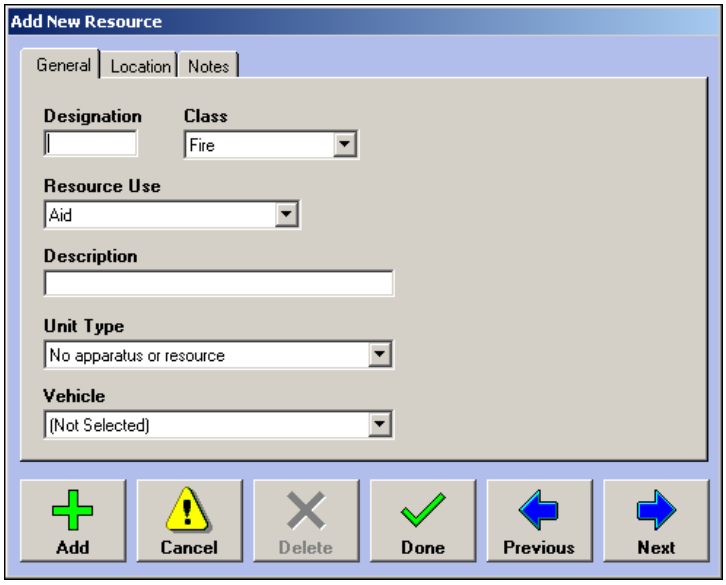


Figure 2-4 *Add New Resource dialog box*

Before you begin

If the resource is associated with a home facility, be sure to add the facility before adding the resource. See "Facilities" on page 2-13. If you want to use resource classes to identify specific resources, add the class on the Resource tab in the General Lists dialog box. See "Customizing Lists" on page 4-2.

To add a resource

1. Select **Add > Resource**.
2. Enter a name in the Designation box and a description of the resource in the Description box. The resource is identified throughout the D-21 system by the text entered in the Designation box.

3 Select a Resource Use from the Resource Use drop-down list. The D-21 uses resource usage to identify the resource class.

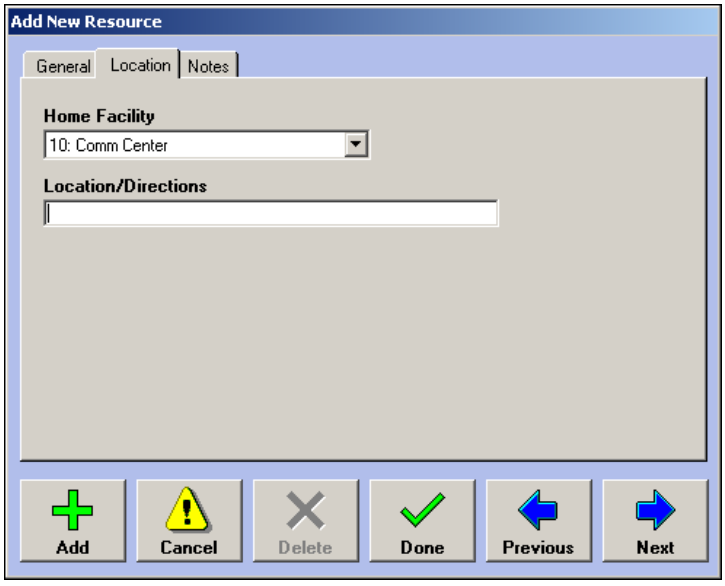
NOTE *You can add custom resource uses via the General Lists dialog box. See "General Lists" on page 4-2.*

4 Choose the class from the drop-down list. The D-21 uses the Resource Class to differentiate between security and fire resources.

5 Choose the unit type from the drop-down list. Unit types are National Fire Reporting System (NFIRS) categories included when you export data from the D-21.

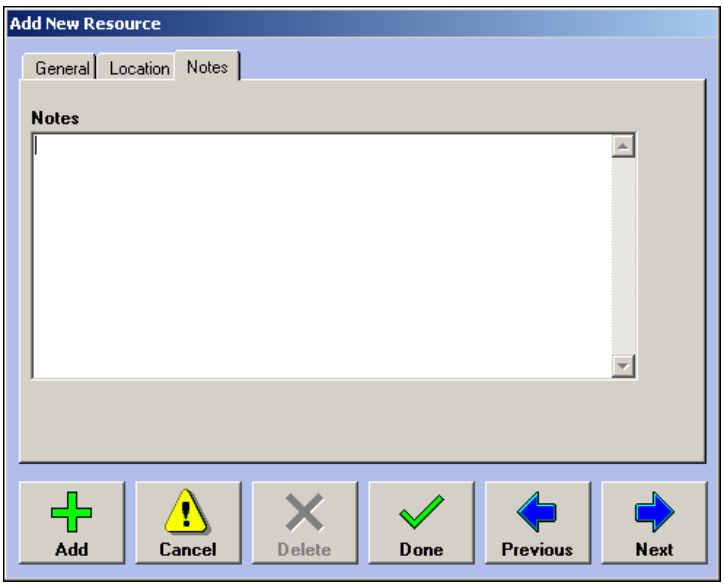
6 If you want to assign a vehicle to this resource, select the vehicle from the Vehicle drop-down list.

7 Click **Next** to advance to the Location tab.



8 Specify the home facility and location where the resource is normally housed.

9 Click **Next** to advance to the Notes tab.



10 Enter additional descriptive information for the resource.

11 Click **Done**.

To edit a resource

1 In the tree pane, click the plus sign (+) next to Resources then right-click the resource you want to edit. The Resource dialog box appears.

2 Change dialog box entries and selections as desired. For more information on the tabs, boxes, and drop-down lists, see "To add a resource" on page 2-103.

3 Click **Done**.

To delete a resource

1 In the tree pane, click the plus sign (+) next to Resources then right-click the resource you want to delete. The Resource dialog box appears.

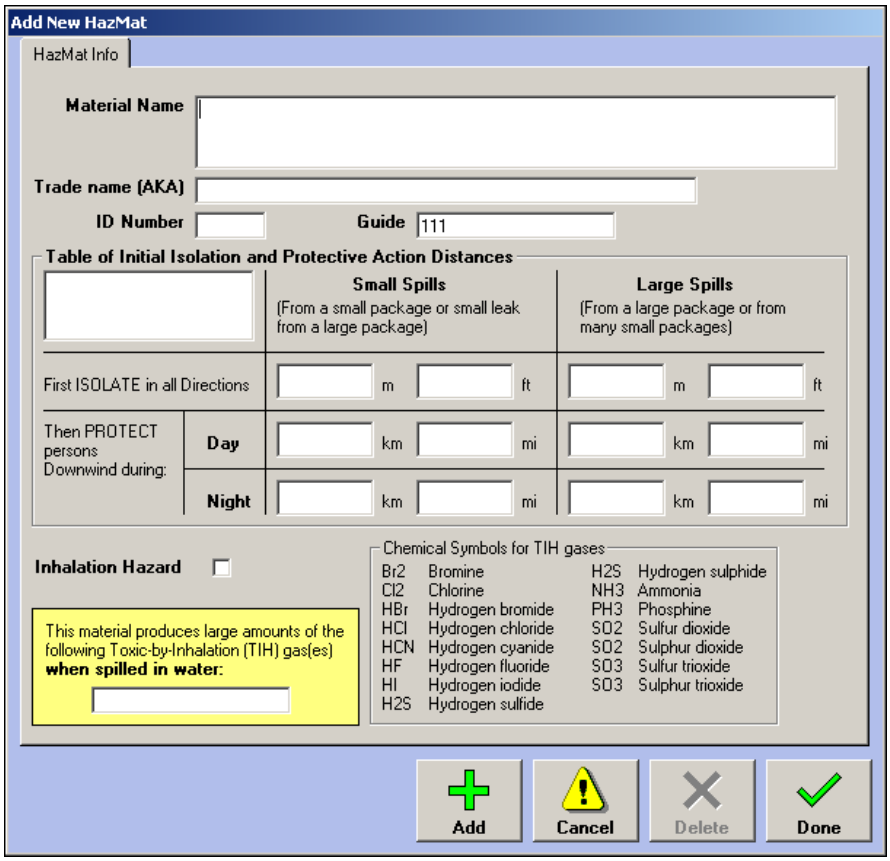
2 Click **Delete**. A message asks you to confirm that you want to delete the resource.

3 Click **Yes**.

HazMats

In the Admin Client click **Add > HazMat** to access the Add New HazMat dialog box to add a hazardous material to the database.

Figure 2-5 *Add New HazMat dialog box*



To add a new hazardous material

1. Select **Add > HazMat**.
2. Enter data in the boxes in the dialog box. The box at the top left of the Table of Initial Isolation and Protective Action Distances is for notes.
3. Click **Done**.

To delete a hazardous material

NOTE *Only custom hazardous materials can be deleted.*

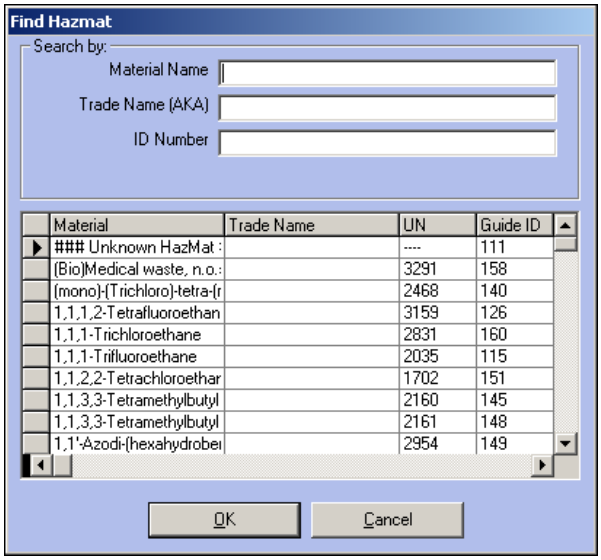
1. In the tree pane, under Custom HazMats, right-click the hazardous material you want to delete. The HazMat Information dialog box appears.
2. Click **Delete**. A confirmation message appears.
3. Click **Yes**.

Editing HazMats

Use the Edit HazMats dialog box to edit the trade name of a standard hazardous material, or to edit information about a custom hazardous material.

NOTE *Only the Trade Name box is editable for standard HazMat entries.*

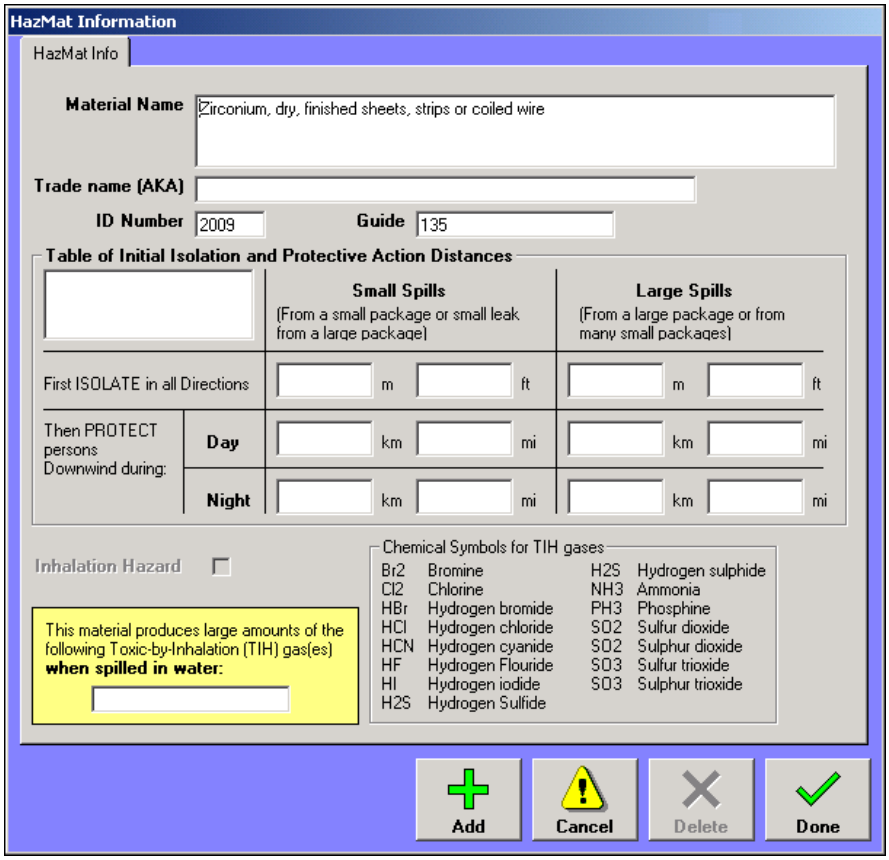
Figure 2-6 *Edit HazMat dialog box*



To edit a HazMat

1. Select **Options > Edit HazMats**.
2. Locate the material in the list. When you enter characters in one of the search boxes, the list of HazMat records scrolls so the entry that begins with the same character(s) appears at the top.
3. Click the material to select it.
4. Click **OK**. If the HazMat you are attempting to edit is a standard HazMat, you will see the following message:

5 Click **OK**. The HazMat Information dialog box appears.



6 If you are editing a standard HazMat, enter the desired data in the Trade name box. If you are editing a custom HazMat, you can modify the data in any of the text-entry boxes.

7 When you have completed the changes, click **Done**.

Hydrants

Use the Add New Hydrant dialog box to add hydrants to the database.

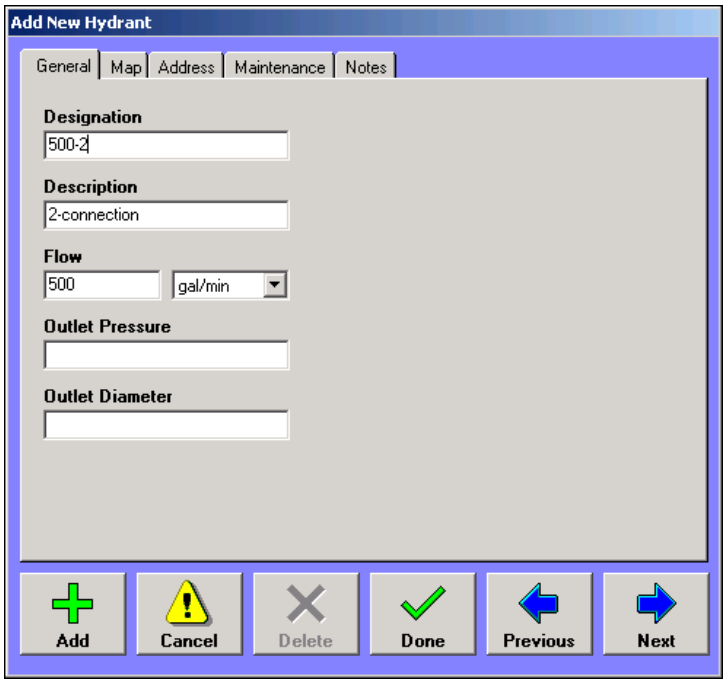
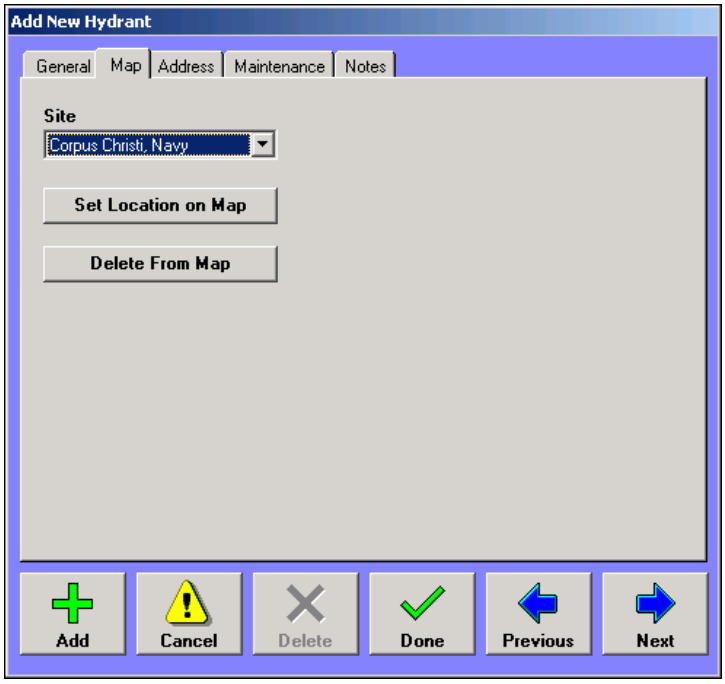


Figure 2-7 *Add New Hydrant dialog box*

To add a hydrant

1. Select **Add > Hydrant**. The Add New Hydrant dialog box appears, with the General tab in the foreground.
2. Enter the designation. The hydrant is identified throughout the D-21 system by the text entered in the Designation box.
3. Enter a description.
4. Enter the flow, and select the correct unit of measure (gal/min or liter/sec) from the drop-down list. Flow and unit of measure are included in the box that pops up when an operator right-clicks a hydrant on a map in the D-21 Incident Client.
5. Enter outlet pressure and diameter.

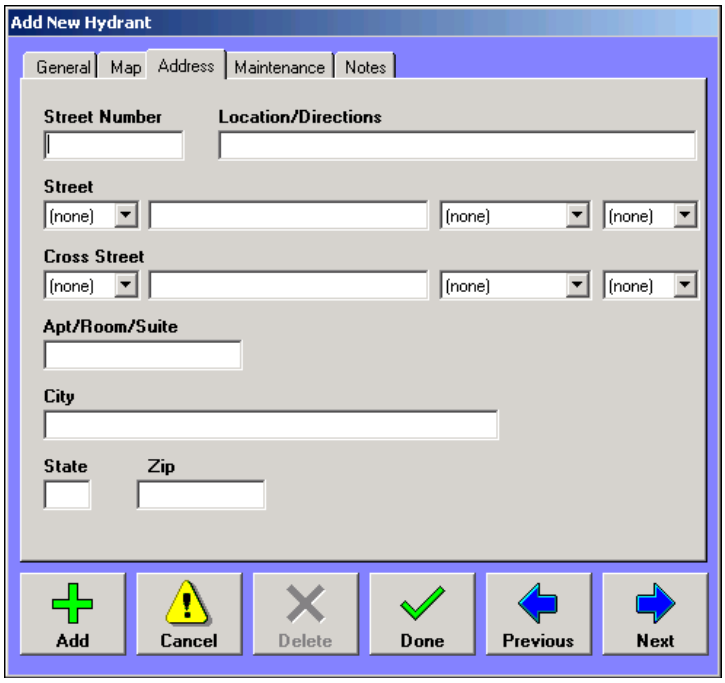
6 Click **Next** to advance to the Map tab. (The Map tab is only available with the D-21M.)



7 Select the site from the drop-down list.

8 Click **Set Location on Map** to position the new hydrant on the site map. For information on using the Select Map Location dialog box, see "Placing Items on the Map (D-21M)" on page 2-112.

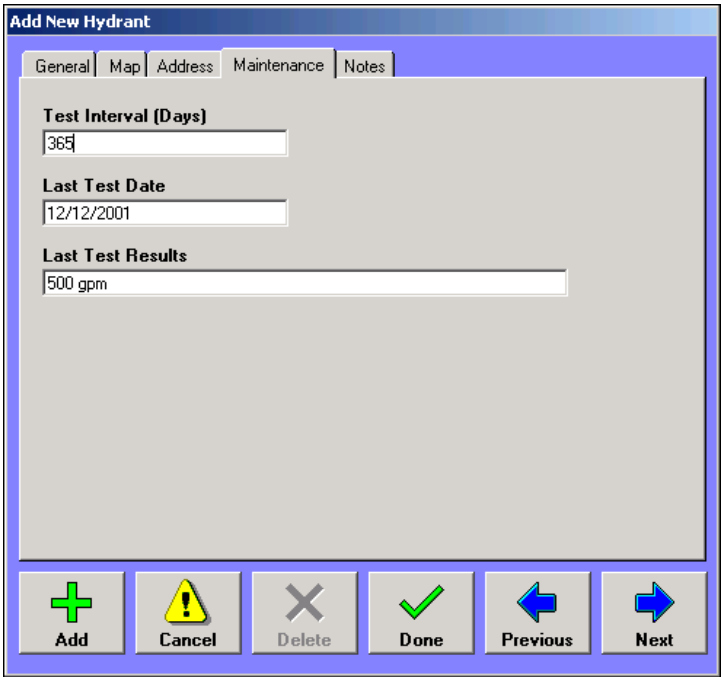
9 Click **Next** to advance to the Address tab.



10 Enter the address, choosing the directional prefix/suffix (N, NW, etc.) and street types (Ave, St, etc.) from the drop-down lists.

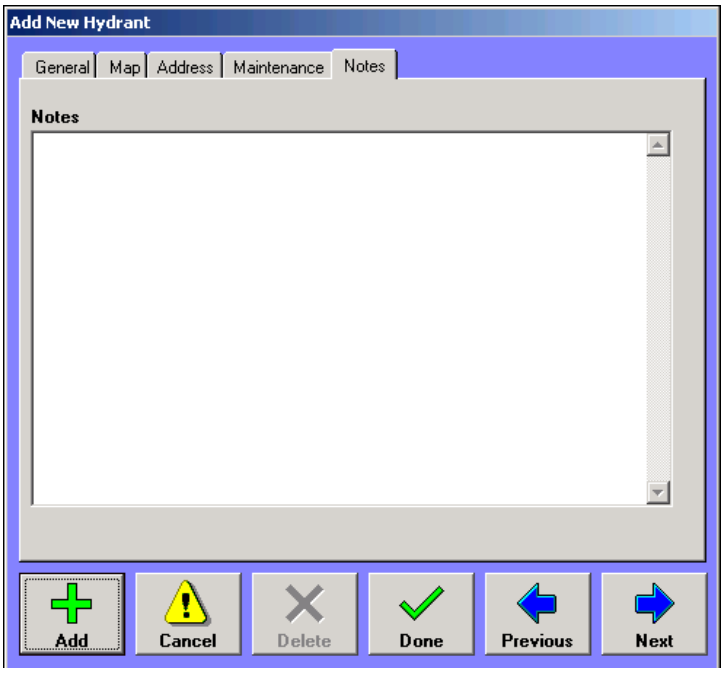
NOTE *You can add to, delete from, and edit the items that appear in the directional prefix/suffix list and street types list in the General Lists dialog box. See* *"Customizing Lists" on page 4-2.*

11 Click **Next** to advance to the Maintenance tab.



12 Enter the most recent test result information for the hydrant.

13 Click **Next** to advance to the Notes tab.



14 Enter notes for the new hydrant.

15 Click **Done**.

To edit a hydrant

1 In the tree pane, right-click the hydrant you want to edit. The Hydrant dialog box appears.

2 Change dialog box entries and selections as desired. For more information on the tabs, boxes, and drop-down lists, see "To add a hydrant" on page 2-109.

3 Click **Done**.

To delete a hydrant

1 In the tree pane, right-click the hydrant you want to delete. The Hydrant dialog box appears.

2 Click **Delete**. A confirmation message appears.

3 Click **Yes**.

Placing Items on the Map (D-21M)

When the D-21 is configured with a site map (D-21M), graphical icons representing the facilities and hydrants can be placed on the map. The numbers, names, and status of the facilities and hydrants can then be viewed from the map in the D-21 Incident Client. For information on setting up and configuring a site map, see "Sites" on page 2-3.

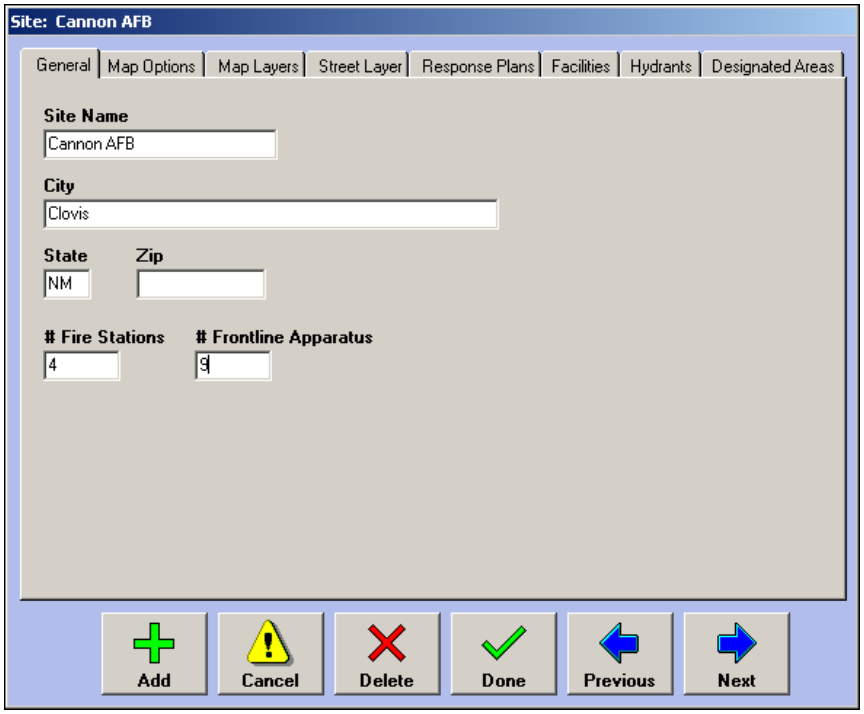
There are two ways to place facilities and hydrants on the map:

- **Single Items** Use the Map tabs in the Facility and Hydrant dialog boxes to place a single facility or hydrant on the map. See "To place a single facility or hydrant on the map" on page 2-119.

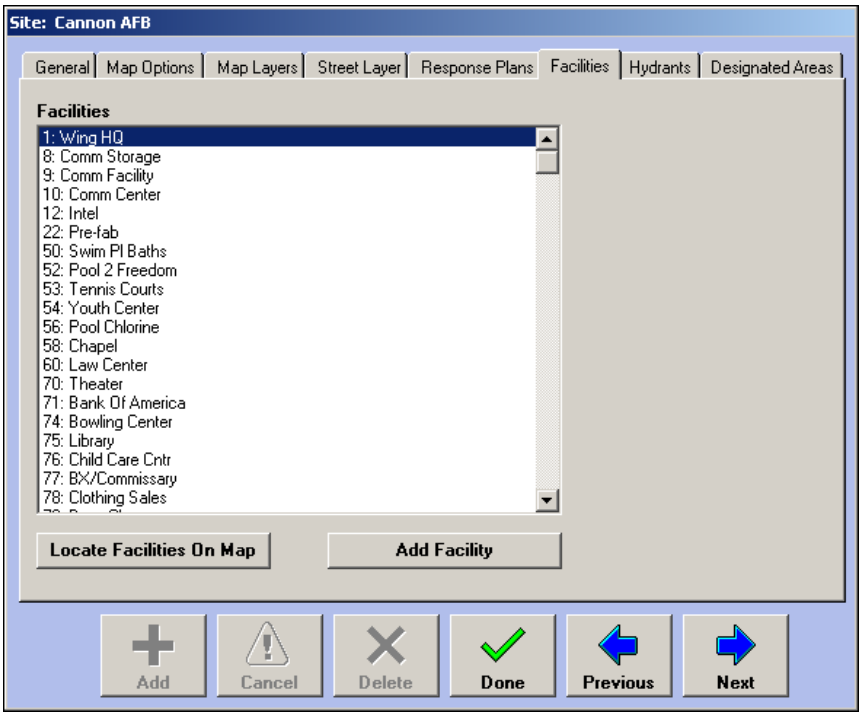
- **Multiple Items** The Site dialog box provides a Facilities tab and a Hydrants tab which you can use to add one or more items to the map. On both tabs, the D-21 displays items which have already been added to the map and items which have not been added to the map. For more information, see:
  - "To place multiple facilities on the map" on page 2-113.
  - "To place multiple hydrants on the map" on page 2-116.

To place multiple facilities on the map

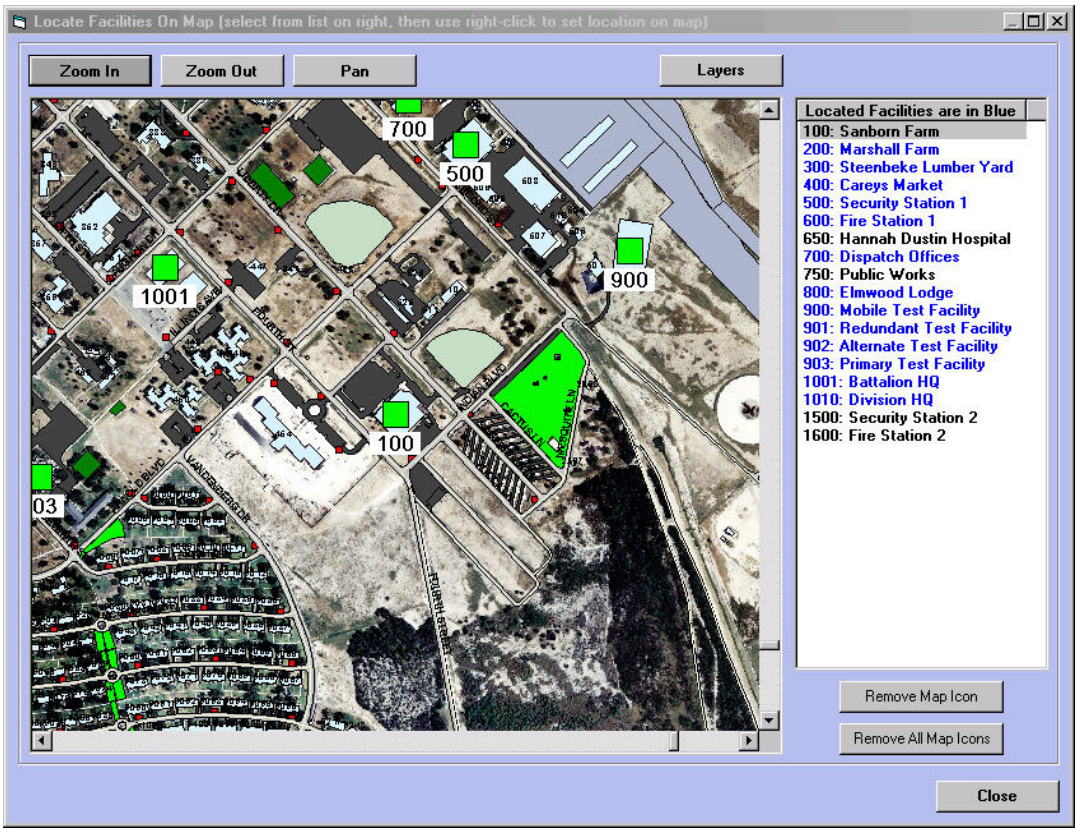
1 In the tree pane, right-click the site. The Site dialog box appears.



2 Click the Facilities tab.



3 Click **Locate Facilities On Map**. The Locate Facilities On Map dialog box appears.



- **Zoom In/Zoom Out** Changes the cursor to a magnifying glass. Use the Zoom In cursor to magnify the map. Use the Zoom Out cursor to reduce the size of the map. Both cursors reposition the center of the map at the location of the mouse click.
- **Pan** Changes the cursor to a hand. Use the Pan cursor to drag the map inside the window.
- **Layers** Use the Map Layers dialog box to turn on and off individual map layers.
- **Remove Map Icon** The icon for the facility that is selected in the list is removed from the map when you click this button.
- **Remove All Map Icons** All facility icons are removed from the map when you click this button.

NOTE *The Remove All Map icons command is irreversible. If you click this button by mistake, you will have to replace all facility icons on the map.*

4 Select a facility from the list displaying all facilities that have been added to the site. Facilities shown in blue have already been placed on the map. Facilities that are not on the map are shown in black.

5 Navigate to the location on the map where you want to place the facility. Use Zoom In, Zoom Out, Pan, and the map window scroll bars to find the facility location.

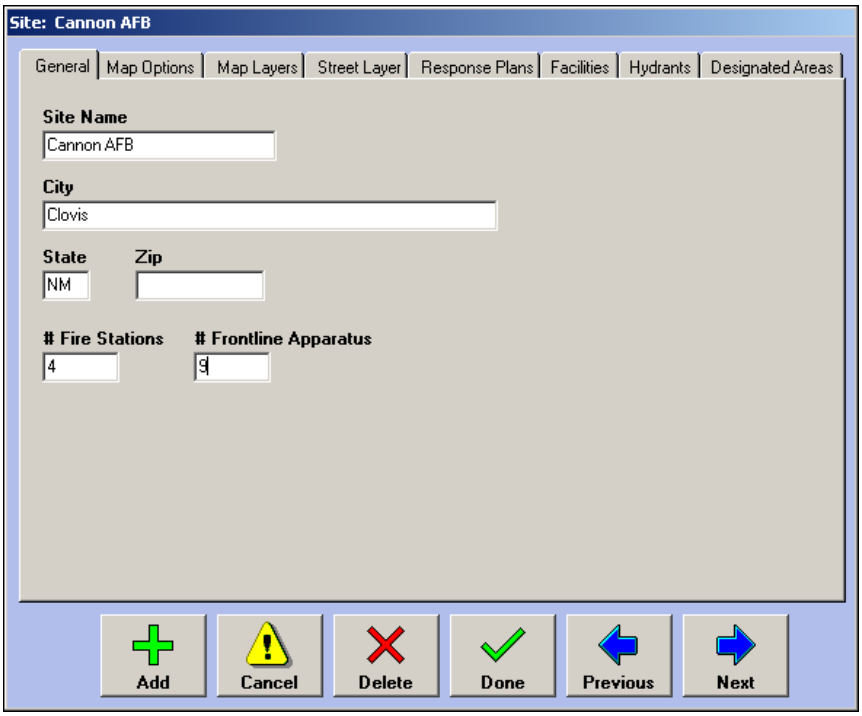
6 Right-click the location. If you need to reposition the facility, select the facility in the list, click **Remove From Map**, and then right-click the new location.

7 Click **Close**.

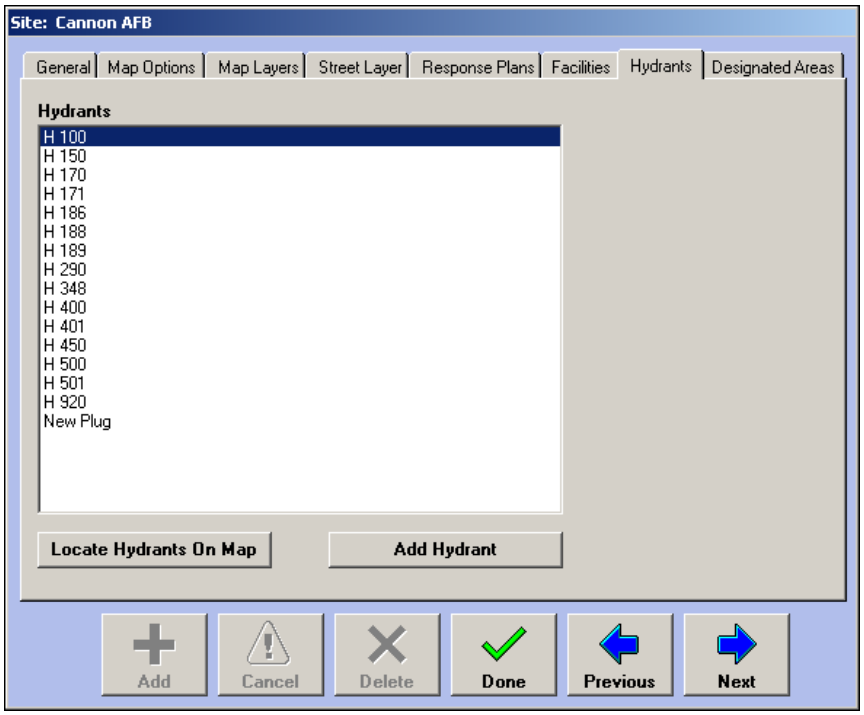
8 Click **Done** in the Site dialog box.

To place multiple hydrants on the map

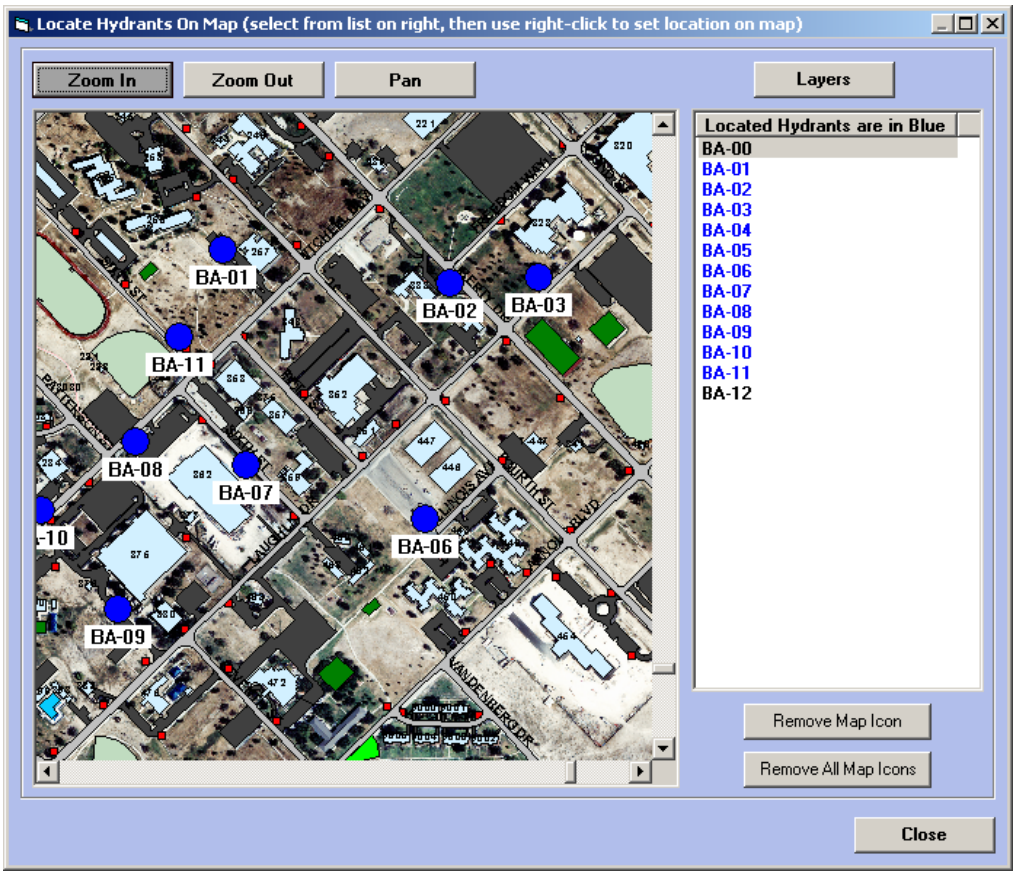
1 In the tree pane, right-click the site. The Site dialog box appears.



2 Click the Hydrants tab.



3 Click **Locate Hydrants On Map**. The Locate Hydrants On Map dialog box appears.



- **Zoom In/Zoom Out** Changes the cursor to a magnifying glass. Use the Zoom In cursor to magnify the map. Use the Zoom Out cursor to reduce the size of the map. Both cursors reposition the center of the map at the location of the mouse click.
- **Pan** Changes the cursor to a hand. Use the Pan cursor to drag the map inside the window.
- **Layers** Use the Map Layers dialog box to turn on and off individual map layers.
- **Hydrant List** Displays all hydrants that have been added to the site. Hydrants shown in blue have already been placed on the map. Hydrants that are not on the map are shown in black.
- **Remove Map Icon** The icon for the hydrant that is selected in the list is removed from the map when you click this button.
- **Remove All Map Icons** All hydrant icons are removed from the map when you click this button.

NOTE *The Remove All Map icons command is irreversible. If you click this button by mistake, you will have to replace all hydrant icons on the map.*

4 Select a hydrant in the list.

5 Navigate to the location on the map where you want to place the hydrant. Use Zoom In, Zoom Out, Pan, and the map window scroll bars to find the hydrant location.

6 Right-click the location. If you need to reposition the hydrant, select the hydrant in the list, click **Remove From Map**, and then right-click the new location.

7 Click **Close**.

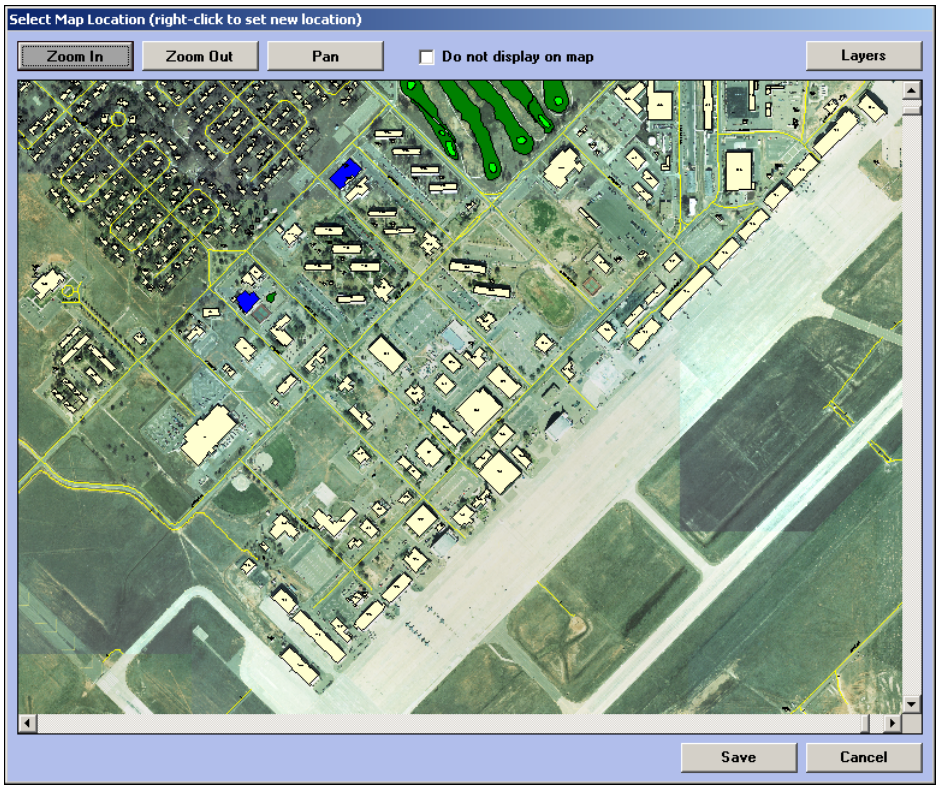
8 Click **Done** in the Site dialog box.

To place a single facility or hydrant on the map

1 In the tree pane, right-click the facility or hydrant you want to place on the map. The corresponding dialog box appears.

2 Click the Map tab.

3 Click **Set Location on Map**.



4 Click **Zoom In**, **Zoom Out**, **Pan**, or use the map window scroll bars to find the location. The navigation buttons function as follows:

- **Zoom In/Zoom Out** Changes the cursor to a magnifying glass. Use the Zoom In cursor to magnify the map. Use the Zoom Out cursor to reduce the size of the map. Both cursors reposition the center of the map at the location of the mouse click.
- **Pan** After clicking **Pan**, the cursor becomes a hand. Hold down the left mouse button while moving the mouse to drag the map within the pane.
- **Do not display on map** When checked, the facility is only displayed on the map when the facility is in alarm or trouble, or when you create a manual incident at the facility.

- **Layers** Displays the Map Layers dialog box.

5. Click the check box next to those layers of the map you want to appear in the window and then click **OK**. See "To edit a facility" on page 2-26.
6. Right-click the location on the map where you want to place the facility or hydrant. You can change the position of an item on the map by right-clicking in a new place.
7. Click **Save**.
8. Click **Done**.

To delete a facility from the map

1. In the tree pane, right-click the facility you want to delete from the map. The Facility dialog box appears.
2. Click the Map tab.
3. Click **Delete From Map**. A confirmation message appears.
4. Click **Yes**.

To delete a hydrant from the map

1. In the tree pane, right-click the hydrant you want to delete from the map. The Hydrant dialog box appears.
2. Click the Map tab.
3. Click **Delete From Map**. A confirmation message appears.
4. Click **Yes**.

Section 3
Setting Up Incident Processing

Read this section to learn how to set up the information required when responding to incidents. This section also contains instructions for customizing the way alerts and incidents are handled.

Contents

Response Plans 3-2
- Emergency Cards 3-20
- Pre-Plans 3-23

Actions 3-27
- Using Actions 3-27
- Attaching Actions to Custom Buttons 3-36
- Attaching Actions to Status Changes 3-37

Standard Operating Procedures (SOPs) 3-38

Incident Processing 3-44
- Setting Up Alert Processing 3-45
- Customizing Incident Numbers 3-53
- Customizing Incident Class and Status Colors 3-55
- Setting Alert Sounds 3-57
- Resetting Incident Editing Controls 3-58

Dispatch Configuration 3-58
- Incident Types 3-61
- Resource Classes 3-65
- Resource Groups 3-66

Response Plans

Response plans contain call lists, pre-plans, information for dispatching resources, graphics of equipment and floor plans, HazMat information, and actions. A response plan can be attached to sites, facilities, zones, or emergency cards. When an incident is created at a facility, all of the response information attached to the facility is made available to the operator responding to the incident.

When an incident is created from an automatic alert, the D-21 first looks for a response plan for the zone reporting the alarm. If there is a response plan attached to the zone, its information is displayed in the D-21 Incident Client incident pane. If there is no response plan for the zone, the D-21 looks for a response plan for the zone's facility. If there is no response plan for the facility, the D-21 looks for a site response plan. To determine if a facility has a response plan, see "To view facilities with response plans attached" on page 3-19.

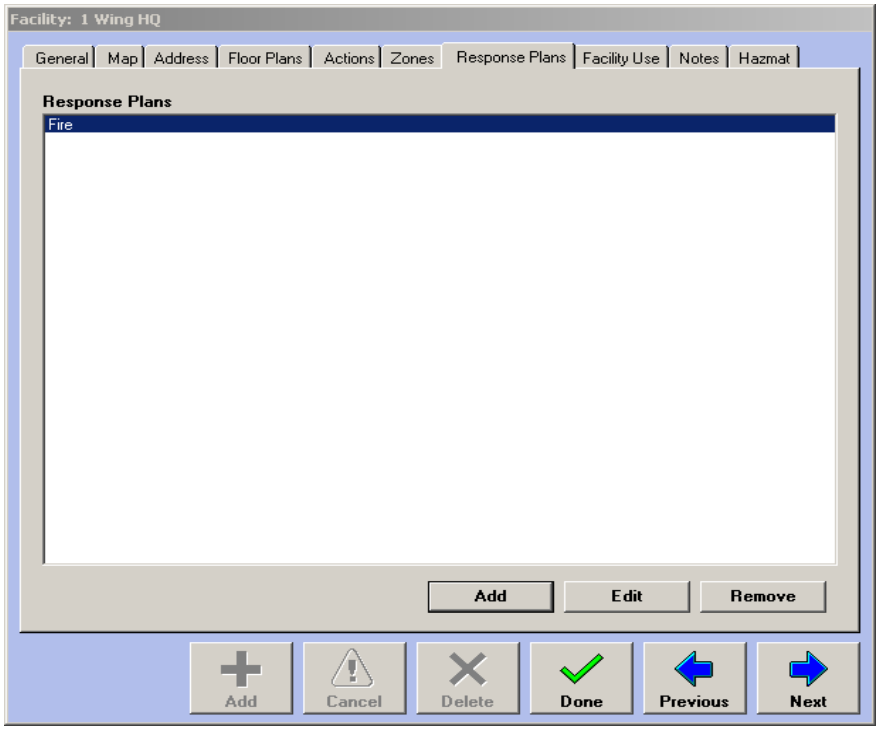
Emergency cards can be used to create response plans that are independent of site, facility, or zone. These response plans can be attached to incidents as they are created by operators. See "Emergency Cards" on page 3-20 for more information.

This section includes the following procedures:

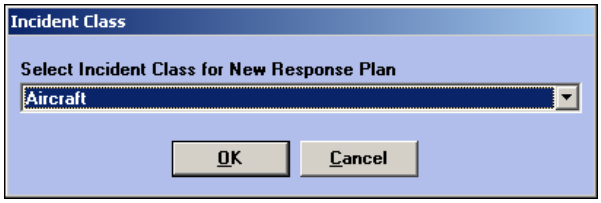
- "To add a response plan" on page 3-3.
- "To add a call list to a response plan" on page 3-3.
- "To add a Monaco pre-plan to a response plan" on page 3-5.
- "To add a pre-plan file to a response plan" on page 3-7.
- "To add dispatch instructions to a response plan" on page 3-9.
- "To add mutual aid resources to a response plan" on page 3-11.
- "To add graphics to a response plan" on page 3-12.
- "To add hydrant information to a response plan" on page 3-13.
- "To add an action to a response plan" on page 3-15.

To add a response plan

1. In the tree pane, right-click the site, facility, zone, or emergency card for which you want to create the response plan. The editing dialog box for the item you clicked appears.
2. Click the Response Plans tab.



3. Click **Add**. The Select Incident Class dialog box appears.



4. Select an incident class for the response plan. If the site, facility, or zone is monitored for fire, select Fire. If the item is monitored for security, select Security, and so on. You can add as many response plans as make sense for the situation.
5. Click **OK**. The Response dialog box appears with tabs for each type of information you can add to the response plan.

To add a call list to a response plan

1. In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the call list.
2. Click the Response Plans tab.

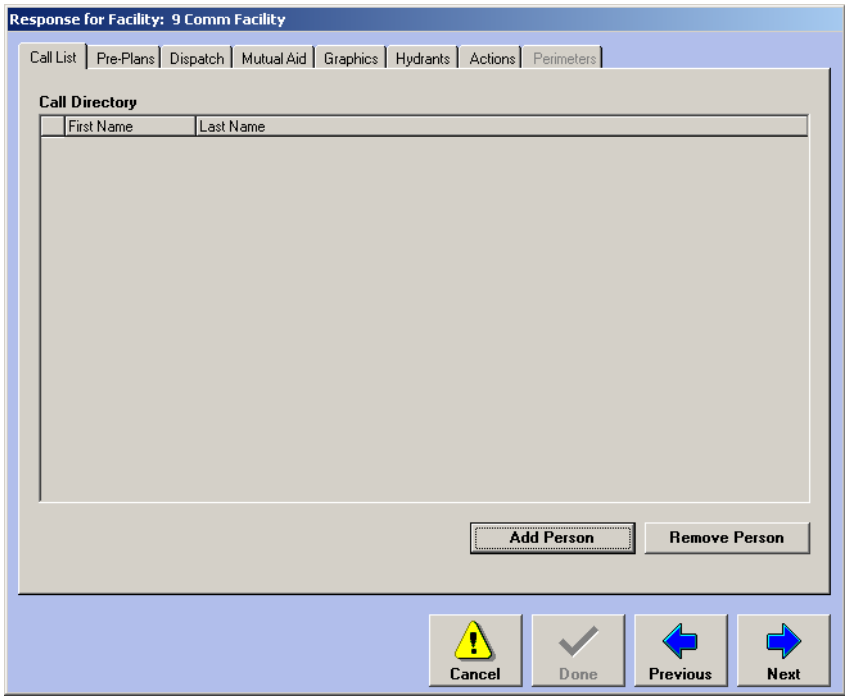
3 Do one of the following:

- Click **Add** to add a new response plan.

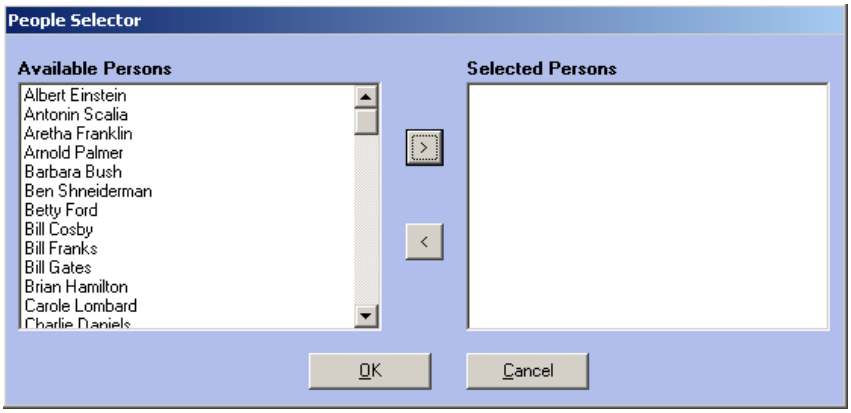
OR

- Select an existing response plan and click **Edit** to add the call list to the selected response plan.

4 Click the Call List tab.



5 Click **Add Person** to create a phone list. The People Selector dialog box appears.



6 Select the people you want to add to the response plan Call List from the Available Persons list.

NOTE *Only people who have been added to the D-21 database with the Add Person command are available for the Call List.*

7 Click the right arrow button (**>**) to move them into the Selected Persons list.

8 Click **OK**.

To add a Monaco pre-plan to a response plan

NOTE *This procedure describes adding a Monaco pre-plan to a response plan. Monaco pre-plans are based on pre-plan templates provided by Monaco. See "Pre-Plans" on page 3-23. For information on adding an image file pre-plan to a response plan, see "To add a pre-plan file to a response plan" on page 3-7.*

1 In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the Monaco pre-plan.

2 Click the Response Plans tab.

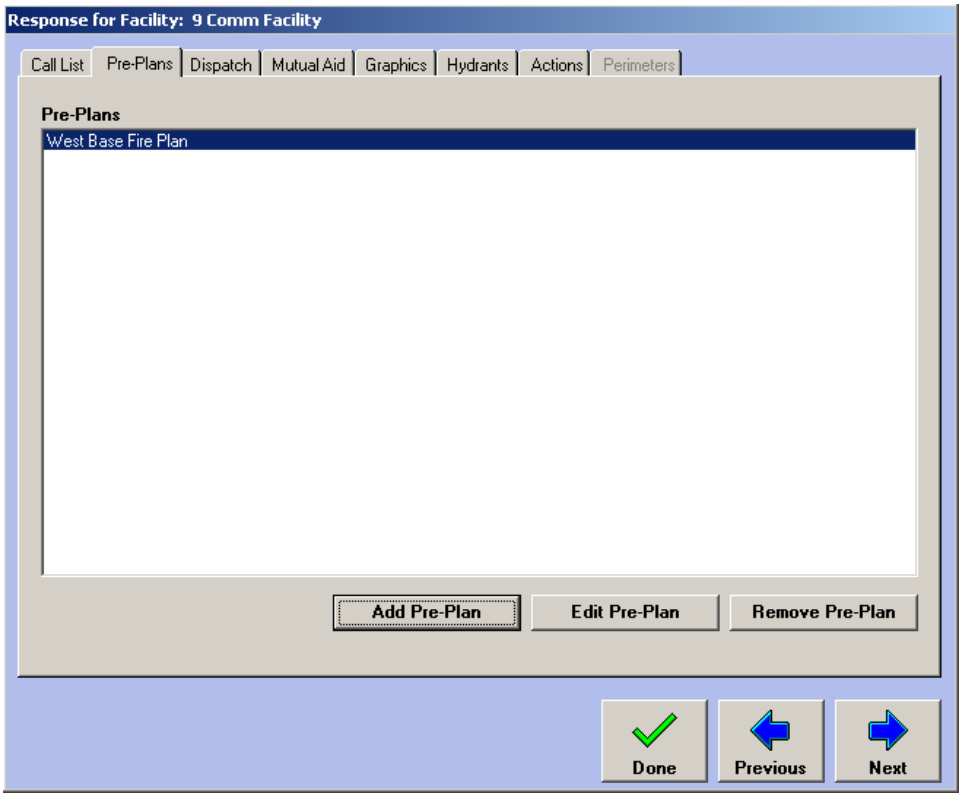
3 Do one of the following:

- Click **Add** to add a new response plan.

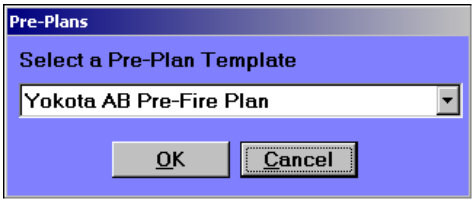
OR

- Select an existing response plan and click **Edit** to add the pre-plan to the selected response plan.

4 Click the Pre-Plans tab.

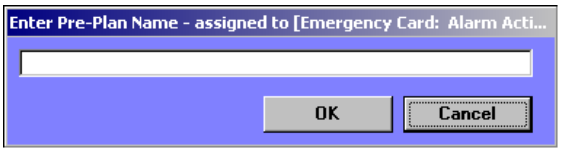


5 Click **Add Pre-Plan**. The Pre-Plans dialog box appears.

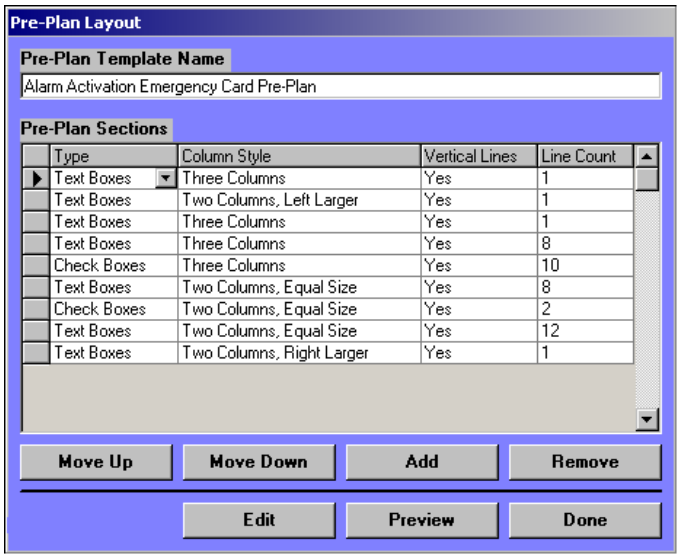


6 Select the Pre-Plan template you want to use to build the pre-plan.

7 Click **OK**. The Enter Pre-Plan Name dialog box appears.



8 Enter a name for the pre-plan and click **OK**. The Pre-Plan Layout dialog box appears.



9 If you want to change the pre-plan name, edit the text in the Pre-Plan Template Name box.

10 Click **Edit**. Edit the pre-plan as described in "Pre-Plans" on page 3-23, keeping in mind this pre-plan is not a template, but the actual pre-plan for the site, zone, facility, or emergency card response plan you are configuring.

11 When you have completed editing the pre-plan, click **Done**.

To add a pre-plan file to a response plan

NOTE *This procedure describes adding an image file pre-plan to a response plan. You can add pre-plans that are graphical image files or.pdf files created with Adobe Acrobat. See "Pre-Plans" on page 3-23 for more information. For information on adding a Monaco pre-plan to a response plan, see "To add a Monaco pre-plan to a response plan" on page 3-5.*

1 In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the Monaco pre-plan.

2 Click the Response Plans tab.

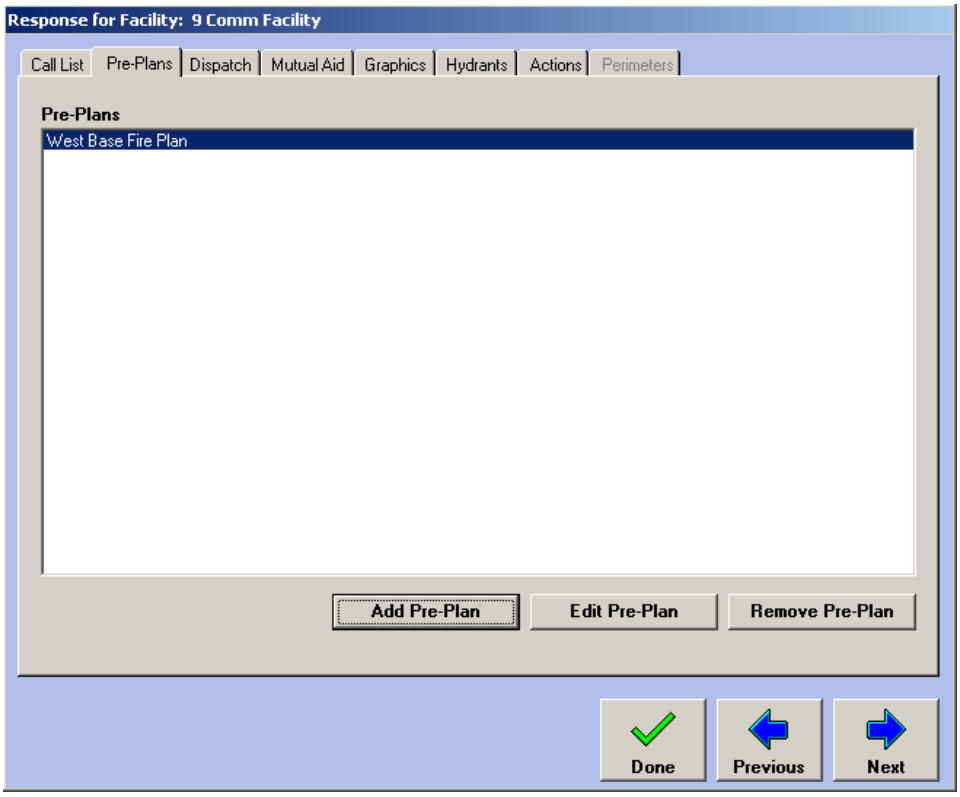
3 Do one of the following:

- Click **Add** to add a new response plan.

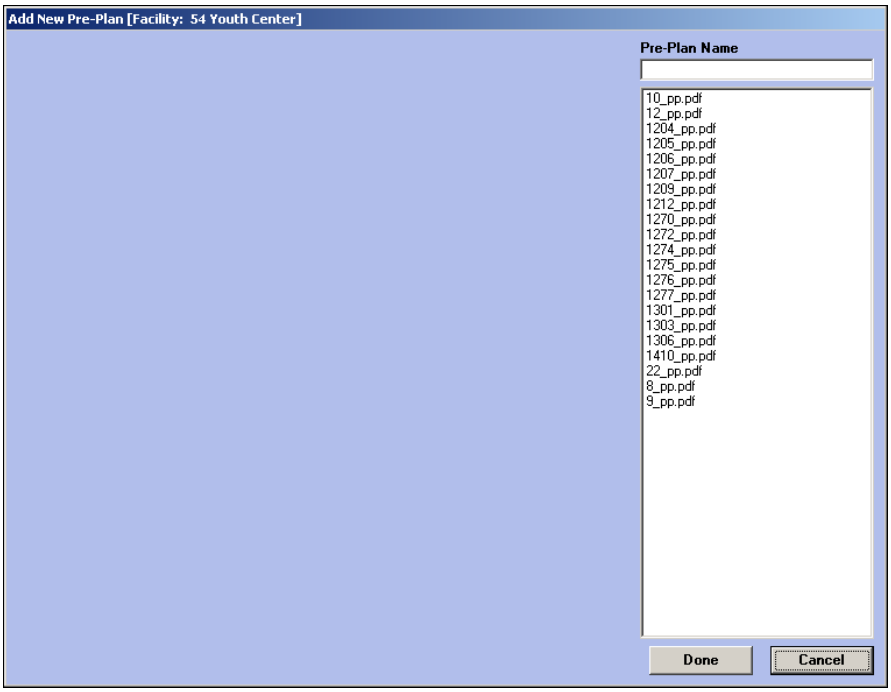
OR

- Select an existing response plan and click **Edit** to add the pre-plan file to the selected response plan.

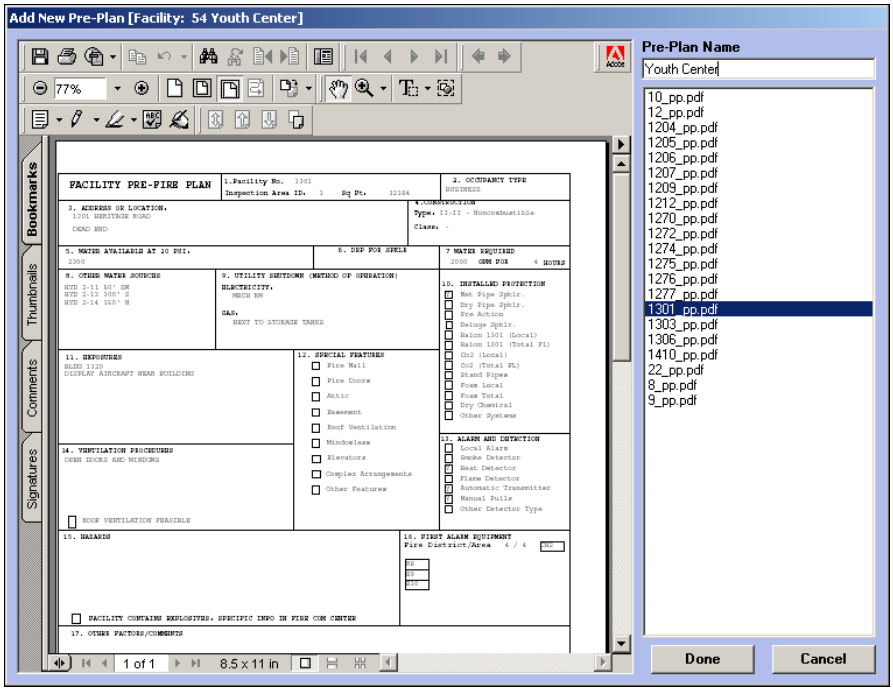
4 Click the Pre-Plans tab.



5 Click **Add Pre-Plan**. The Add New Pre-Plan dialog box appears.



- **Pre-Plan Name** Enter a name for the pre-plan.
- **Pre-Plan List** Select the file that contains the pre-plan you want to add to the response plan. Only files located in `C:\Program Files\D-21\Media\PrePlans` are available. See "Floor Plans, Pre-Plans, and Response Graphics" on page 5-3 for more information on pre-plan files. The pre-plan image is displayed on the left side of the window.



6 Click **Done**.

To add dispatch instructions to a response plan

1 In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the response plan dispatch instructions.

2 Click the Response Plans tab.

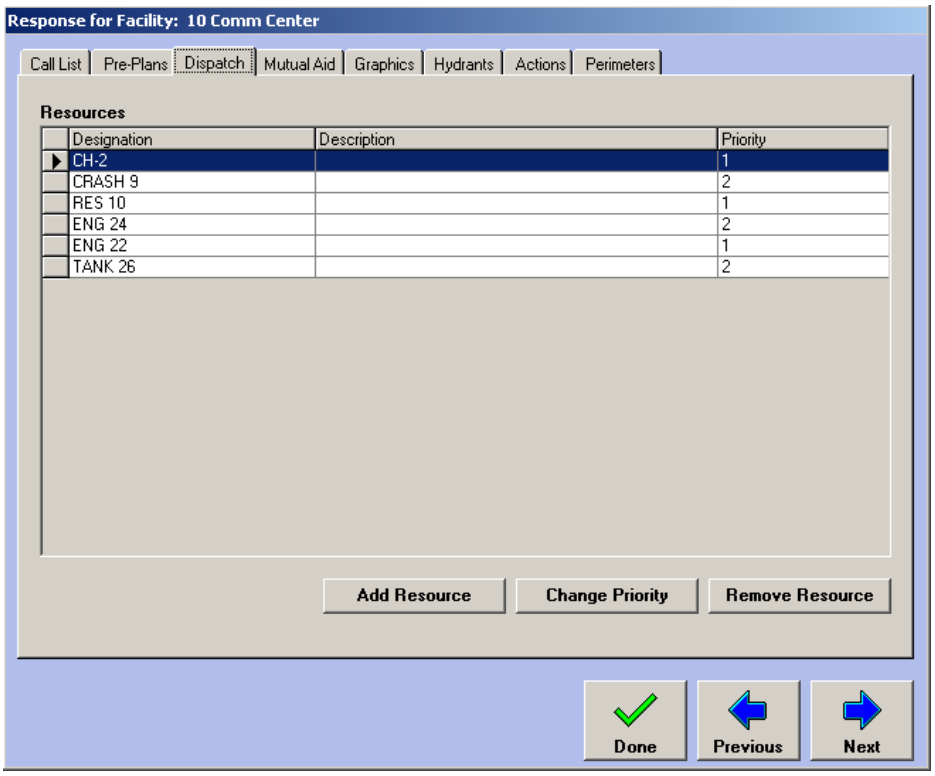
3 Do one of the following:

- Click **Add** to add a new response plan.

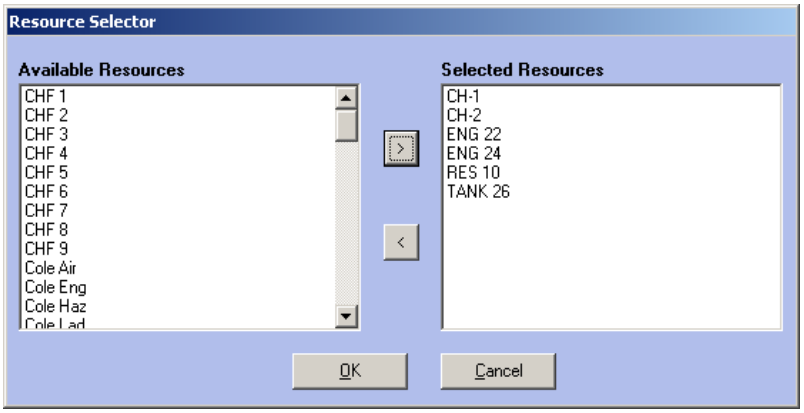
OR

- Select an existing response plan and click **Edit** to add dispatch instruction to the selected response plan.

4 Click the Dispatch tab.



5 Click **Add Resource**. The Resource Selector dialog box appears.



6 In the Available Resources list, select the resources you want to add to the response plan.

7 Click the **>** button to add the resources to the Selected Resources list.

8 Click **OK**.

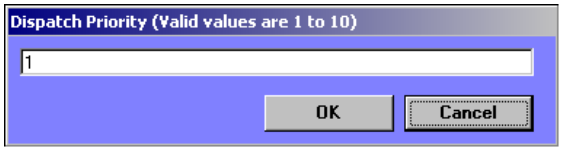
NOTE *See "Dispatch Configuration" on page 3-58 for more information about dispatch options.*

To change the dispatch priority of a resource

Use resource priority to specify the response wave in which a resource should be dispatched during an incident. By default, all resources added to a response plan are given priority 1.

1 Select the resource in the list on the response plan's Dispatch tab.

2 Click **Change Priority**. The Dispatch Priority dialog box appears.



3 Enter a number to specify the dispatch priority.

4 Click **OK**.

NOTE *Priority 1 resources are assigned by default to incidents to which the response plan is applicable when the dispatch mode is by response plan. See "Dispatch Modes" on page 3-59.*

To add mutual aid resources to a response plan

1 In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the response plan mutual aid resources.

2 Click the Response Plans tab.

3 Do one of the following:

- Click **Add** to add a new response plan.

OR

- Select an existing response plan and click **Edit** to add the mutual aid resources to the selected response plan.

4 Click the Mutual Aid tab.

5 Enter the desired information in the text box.

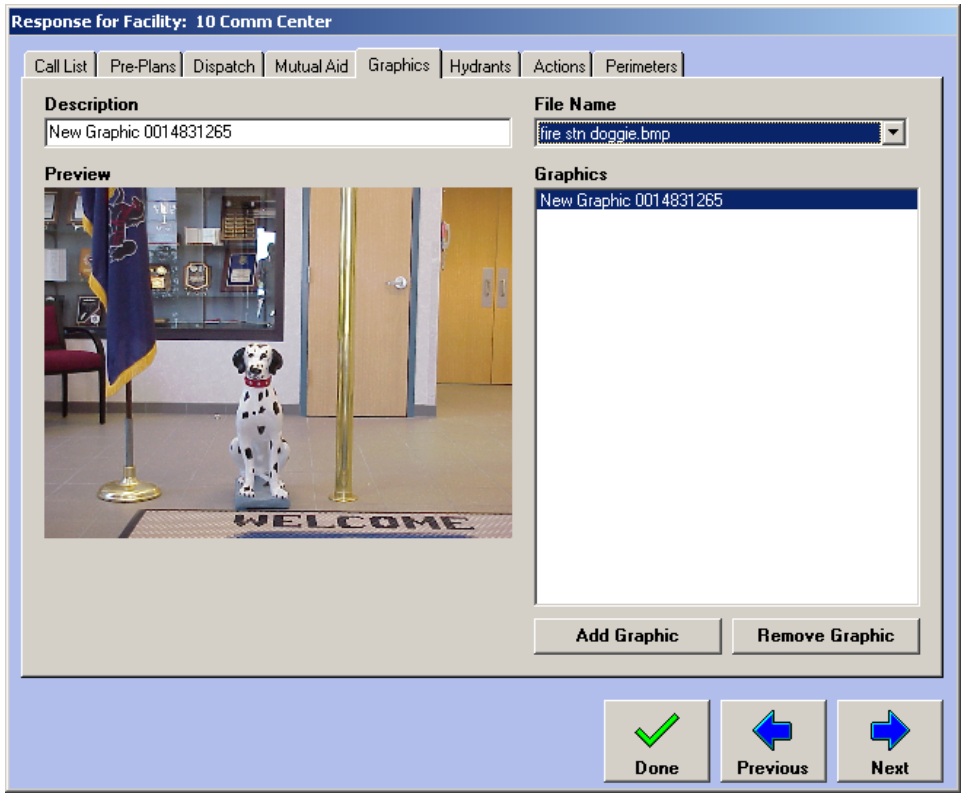
6 Click **Done**.

To add graphics to a response plan

NOTE *The graphics being added to a response plan must be located in* `C:\Program Files\D-21\Media\ResponseGraphics`.

1. In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the response plan graphic.
2. Click the Response Plans tab.
3. Do one of the following:
   - Click **Add** to add a new response plan.

   OR
   - Select an existing response plan and click **Edit** to add the graphic to the selected response plan.
4. Click the Graphics tab.



5. Click **Add Graphic** to add a file to the Graphics list.
6. **Description** Delete the default New Graphic name and enter a meaningful name for the graphic.

7 **File Name** Select an image file. Only image files in the `\D-21\Media\ResponseGraphics` folder are available in this list. To add to the available graphics, see "Floor Plans, Pre-Plans, and Response Graphics" on page 5-3.

8 Click **Done** when you are finished adding graphics to the response plan.

To add hydrant information to a response plan

NOTE *You must add a hydrant to the D-21 database before it is available to add to a response plan. See "Hydrants" on page 2-109.*

1 In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the response plan hydrant information.

2 Click the Response Plans tab.

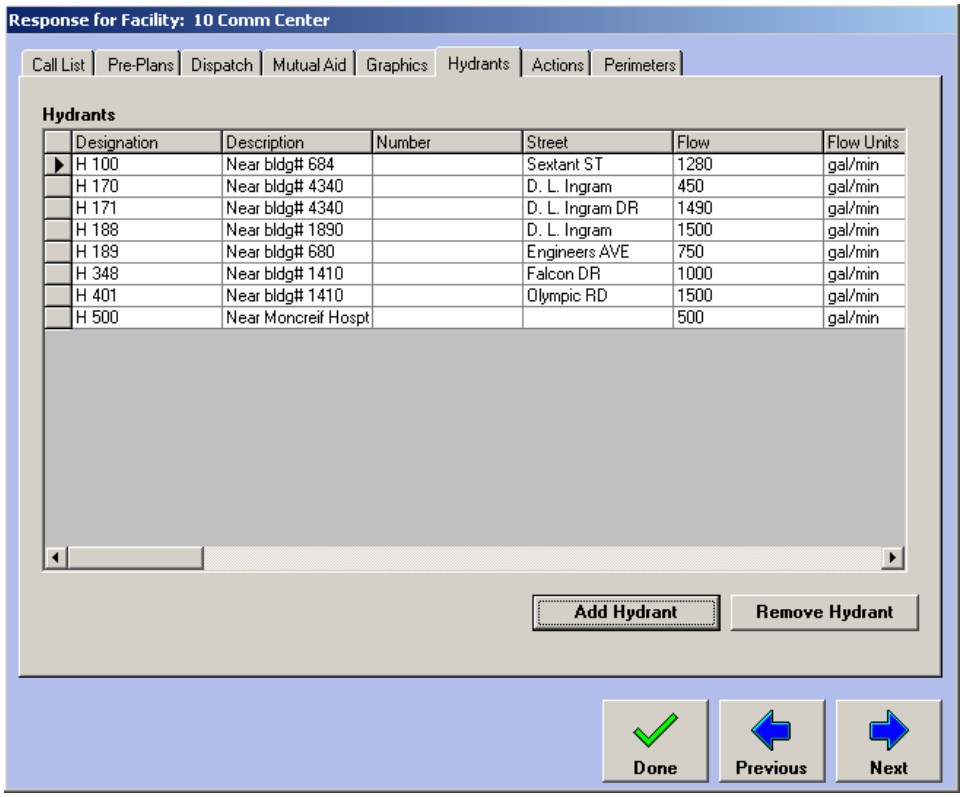
3 Do one of the following:

- Click **Add** to add a new response plan.

OR

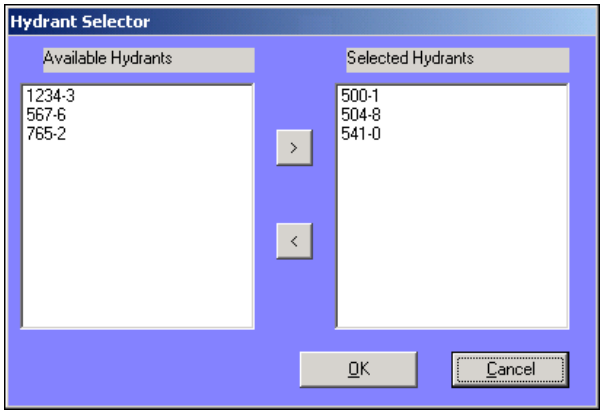
- Select an existing response plan and click **Edit** to add the hydrant to the selected response plan.

4 Click the Hydrants tab.



NOTE *The Hydrant tab is not available for EMS emergency card response plans.*

5 Click **Add Hydrant**. The Hydrant Selector dialog box appears.



6 In the Available Hydrants list, select the hydrant you want to add to the response plan.

7 Click the **>** button to move the selected hydrant to the Selected Hydrants list.

8 Click **OK**.

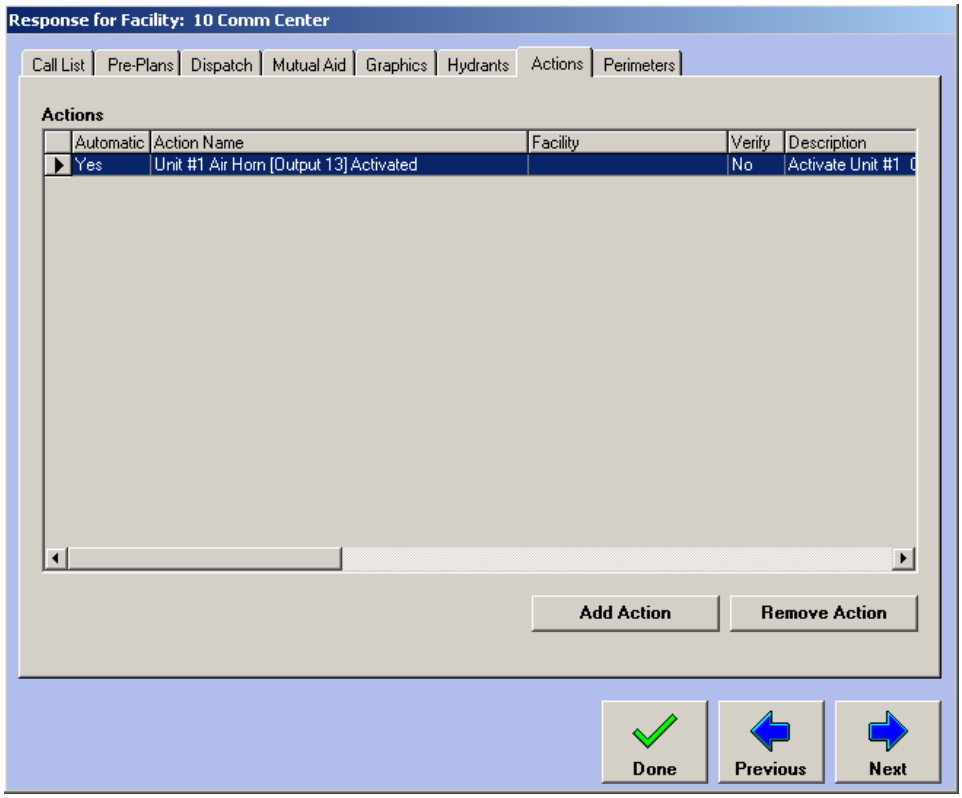
9 Click **Done** in the Response Plan dialog box.

To add an action to a response plan

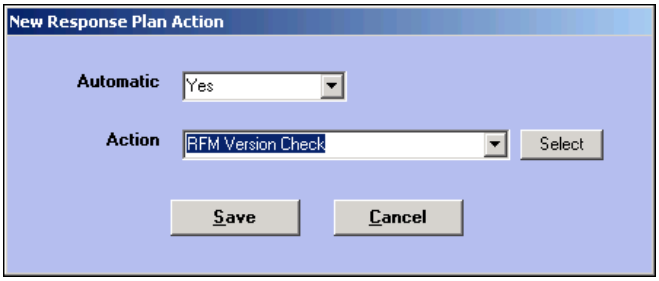
NOTE *You cannot attach Run External Command actions to response plans. You can only attach RID and Reminder actions.*

1. In the tree pane, right-click the site, facility, zone, or emergency card to which you want to add the response plan action.
2. Click the Response Plans tab.
3. Do one of the following:
   - Click **Add** to add a new response plan.

   OR
   - Select an existing response plan and click **Edit** to add the action to the selected response plan.
4. Click the Actions tab.



5 Click **Add Action**. The New Response Plan Action dialog box appears.



- **Automatic** If you want the action carried out automatically when an incident is created, select Yes.
- **Action** Select the action you want to include in your response plan. Only actions that are already created can be seen in the list of available actions. For information on creating actions, see "Using Actions" on page 3-27. To find an action in the list, click **Select**.

NOTE *To change whether an action that is already in the list occurs automatically, remove the action and add it again.*

6 Click **Save**.

7 When you have added all the desired actions, click **Done** to close the Response Plan dialog box.

To add perimeters to a response plan

1 In the tree pane, right-click the facility or zone to which you want to add the response plan action.

2 Click the Response Plans tab.

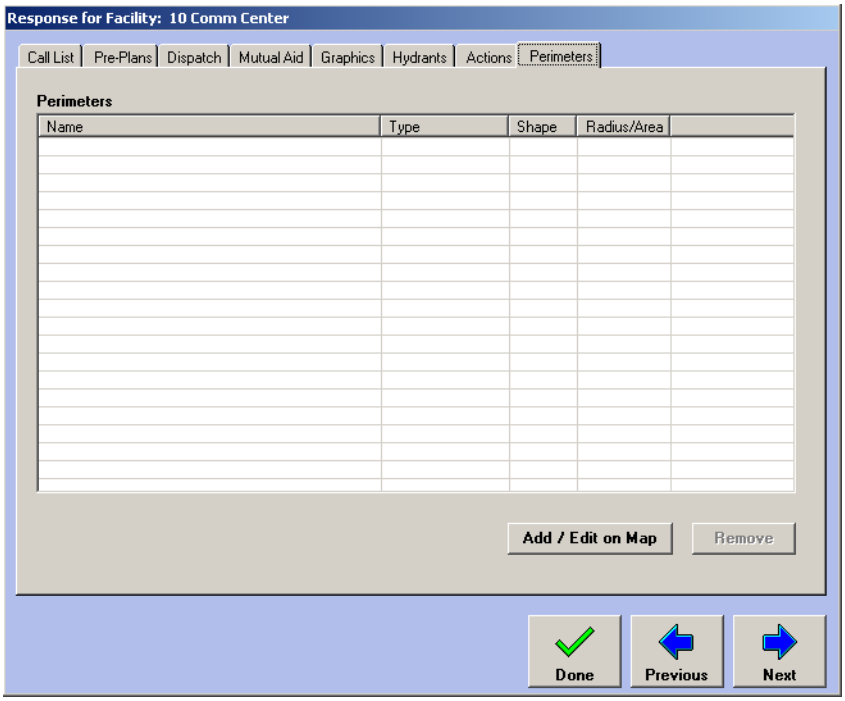
3 Do one of the following:

- Click **Add** to add a new response plan.

OR

- Select an existing response plan and click **Edit** to add the perimeter to the selected response plan.

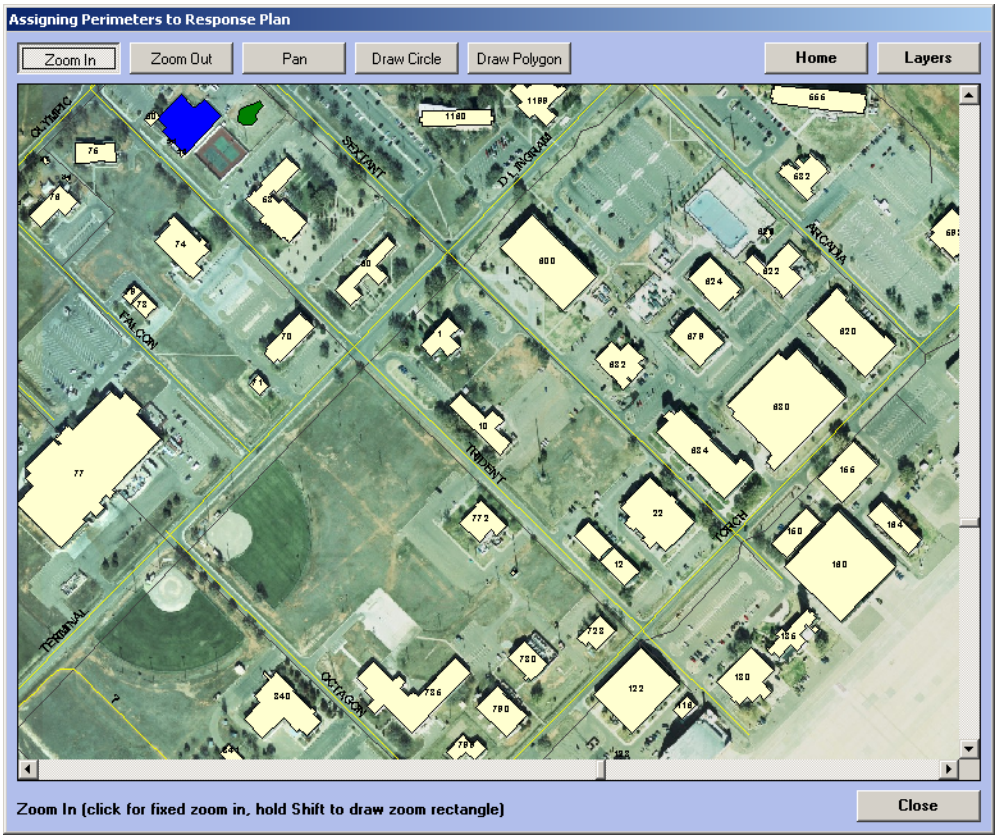
4 Click the Perimeters tab.



NOTE *Perimeters are not available on site or emergency card response plans.*

5 To add a Perimeter click the **Add / Edit on Map** button

6 The Assigning Perimeters to Response Plan window appears.



7 The buttons at the top of the window activate tools you use to create a perimeter.

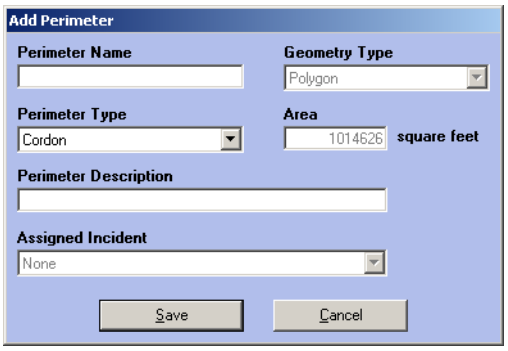
- **Zoom In** and **Zoom Out** buttons activate the magnifying glass tool.
- The **Pan** button allows the user to move the map in any direction (left, right, up, down).
- The **Draw Circle** and **Draw Polygon** buttons allow the user to draw a perimeter.
- The **Home** button returns the map to its original magnification and position.
- The **Layers** button allows the user to turn on and off individual Map Layers in the display.

8 Use the **Zoom In**, **Zoom Out**, and **Pan** buttons to find the area of the map where the perimeter will be drawn.

9 Click **Draw Circle** or **Draw Polygon**. The mouse pointer changes to a cross-hair.

- To draw a **Circular Perimeter**, select a point on the map by clicking and holding the left mouse button. Drag the mouse until the perimeter is the desired size. Release the mouse button.
- To draw a **Polygonal Perimeter**, select a point on the map and click the left mouse button. Continue to click the left mouse button while tracing the perimeter outline. When the last point is reached, double click the point to complete the perimeter.

10 When the perimeter is complete the Add Perimeter dialog box will appear.



11 Fill in the Perimeter name, select the Perimeter Type (Cordon, Hazmat, Mass Notification), and enter a Perimeter Description.

12 Click **Save.**

13 Click **Close** to finalize the settings.

To remove a response plan perimeter

1 Select the Perimeter from the list.

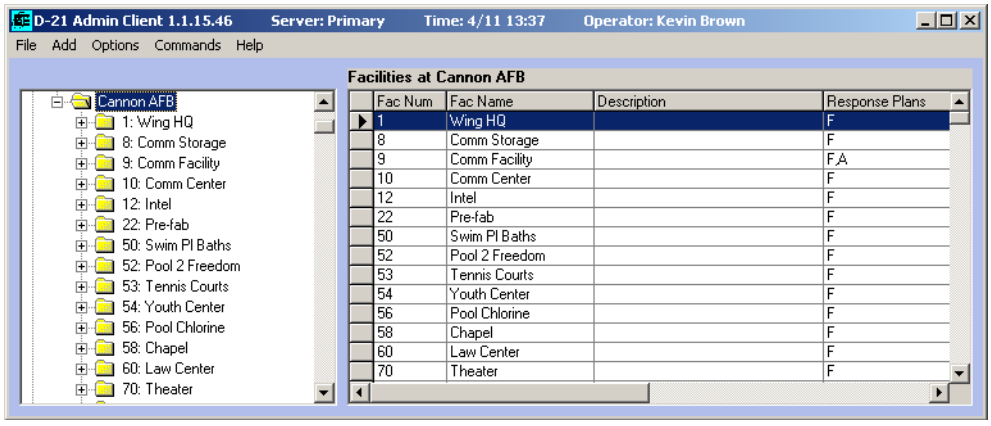
2 Click **Remove.**

3 Click **Yes** when asked if you are sure you want to remove the perimeter.

To view facilities with response plans attached

1 In the tree pane, click the plus sign (**+**) next to Sites to expand the list of sites.

2 Click the site with the facilities you want to display. The Details pane on the right side of the window displays the list of facilities for the site.



The Response Plans field displays the class of each response plan attached to the facility. If the field is blank, the facility does not have a response plan. The classes are abbreviated as follows:

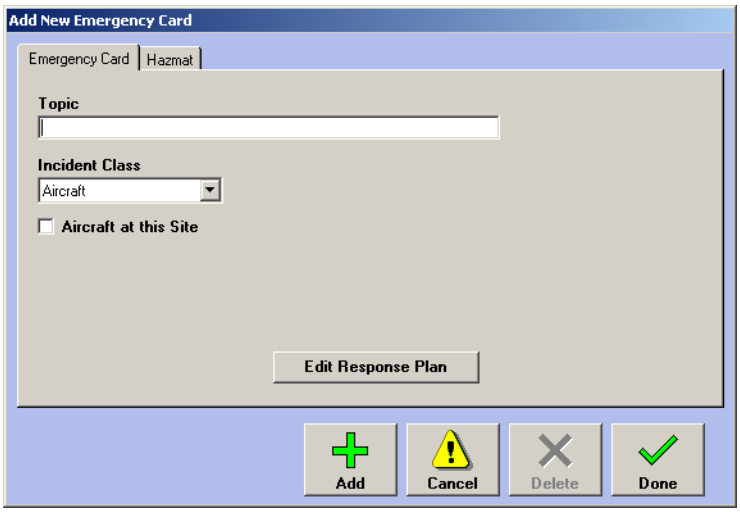
Abbreviation	Response Plan Class
F	Fire
FX	Fire Auxiliary
S	Security
SX	Security Auxiliary
A	Aircraft
H	HazMat
E	EMS

Emergency Cards

An emergency card associates a response plan with a topic. Topics are assigned to an incident by operators when they create incidents in the D-21 Incident Client. In the D-21 Fire system, operators use emergency cards for standard response plans not associated with a facility or zone. For example, an operator could create an emergency card for an earthquake or a wild animal attack and then build a response plan for these scenarios.

In the D-21 Security Client with Law Enforcement, operators use emergency card topics to create custom incident types for each type of security incident an organization handles. Then they can create a separate response plan for each type of incident.

Figure 3-1 *Add New Emergency Card dialog box*



To add an emergency card

1. Select **Add > Emergency Card**.
2. Enter a name for the Topic.

3 Select the Incident Class from the drop-down list. Use the Security class if you are creating incident types for Law Enforcement incidents.

NOTE *The topic is associated with the specified incident class. When an incident is created in the D-21 Incident Client, the list of topics available to the operator is determined by the class. If the class of incident is Security, only topics associated with the Security incident class are available to the operator.*

4 For aircraft emergency cards, the **Aircraft at this Site** check box should be checked to indicate the aircraft defined in the Topic can be found at the site.

NOTE *Using the Aircraft at this Site checkbox allows the operator to choose from a smaller list of possible aircraft when responding to an incident.*

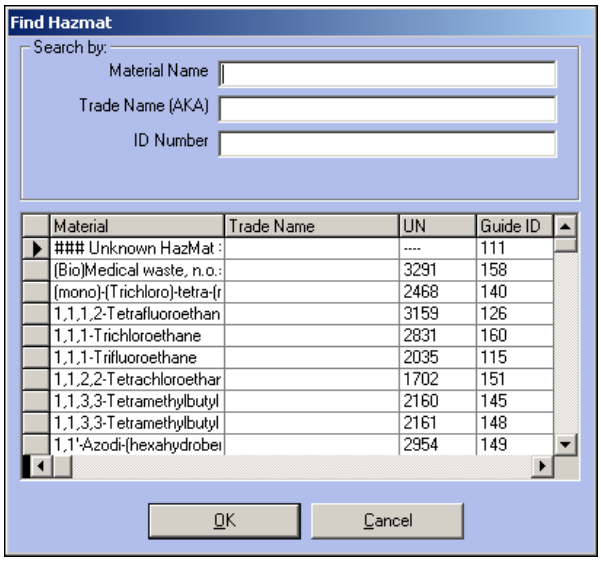
5 Click **Edit Response Plan**. For information on using the Response dialog box, see "Response Plans" on page 3-2.

6 Click the **Hazmat Tab** to enter Hazmat information if needed. HazMats can be associated with all classes of emergency cards.

7 Click **Add HazMat**.

8 Use the Find HazMat screen to locate the HazMat material to be added to the emergency card. Select the HazMat by clicking on it and then click **OK**.

Figure 3-2 *Add HazMat dialog box*



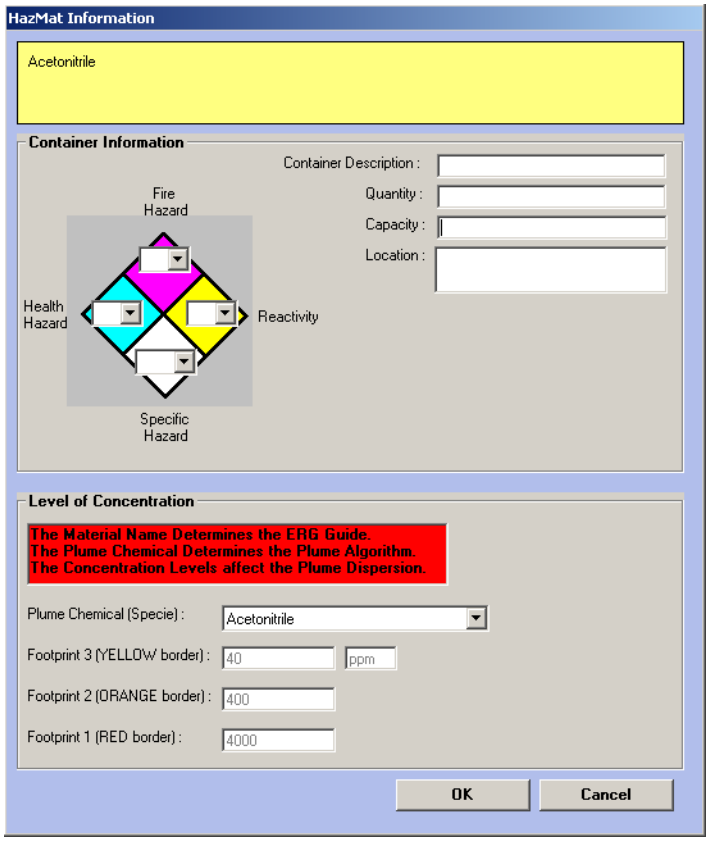
To edit an emergency card HazMat

1 In the tree pane, click Emergency Cards. Click the type of Emergency Card desired, and then right-click the emergency card for which you want to edit the HazMat information.

2 Click the **Hazmat** tab.

3 Locate the material in the HazMat list, and click the material to select it.

4 The HazMat Information window appears.



5 Fill in the appropriate information for Container and Level of Concentration.

6 When you are finished editing the HazMat, click **Done**.

To remove an emergency card HazMat

1 In the tree pane, click Emergency Cards. Select the type of Emergency Card desired then right-click the emergency card for which you want to edit the HazMat information.

2 Click the **Hazmat Tab.**

3 Locate the material in the HazMats list, and click the material to select it.

4 Click **Remove HazMat.**

5 In the Delete Chemical dialog box click **Yes.**

6 Click **Done.**

To edit an emergency card

1 In the tree pane, right-click the emergency card you want to edit. The Emergency Card dialog box appears.

2 Change dialog box entries and selections as desired. For more information on the dialog box, see "To add an emergency card" on page 3-20.

3 Click **Done**.

To delete an emergency card

1. In the tree pane, right-click the emergency card you want to delete. The Emergency Card dialog box appears.
2. Click **Delete**. A confirmation message appears.
3. Click **Yes**.

Pre-Plans

A pre-plan contains information responders need to know about a facility to which they may be dispatched. In a pre-plan you can store information about the construction of a facility, its fire and security systems, hazardous materials it contains, and more.

The D-21 provides two ways to attach pre-plans to a facility. You can use Monaco pre-plan templates to create pre-plans in the D-21 Admin Client for each response plan, or you can attach existing pre-plan files that were created in other software applications. The D-21 database is configured by Monaco to either use pre-plan templates with response plans or pre-plan files, but not both.

NOTE *Contact Monaco technical support for assistance with configuring your database to use Monaco pre-plan templates.*

For more information on working with pre-plan files, see:

- "Importing Floor Plans, Response Graphics, and Pre-Plans" on page 5-5.
- "To add a pre-plan file to a response plan" on page 3-7.

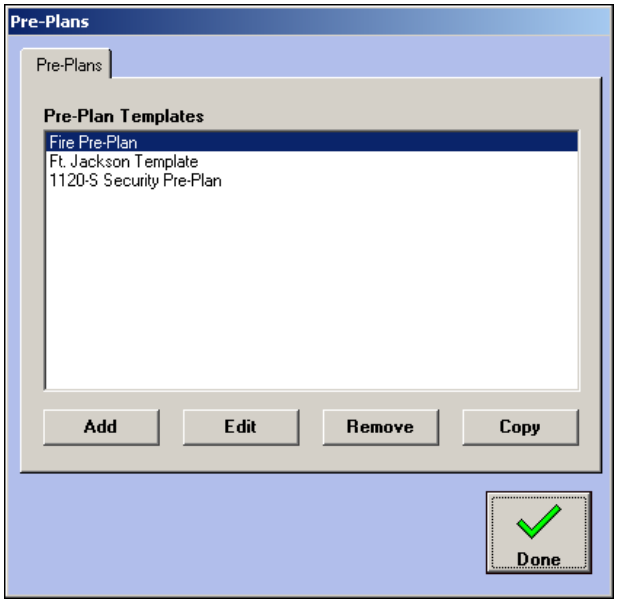
This section describes how to edit an existing pre-plan template to make a new template for use with your response plans. For information on adding a pre-plan based on one of these templates to a specific response plan, see "To add a Monaco pre-plan to a response plan" on page 3-5.

Monaco provides pre-plan templates that can be modified for each response plan you attach to a site, facility, zone, or emergency card. Changes you make to the pre-plan template for a specific response plan are saved with that response plan; the original pre-plan template provided by Monaco can be used again for creating other pre-plans.

IMPORTANT *The Options > Pre-Plans command is only available if you are using the pre-plan templates supplied by Monaco. For information on obtaining templates, contact Monaco support.*

To edit a pre-plan template

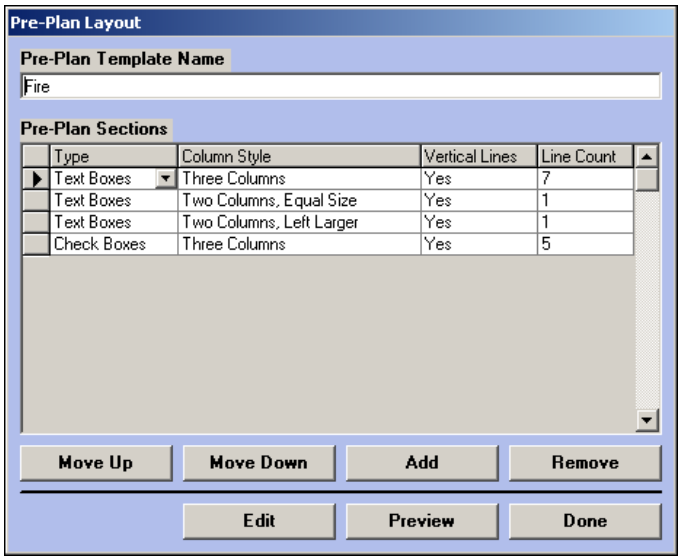
1 Select **Options > Pre-Plans**. The Pre-Plans dialog box appears.



2 Select the pre-plan you want to edit, and click **Edit**. The Pre-Plan Layout dialog box appears.

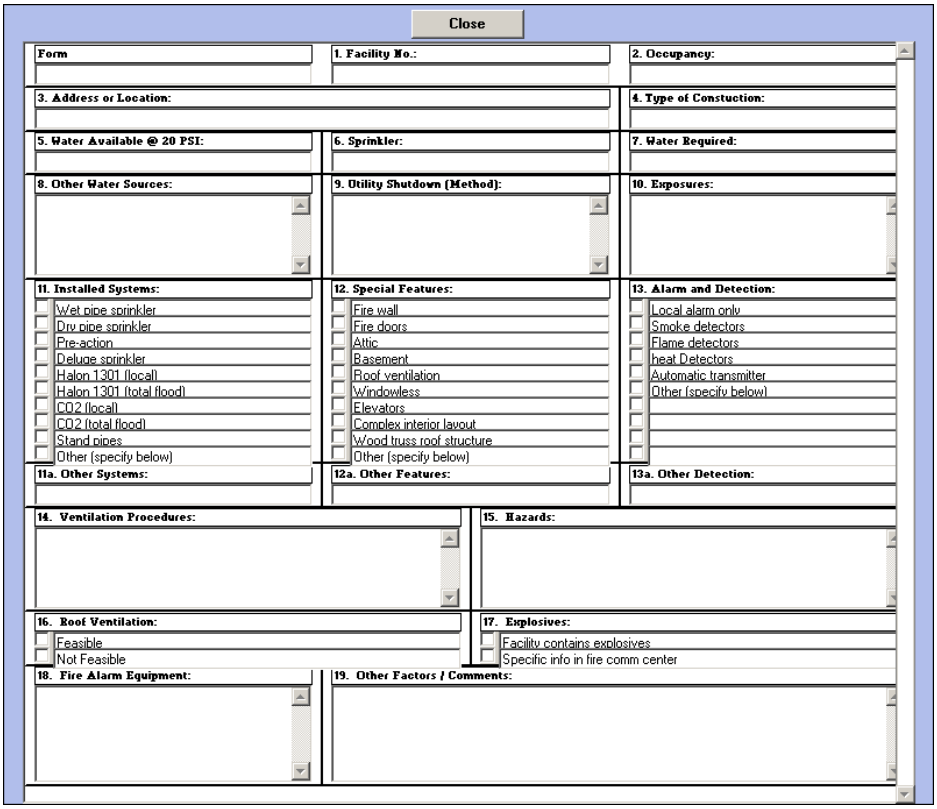
3 The Pre-Plan Template Name can be changed in the Pre-Plan Template Name field.

NOTE *Monaco provides the pre-plan layout. To obtain a modified layout, contact Monaco support.*



- **Pre-Plan Template Name** Enter a new name for the template, if desired.
- **Pre-Plan Sections** Each line in the grid represents a section of the pre-plan template. Each section has the following elements:
  - **Type** A section can consist of text boxes or check boxes, but not both. The number of items included in the section depends on the Column Style and Line Count settings.
  - **Column Style** Provides five different column configurations for the section. If you select the Three Columns style for a section with text boxes, the section will have three text boxes of equal size.
  - **Vertical Lines** Select Yes to place vertical rules between each text or check box in the section. Select No to omit lines between items in the section.
  - **Line Count** Enter the number of rows in the section. For example, if you select Text Boxes, specify Three Columns, and enter a line count of 5, the pre-plan will have three columns of text boxes five rows deep.
- **Move Up** Select a section in the Pre-Plan Sections list and click this button to move the entire section higher up on the pre-plan template.
- **Move Down** Select a section in the Pre-Plan Sections list and click this button to move the entire section lower down on the pre-plan template.
- **Add** Adds a new section entry to the Pre-Plan Sections list.
- **Remove** Removes the selected section from the pre-plan template.
- **Preview** Displays an uneditable preview window that shows what the pre-plan template looks like.

4 Click **Edit** to edit the text and check boxes for the specific pre-plan you are creating.



5 Make the following edits to the pre-plan:

- Change text on the pre-plan by selecting it and typing new text.
- Fill out text fields by clicking in the text box and typing text.
- Place a check in check boxes that apply to this pre-plan.

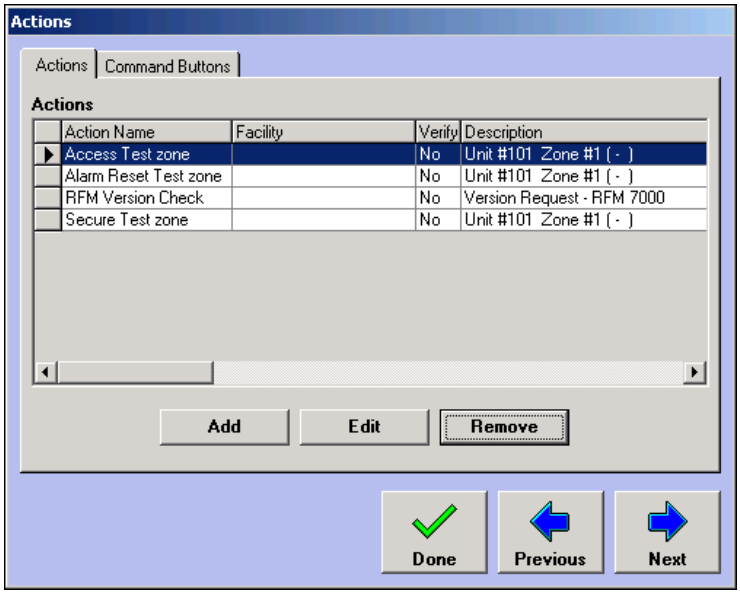
6 Click **Close**. Use the Preview button to double-check the look and content of the pre-plan.

7 Click **Done** when you are finished editing the new pre-plan.

Actions

Use the Actions dialog box to create the actions available in the Actions drop-down list that appears in a variety of locations in the D-21 Admin Client and D-21 Incident Client, and to create buttons for initiating actions in the D-21 Incident Client.

Figure 3-3
Actions dialog box



Using Actions

Actions provide several ways to customize and automate your D-21 system. Actions can be used to control RIDs, units, zones, and outputs, as well as display reminders and run external programs. You can run actions based on status changes such as when an alarm, trouble, or return to normal status occurs with a RID, remote unit, zone, or output. Actions can be attached to response plans and to custom command buttons in the D-21 Incident Client to meet specific needs, and they can also be added to the list of Daily Activities automatically performed by the D-21 at preset times and intervals.

When you add outputs or security zones, the D-21 can automatically create actions for those devices. For more information on adding outputs, see “Outputs” on page 2-74. For more information on working with security zones, see “Setting Up the BT-X Security Unit” on page 9-11.

The D-21 provides four types of actions:

AutoMNS Use an AutoMNS action to schedule an MNS message to play automatically at a scheduled time or when a specific zone’s status changes. See “Configuring AutoMNS in the D-21” on page 7-29.

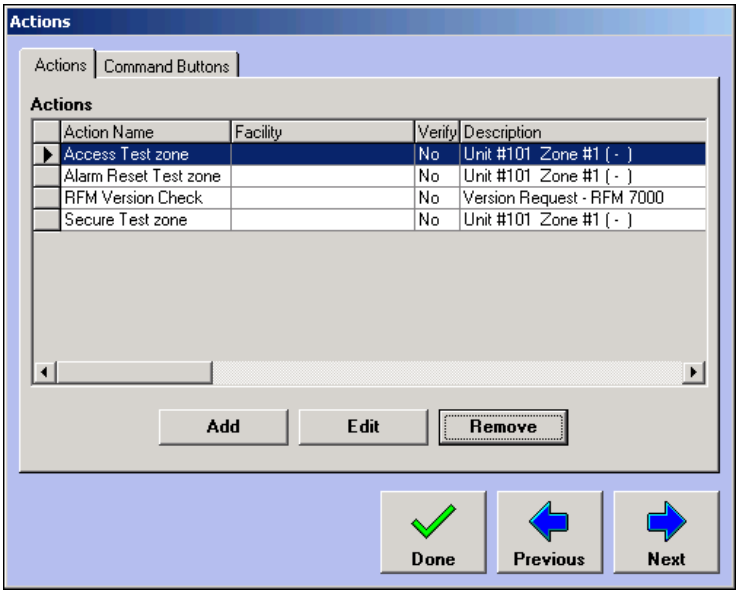
Remote Command Use a Remote Command action to send a command to RIDs, remote units, and outputs. You can also create actions that send Access, Secure, and Alarm Reset commands to security units and zones. See the D-21 Incident Client User Guide (P/N 001-392-00) for more information on RID and remote unit commands. See "To create a Remote Command action" on page 3-29.

Run External Program Use a Run External Program action to launch a Windows-based program. Run External Program actions can be attached to custom buttons that are available in the right button bar in the D-21 Incident Client or scheduled from the Actions pane in the Daily Activities window. However, Run External Program actions cannot be attached to response plan status changes. See "To create a Run External Program action" on page 3-32.

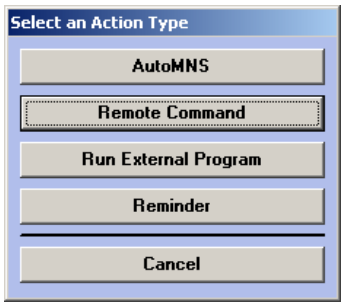
Reminder Use a Reminder action to generate an administrator-defined message that appears only to the person or workstations specified by the administrator. "To create a Reminder action" on page 3-34.

To create an AutoMNS action

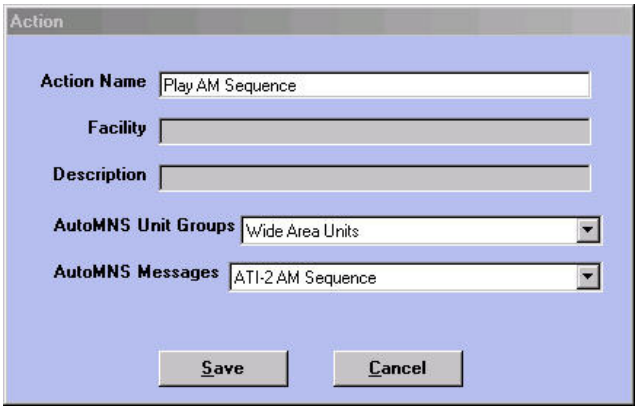
1 Select **Options > Actions**. The Actions dialog box appears.



2 Click **Add**. The Select an Action Type dialog box appears.



3 Click **AutoMNS**. The AutoMNS Action dialog box appears.



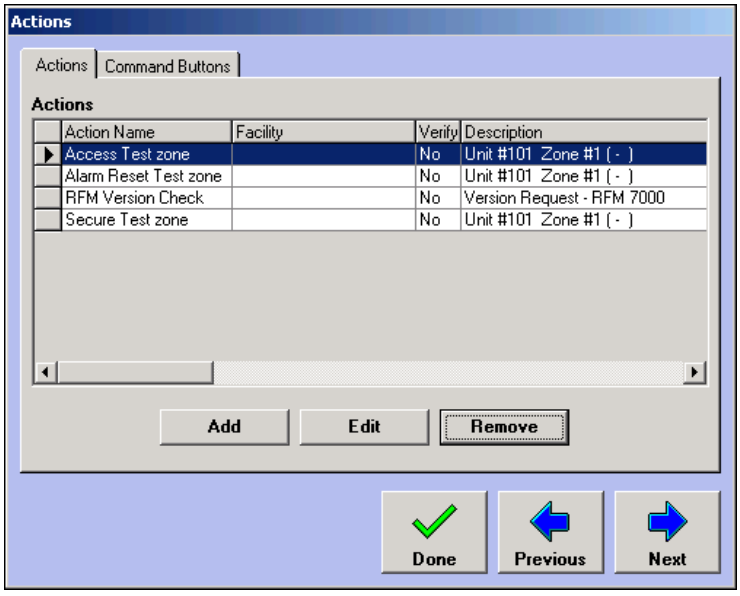
- **Action Name** Enter a name for the action. This name identifies the action throughout the D-21. Use a name that is easily identifiable.
- **AutoMNS Unit Groups** Select the remote unit group which should play the AutoMNS Message. See "To add an AutoMNS unit group" on page 7-29.
- **AutoMNS Messages** Select the MNS message which should play. See "To add an AutoMNS message" on page 7-31.

4 When you are finished, click **Save**.

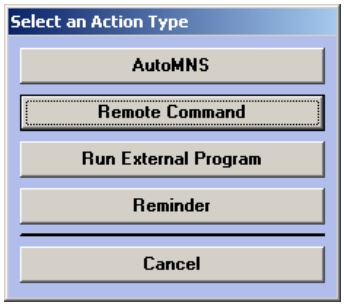
5 Click **Done**.

To create a Remote Command action

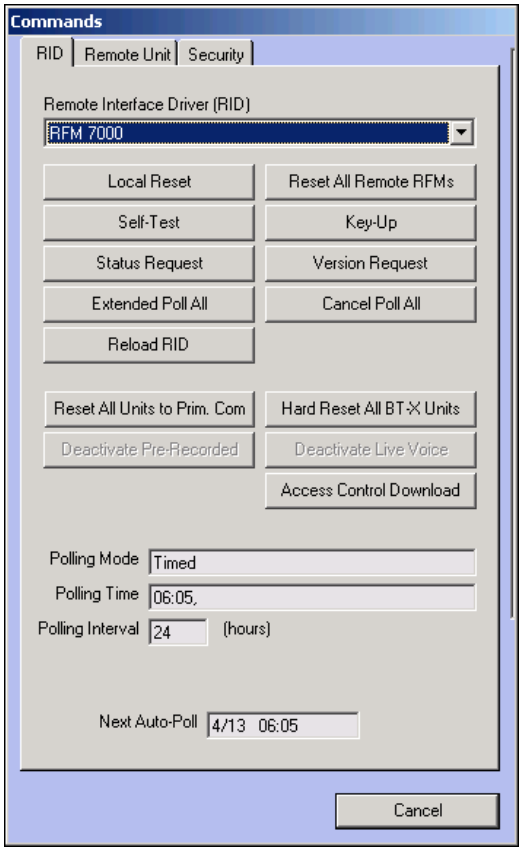
1 Select **Options > Actions**. The Actions dialog box appears.



2 Click **Add**. The Select an Action Type dialog box appears.



3 Click **Remote Command**. The Commands dialog box appears.



See the D-21 Incident Client User Guide (P/N 001-392-00) for more information on the commands that are available for each of the RIDs

NOTE *The Security tab only appears if the D-21 Security Client is enabled on this workstation.*

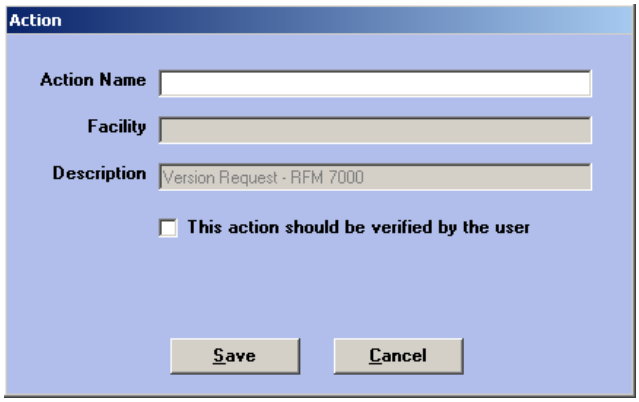
4 Do one of the following:

- If you want to create an action for a RID, click the RID tab and select the specific RID from the Remote Interface drop-down list.

OR

- If you want to create an action for a remote unit or output, click the Remote Unit tab and select the facility, remote unit, or output for which you want to create the action.

5 Click the command button you want the action to use. The Action dialog box appears.



- **Action Name** Enter a name for the action. This name identifies the action throughout the D-21. Use a name that is easily identifiable.
- **Facility** Displays the facility in which the action will take place.
- **Description** Displays the command selected for the action.
- **This action should be verified by the user** Check this box if you want the D-21 Incident Client operator to be prompted before the action is performed.

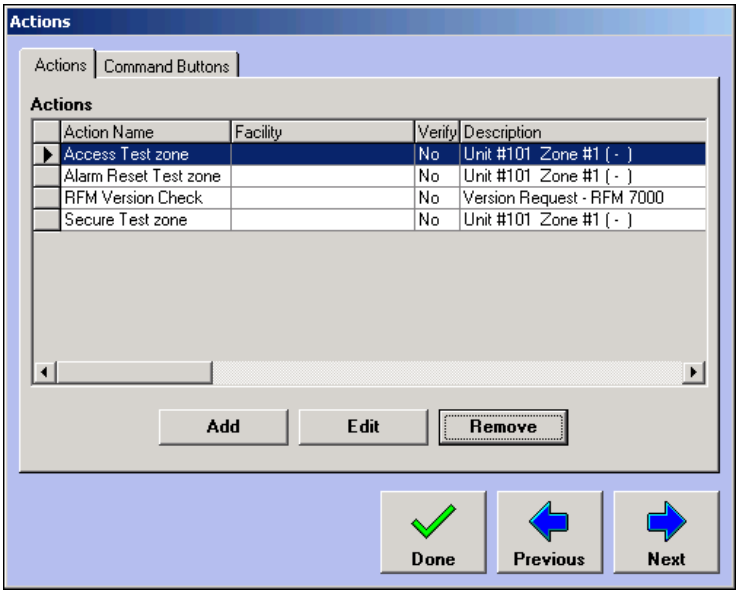
6 When you are finished, click **Save**.

7 Click **Done**.

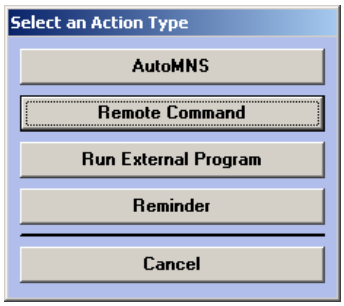
To create a Run External Program action

NOTE *You cannot attach an external program action to a response plan status change.*

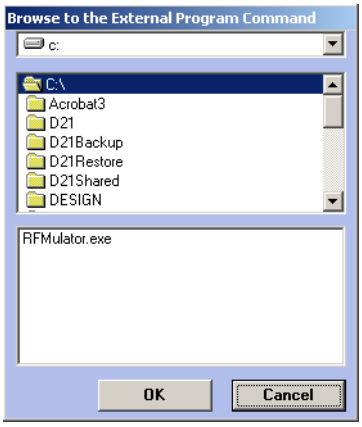
1 Select **Options > Actions**. The Actions dialog box appears.



2 Click **Add**. The Select an Action Type dialog box appears.



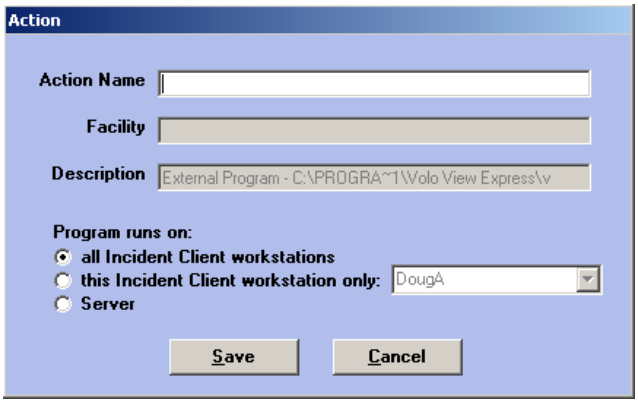
3 Click **Run External Program**. The Browse to the External Programs Command dialog box appears.



4 Browse to the desired executable file and select it.

NOTE *Only executable files can be launched by an action; executable files have a* `.exe` *extension.*

5 Click **OK**. The Action dialog box appears



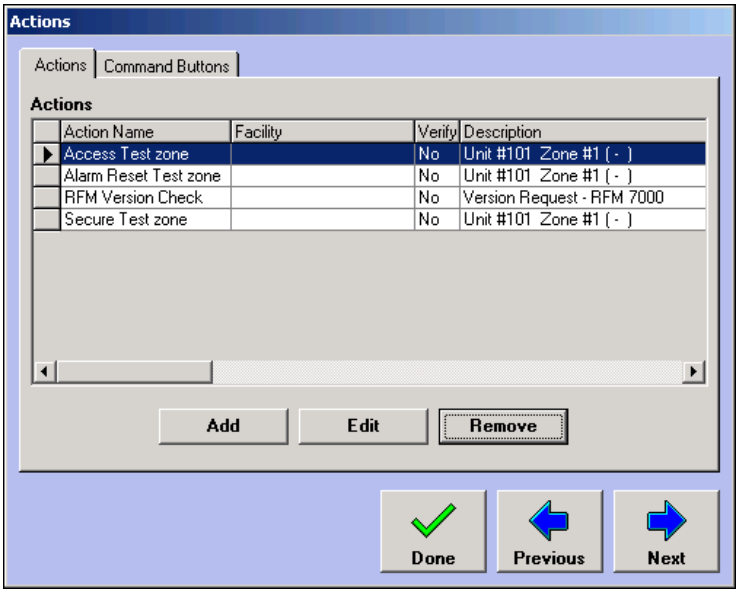
- **Action Name** Enter a name for the action. This name identifies the action throughout the D-21. Use a name that is easily identifiable.
- **Description** Displays the command selected for the action.
- **Program runs on** Select the appropriate radio button for where you want the external program to operate from (for example: all logged in workstations, one particular workstation, the server).

6 When you are finished, click **Save**.

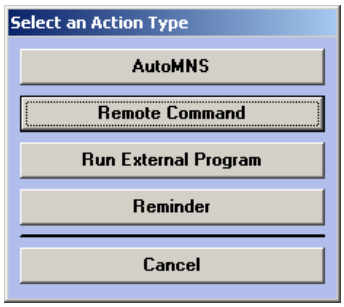
7 Click **Done**.

To create a Reminder action

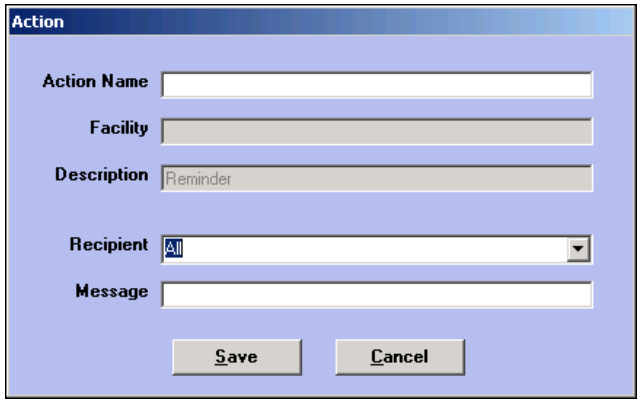
1 Select **Options > Actions**. The Actions dialog box appears.



2 Click **Add**. The Select an Action Type dialog box appears.



3 Click **Reminder**. The Action dialog box for reminders appears.



- **Action Name** Enter the name of the reminder action.
- **Description** Displays the type of action.

- **Recipient** Select the person or workstation who should see the reminder.
- **Message** Enter the text of your reminder message.

4 When you are finished, click **Save**.

5 Click **Done**.

To rename an action

1 Select **Options > Actions**. The Actions dialog box appears.

2 Select the action to be renamed and click **Edit**. The Action dialog box appears.

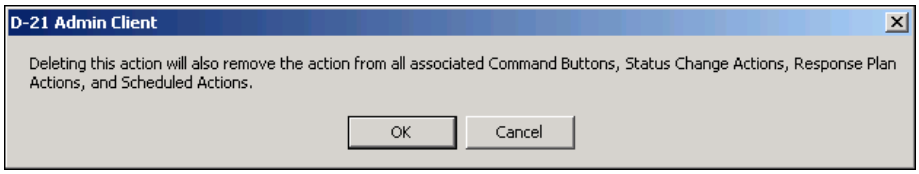
3 Modify the action name as desired and click **Save**. The modified name of the action appears in the Actions dialog box.

4 Click **Done**.

To remove an action

1 Select **Options > Actions**. The Actions dialog box appears.

2 Select the action you want to remove and click **Remove**. The following message appears:



3 Click **OK**.

4 In the Actions dialog box, click **Done**.

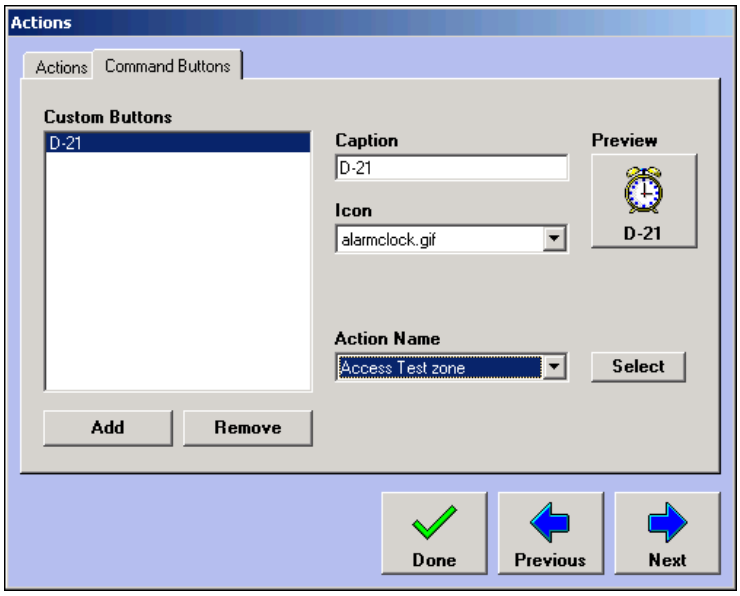
Attaching Actions to Custom Buttons

Administrators can create custom buttons that appear on the right button bar in the D-21 Incident Client.

Before you begin The action you want to associate with the new button must be defined before you create the button. See "Using Actions" on page 3-27.

To create a custom button for an action

1. Select **Options > Actions**. The Actions dialog box appears.
2. Click the Command Buttons tab.



3. Click **Add**.
4. In the Caption box, enter the text you want to appear on the button.
5. Select the desired action from the Action drop-down list.
6. Select the desired icon from the Icon drop-down list. You can scroll through the available icons by selecting the icon box and then using the up and down arrow keys.

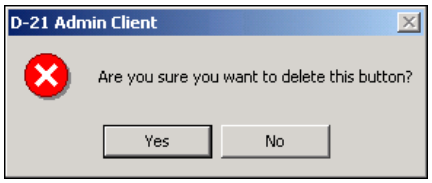
NOTE *To add to the list of available icons, see "Icons" on page 5-12.*

7. Click **Done**.

To remove a custom button

1. Select **Options > Actions**. The Actions dialog box appears.
2. Click the Command Buttons tab.

3 In the Custom Buttons box, select the button you want to remove and click **Remove**. A message appears, asking whether you want to remove the button.



4 Click **Yes**.

5 Click **Done**.

To edit a custom button

1 Select **Options > Actions**. The Actions dialog box appears.

2 Click the Command Buttons tab.

3 In the Custom Buttons box, select the name of the button you want to edit.

4 Modify the entries you want to change in the Caption, Action, and Icon boxes.

5 To edit a different button, click the name of the button in the Custom Buttons box.

6 After you have modified the button(s) you want to change, click **Done**.

Attaching Actions to Status Changes

By attaching actions to status changes in RIDs, remote units, or zones, you can configure your D-21 system to respond consistently and automatically to input. You can attach actions to alarm, trouble, and normal conditions for zones, and to normal and trouble conditions for RIDs and remote units.

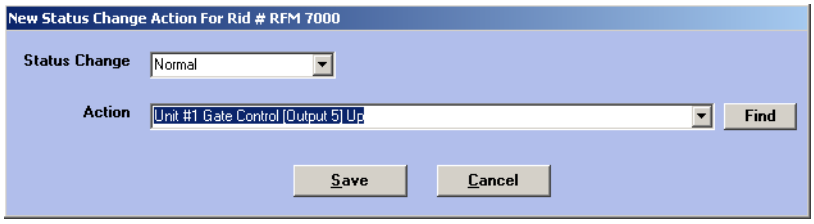
NOTE *An RFM, CPS 484, or remote unit has only two states: normal and trouble; therefore, an action assigned to any of them for "When entering an alarm state" will never occur.*

To associate an action with a status change

1 In the tree pane, right-click a RID, remote unit, or zone to select it. The RID, Remote Unit, or Zone dialog box appears.

2 Click the Actions tab.

3 Click **Add Action**. A dialog box appears from which you can select an action. For information on adding to the list of available actions, see "Using Actions" on page 3-27.



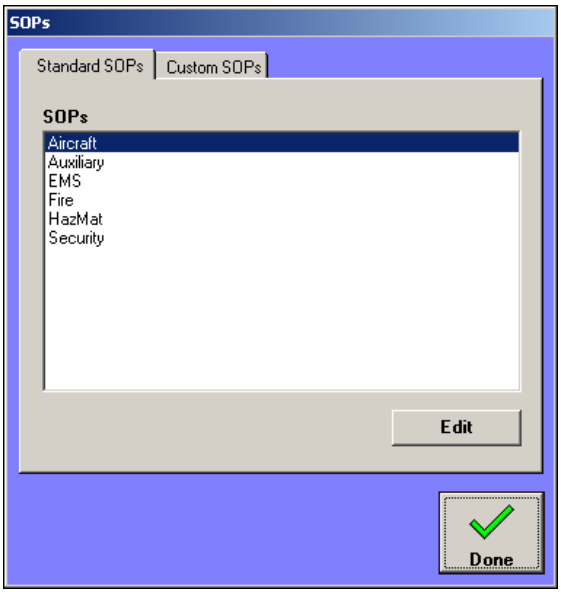
- **Status Change** Select the status condition of the RID, remote unit, or zone which you want to trigger the action.
- **Action** Select the action that you want to run when the selected status condition occurs.

4 Click **Save**.

Standard Operating Procedures (SOPs)

Use the SOP dialog box to edit the standard operating procedures (SOPs) accessible in the D-21 Incident Client. You can edit the standard SOPs that are provided with the D-21, or you can create your own custom SOPs.

Figure 3-4
SOP dialog box



Before you begin If you are creating custom SOPs, you must first create an emergency card for the SOP. See "Emergency Cards" on page 3-20.

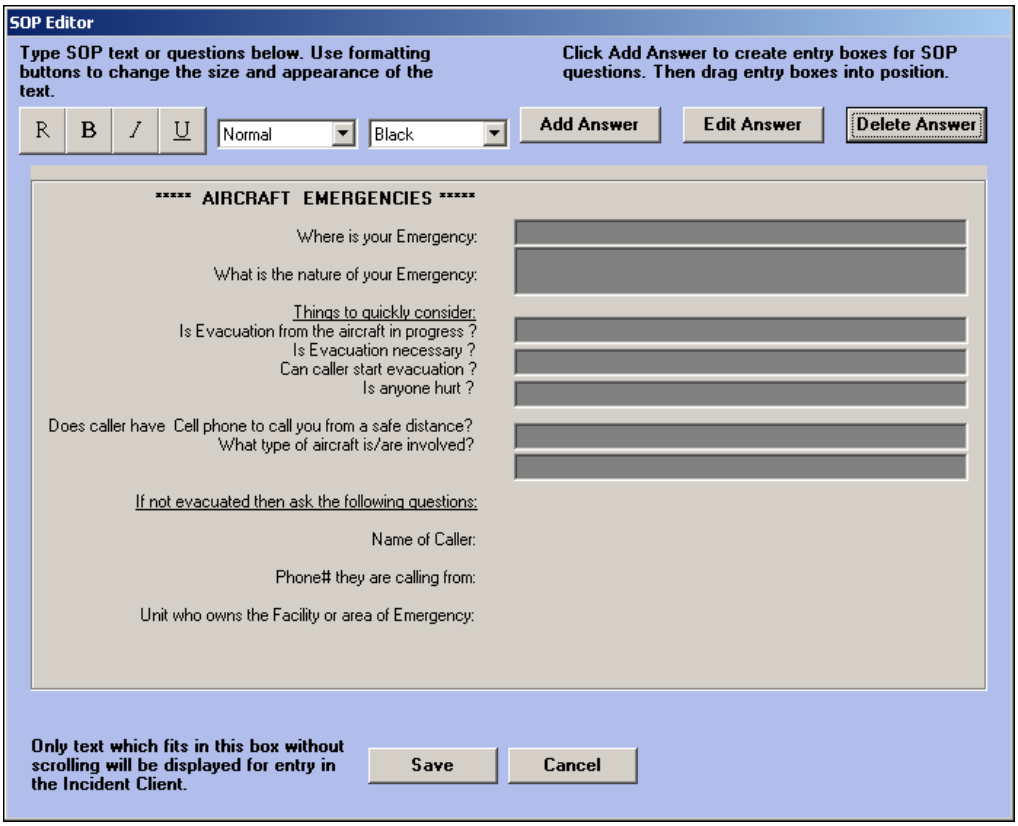
To edit an SOP

1 Select **Options > SOPs**.

2 Select the SOP to edit from either the Standard SOP or Custom SOP tab.

3 Click **Edit**.

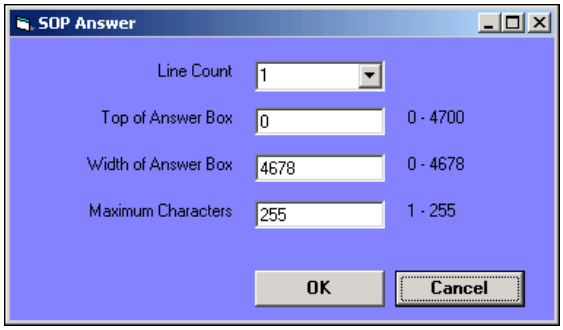
4 The SOP Editor dialog box appears.



5 Edit the text, located on the left side of the dialog box, as desired. The buttons and drop-down lists function as follows:

- **R** Removes bold, italic, and underline attributes.
- **B** Applies the **bold** attribute to selected text.
- **I** Applies the *italic* attribute to selected text.
- **U** Applies the underline attribute to selected text.
- **Size drop-down list** Specifies the size of the text: Normal, Large, or Extra large.
- **Color drop-down list** Specifies the color of selected text: black, red, blue, or green.

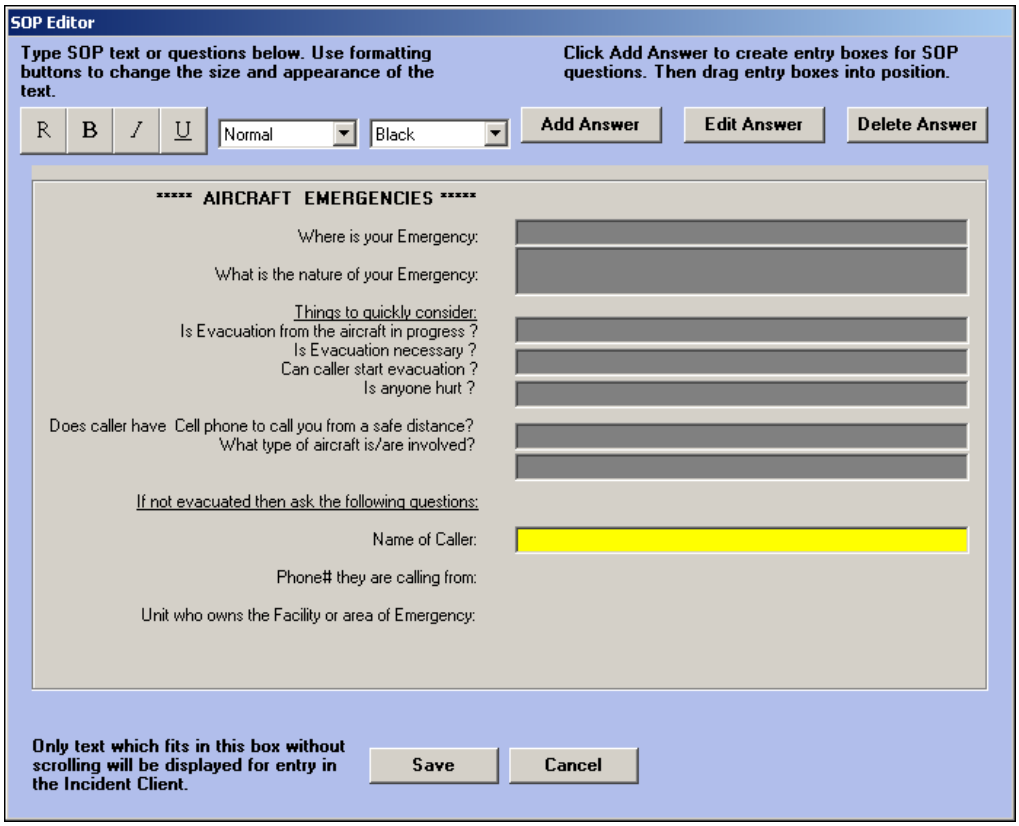
6 Click **Add Answer** to add a text entry box in which operators can type data while processing the incident.



7 Specify the size and position of the answer box.

- **Line Count** Specify the number of lines needed for the answer.
- **Top of Answer Box** Specify the vertical position for the answer box. The position is measured from the top of the SOP text area. You can also position answer boxes manually by dragging the box with the mouse.
- **Width of Answer Box** Specify the width of the answer box. For example, you may want a smaller entry box for questions with yes/no answers.
- **Maximum Characters** Specify the maximum number of characters that can be typed in the answer box. The maximum number of characters that can be allowed is 255.

8 Click **OK**.



9 If necessary, click and drag the answer box with the mouse to reposition.

10 Click **Save**.

11 In the SOP dialog box, click **Done**.

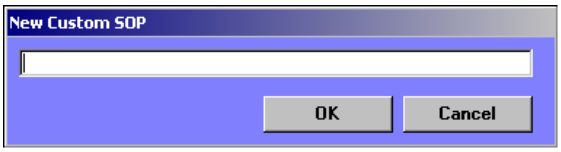
To add a custom SOP

IMPORTANT *You must associate an emergency card with a custom SOP. If you do not have an emergency card set up for the SOP you want to create, see "Emergency Cards" on page 3-20 before starting this procedure.*

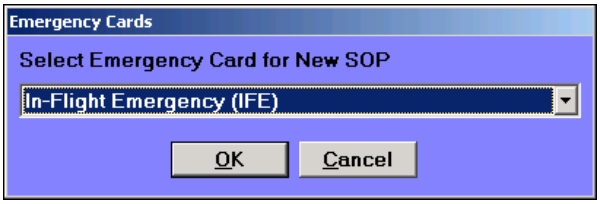
1 Select **Options > SOPs**.

2 Click the Custom SOP tab.

3 Click **Add.** The New Custom SOP dialog box appears.



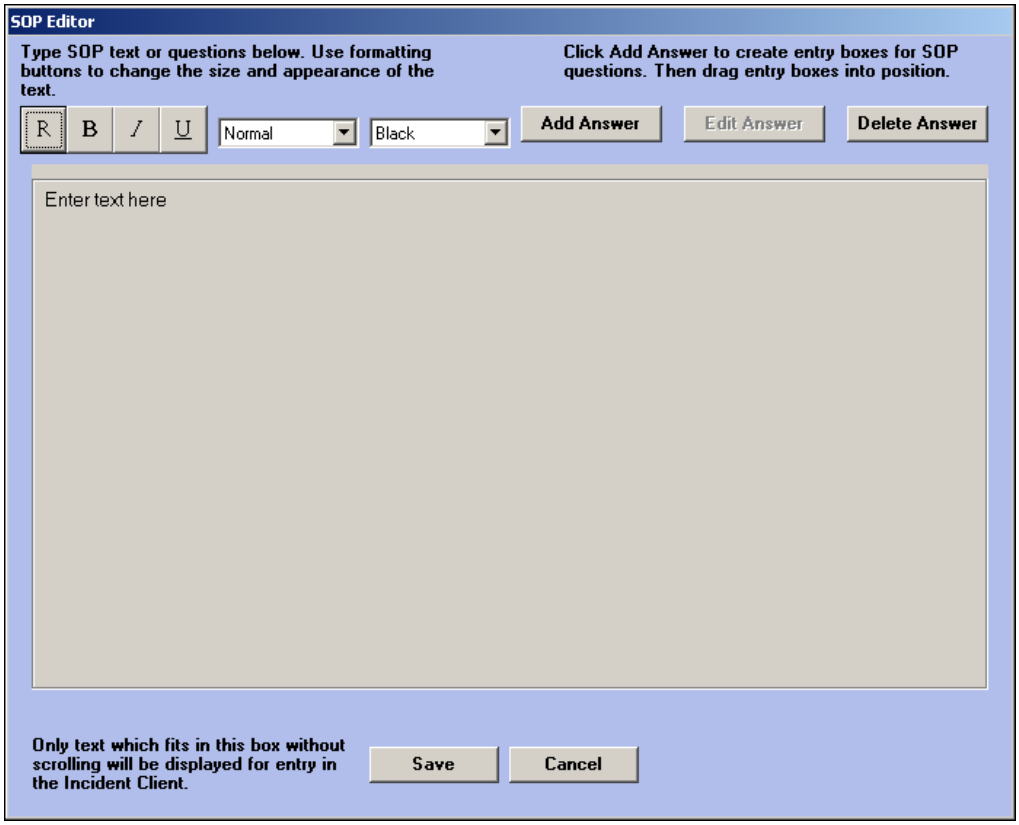
4 Enter a name for the SOP and click **OK.** The Emergency Cards dialog box appears.



5 Select an emergency card topic from the list. The D-21 uses the emergency card to associate the SOP with an incident class (Fire, Security, Aircraft, etc.). For more information on emergency cards, see "Emergency Cards" on page 3-20.

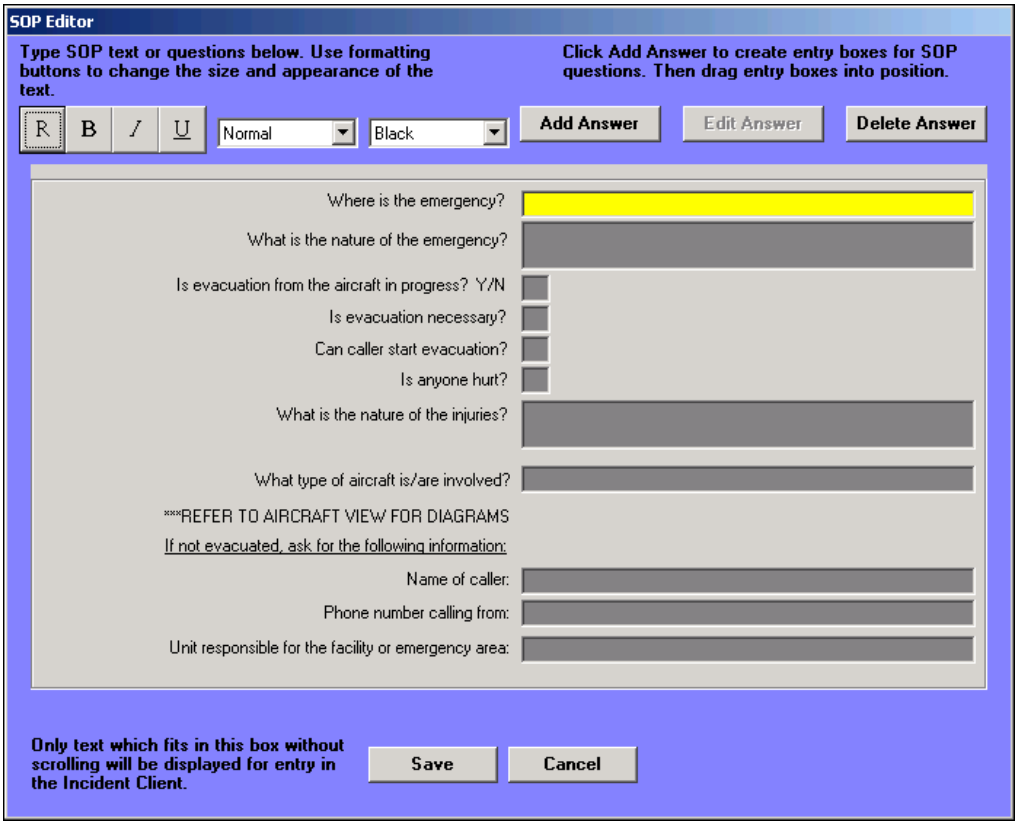
6 Click **OK** to return to the SOP dialog box.

7 Select the new SOP and click **Edit**. The SOP Editor dialog box appears.



8 Click anywhere on the left side of the window and type SOP text and questions.

9 Click **Add Answer** to create entry boxes for answers to SOP questions, if desired. Answer boxes are not required for SOPs.



For information on the text formatting controls, see "To edit an SOP" on page 3-38.

10 Click **Save** when you are finished creating the custom SOP.

11 In the SOP dialog box, click **Done**.

To remove a custom SOP

1 Select **Options > SOPs**.

2 Click the Custom SOP tab.

3 Click the name of the SOP you want to delete and click **Remove.** A message appears, asking for confirmation that you want to delete the SOP.

4 Click **Yes**.

5 In the SOP dialog box, click **Done**.

Incident Processing

Use the Incident Processing dialog box to configure the way the D-21 Incident Client handles alerts and incidents. This section includes the following procedures:

- "To enable automatic acknowledgement of alerts" on page 3-48.
- "To disable alerts from auxiliary zones" on page 3-46.
- "To disable alerts from relay outputs" on page 3-47.
- "To disable and enable unattended alarm alerts" on page 3-52.
- "To suppress duplicate trouble and normal alerts" on page 3-49.
- "To display zone numbers in alert log entries" on page 3-51.
- "To display the Alarm ID or Box Number on alerts" on page 3-51.
- "To configure the Alert Manager" on page 3-50.
- "To resound trouble alerts at regular intervals" on page 3-51.
- "To create secondary incident ID numbers" on page 3-54.
- "To change the color of alerts" on page 3-55.
- "To change the color of special status alerts" on page 3-56.
- "To change alert sounds" on page 3-57.

Setting Up Alert Processing

Alert priorities determine the order in which the D-21 displays alerts at the D-21 Incident Client. The D-21 always processes and displays alerts in the following order, with alarms given the highest priority.

Alert Type	Comments
Alarm	Any alarm alert, regardless of class, that originates at a remote unit zone is displayed before a trouble, reminder, or normal alert.
Priority 1	Zone priority is user-configurable and can be set in the Zone dialog box for each zone. The default zone priority is 4. For more information, see "To add a zone" on page 2-65. **NOTE** E911 alerts are also prioritized as automatic alarms. See "Configuring an E-911 System" on page 10-2 for more information.
Priority 2	
Priority 3	
Priority 4	
Priority 5	
Priority 6	
Priority 7	
Priority 8	
Supervisory	
Trouble	Any zone, unit, or system trouble, regardless of class is displayed before a reminder or normal alert.
Reminder	Action reminders and D-21 Incident Client Daily Activity reminders are displayed after alarms and troubles, but before normal alerts. See "Using Actions" on page 3-27 for more information about creating reminders in the D-21 Admin Client.
Normal	Alerts that inform the operator when an alarm or trouble condition has returned to normal are the lowest priority alert.

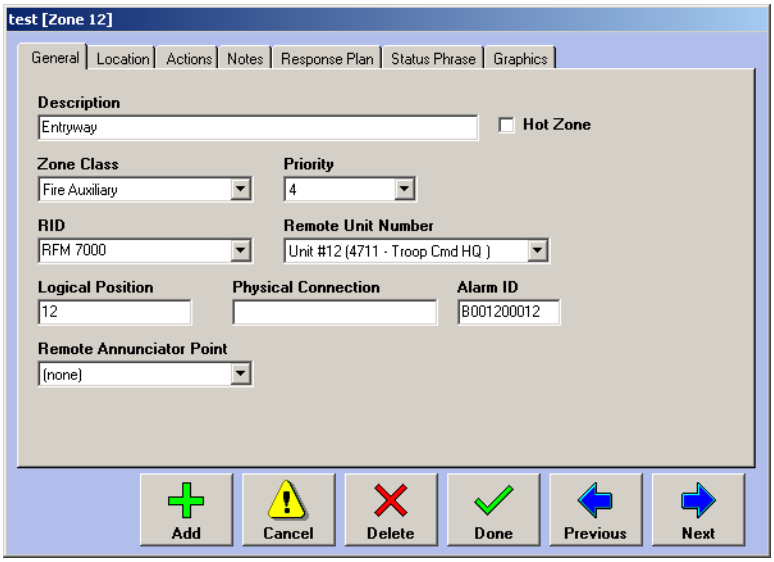
The D-21 generates alerts to notify you of many different types of conditions such as trouble states, return-to-normal states, and attempts to gain access to an area. Usually, you need to acknowledge these alerts, and can specify alert types you want the D-21 to acknowledge automatically. Automatically acknowledged alerts appear in the history log, but require no operator action. Also, you can specify whether an output generates an alert when its status changes.

IMPORTANT *Alarm alerts cannot be acknowledged automatically.*

You can also configure the display of automatic alerts at each workstation. For more information, see "Setting Workstation Options" on page 4-49.

To disable alerts from auxiliary zones

1 In the tree pane, right-click the fire or security auxiliary zone to select it. The Zone dialog box appears.



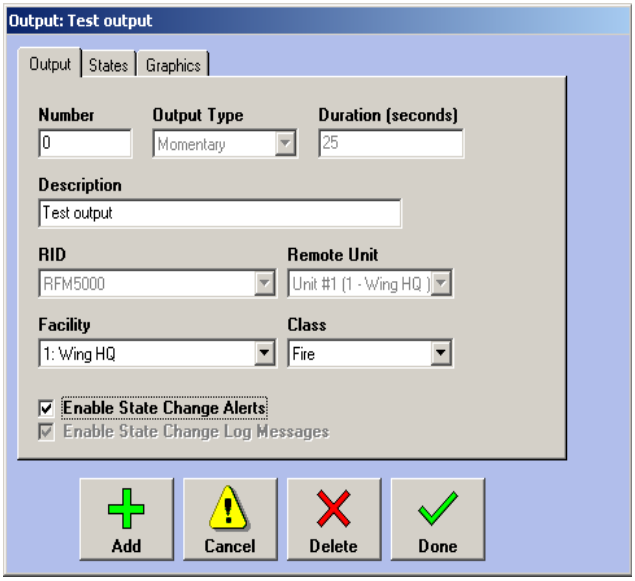
2 Select one of the following in the Priority drop-down list:

- **No Alert** Zone status changes will not generate an alert at the D-21, but the change will be logged.
- **No Log** Zone status changes will not generate an alert, and the D-21 will not log the change.
- **Log MNS Alarms** Alarm and normal status changes will not generate an alert at the D-21, but trouble status changes will generate an alert. All status changes will be logged. The Log MNS Alarms priority is only available for the Fire Auxiliary zone class. It is typically assigned to MNS Unit Zones which report an alarm when an MNS message plays. See "Configuring Mass Notification" on page 7-1 for more information on MNS.

3 Click **Done**.

To disable alerts from relay outputs

1 In the tree pane, right-click an output to select it. The Output dialog box appears.



2 Clear the Enable State Change Alerts check box.

NOTE *Turning off the Enable State Change Alerts option affects the display of output alerts on all D-21 workstations. Consult Monaco technical support for assistance, for each individual D-21 workstation, when disabling output alerts.*

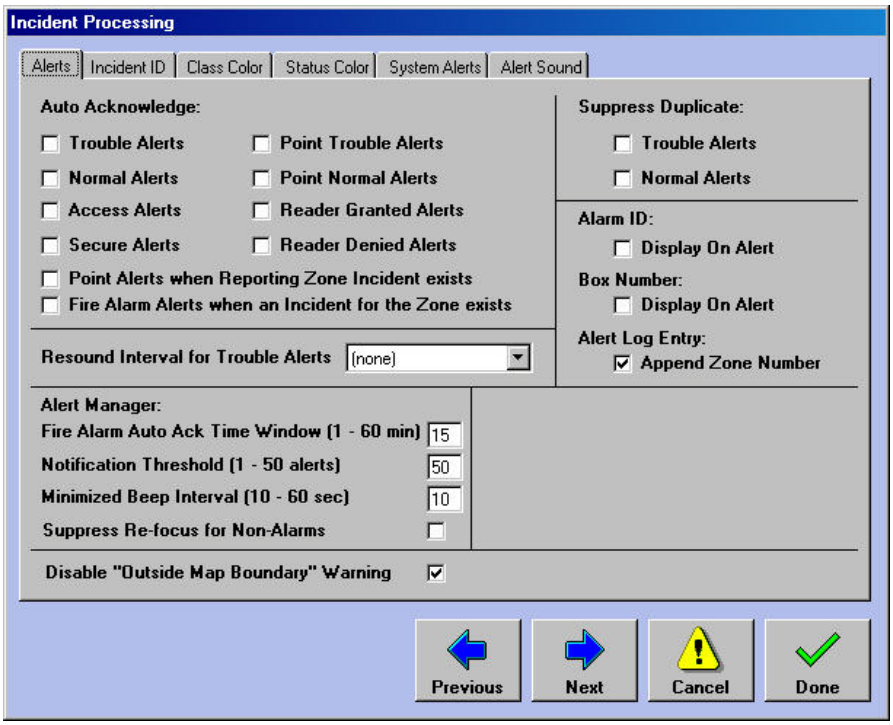
3 If you do not want the status changes recorded in the log, clear the Enable State Change Log Messages check box.

4 Click **Done**.

For more information, see "Outputs" on page 2-74.

To enable automatic acknowledgement of alerts

1 Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alerts tab displayed.



2 In the Alerts tab, click the check boxes next to the alert types you want the D-21 to acknowledge automatically.

NOTE *Alarm alerts cannot be automatically acknowledged in most circumstances. See below, Fire Alarm Alerts when an Incident for the Zone exists, for the single exception to this rule.*

- **Trouble Alerts** A Trouble alert indicates a unit or zone is not configured properly, or is partially or completely non-functional.
- **Normal Alerts** A Normal alert indicates a unit or zone has recovered from an Alarm or Trouble condition.
- **Access Alerts** An Access alert is generated when an Intrusion Detection zone has been disarmed. See "Configuring Intrusion Detection" on page 9-1 for more information.
- **Secure Alerts** A Secure Alert is generated when an Intrusion Detection zone has been armed. See "Configuring Intrusion Detection" on page 9-1 for more information.
- **Point Alerts when Reporting Zone Incident exists** Point alerts are generated by MAAP(+) units only. Selecting this option suppresses additional point alerts after an incident has been created for the zone through which the points report. See the Monaco Addressable Plus Planner Guide (P/N 001-359-01) for more information.

- **Fire Alarm Alerts when an Incident for the Zone exists** Selecting this option suppresses additional fire alarm alerts when a Fire incident has already been created at the reporting zone's facility.
- **Point Trouble Alerts** A Point Trouble alert indicates a point is not configured properly, or is partially or completely non-functional. See the Monaco Addressable Plus Planner Guide (P/N 001-359-01) for more information.
- **Point Normal Alerts** A Point Normal alert indicates a point has recovered from an Alarm or Trouble condition. See the Monaco Addressable Plus Planner Guide (P/N 001-359-01) for more information.
- **Reader Granted Alerts** A Reader Granted alert is generated when an Access Control card is successfully used. See "Configuring Access Control" on page 8-1 for more information.
- **Reader Denied Alerts** A Reader Denied alert is generated when an Access Control card is unsuccessfully used. See "Configuring Access Control" on page 8-1 for more information.

3 Click **Done**.

To suppress duplicate trouble and normal alerts

When remote units in the field are being serviced or experiencing intermittent communications with the D-21, multiple occurrences of the same trouble or normal alert can stack up quickly. These options provide a global way to limit repeat occurrences of the same alert by inhibiting duplicate trouble and normal alerts, so only one trouble and/or one normal alert is displayed for each unit or zone. When these options are configured, only the most recent trouble and/or normal alert will display for any one unit or zone. All of the alarm alerts will still be displayed, even if they are for the same zone.

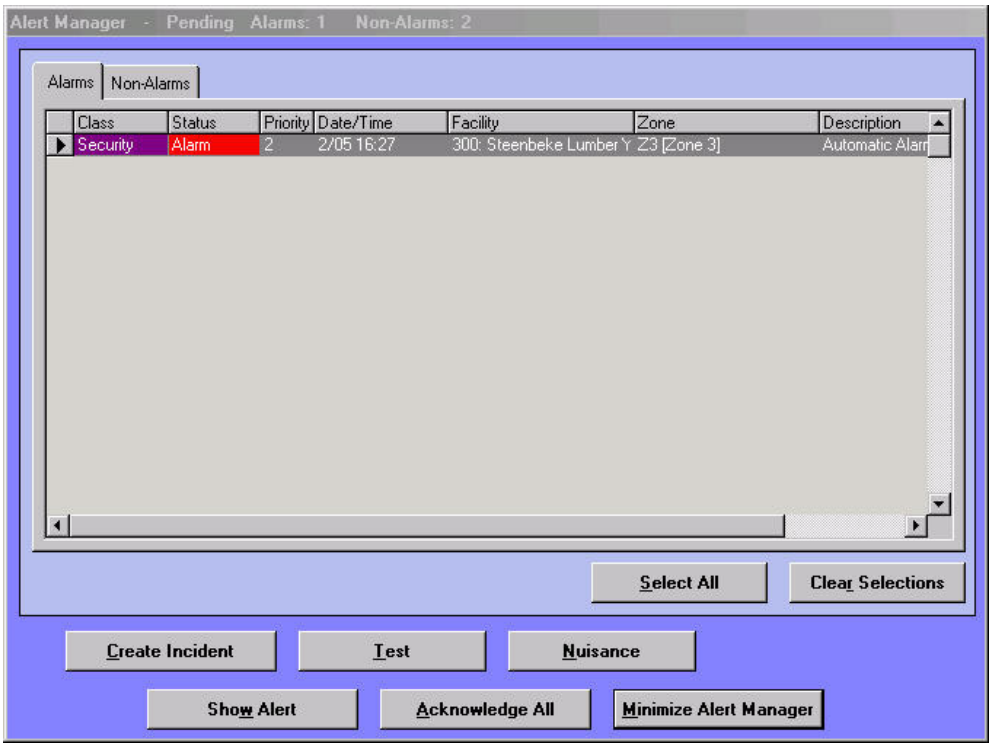
1 Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alerts tab displayed.

2 In the **Suppress Duplicate** section, check the boxes labelled **Trouble Alerts** and **Normal Alerts**.

3 Click **Done**.

To configure the Alert Manager

The Alert Manager provides an interface that displays alarms and non-alarms and allows operators to select and handle multiple alerts at the same time. Whenever an alert comes in to the D-21 Incident Client, the operator has the option to open the Alert Manager (see the following graphic). Some elements of Alert Manager behavior can be configured in the D-21 Admin Client.



1. Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alerts tab displayed.
2. Enter numeric values in the following fields to configure the Alert Manager:
   - **Notification Threshold** Specify the number of single alerts displayed before all alerts are displayed in the Alert Manager.
   - **Minimized Beep Interval** Specify the number of seconds (from 10 to 60) between the audible beeps that sound while the Alert Manager is minimized.
   - **Suppress Re-focus for Non-Alarms** Check this box to allow the Alert Manager to remain minimized when non-alarm alerts (i.e. troubles, normals) come in.
3. Click **Done**.

To display zone numbers in alert log entries

By default, the zone number is appended to all log entries referring to an alert. However, this behavior can be suspended if desired.

1. Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alerts tab displayed.
2. In the **Alert Log Entry** section, uncheck the checkbox labelled **Append Zone Number**.
3. Click **Done**.

NOTE *This modification should not be taken lightly, as it requires that the D-21 Server be re-started before it will take effect. The simplest way to do this is to reboot the primary server computer.*

To display the Alarm ID or Box Number on alerts

If you are not using Secondary Incident IDs (see "Customizing Incident Numbers" on page 3-53), you can choose to display the Alarm ID on zone alerts.

1. Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alert tab displayed.
2. In the **Alarm ID** section, check the checkbox labelled **Display On Alert**.
3. In the **Box Number** section, check the checkbox labelled **Display On Alert**.

To resound trouble alerts at regular intervals

1. Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alert tab displayed.
2. Select a time interval in the **Resound Trouble Time** drop-down list.

NOTE *If Trouble Alerts are set to acknowledge automatically, troubles are added to the history log at the selected interval but no trouble alert is generated.*

3. Click **Done**.

To disable E-911 map warnings

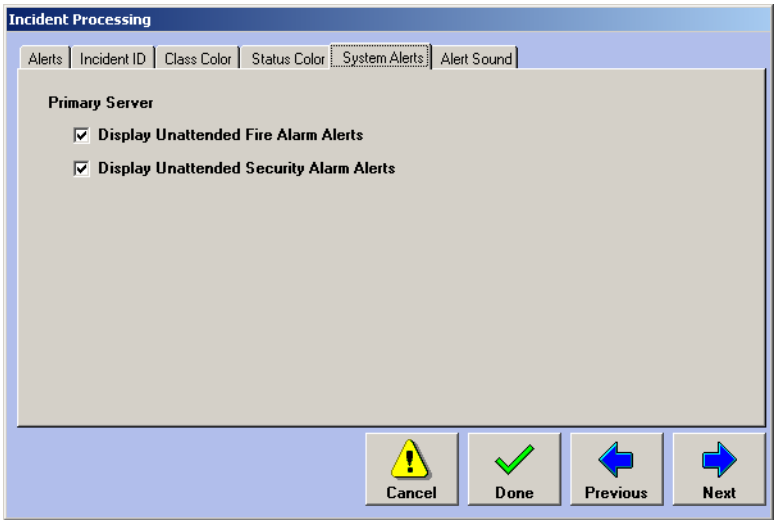
When an E-911 system has the capability to send geographical coordinates for incoming calls to the D-21, the location of incidents created from these calls can sometimes fall outside the defined extent of the D-21 Incident Client's map. When the coordinates are not available on the map, by default, a warning message is displayed to the operator. The display of this message can be disabled, if desired.

1. Select **Options > Incident Processing**. The Incident Processing dialog box appears with the Alert tab displayed.
2. Click the checkbox labelled **Disable "Outside Map Boundary" Warning** to deselect it.
3. Click **Done**.

To disable and enable unattended alarm alerts

1 Select **Options > Incident Processing**.

2 Click the System Alerts tab.



- **Display Unattended Fire Alarm Alerts** Select this option to display an alert whenever there is a fire alarm and there is no operator currently logged into the system.
- **Display Unattended Security Alarm Alerts** Select this option to display an alert whenever there is a security alarm and there is no operator currently logged into the system.

3 Click **Done**.

Customizing Incident Numbers

The Incident ID tab in the Incident Processing dialog box varies depending on the D-21 modules you have purchased. If you have the D-21 Fire Client installed, you can customize the primary incident number and a secondary incident number. A secondary number can help with organization-specific paperwork or with exporting incident data to other programs. If you also have the D-21 Security Client and/or Facility Management installed, you can use this tab to customize the incident numbers that are assigned to those incident classes.

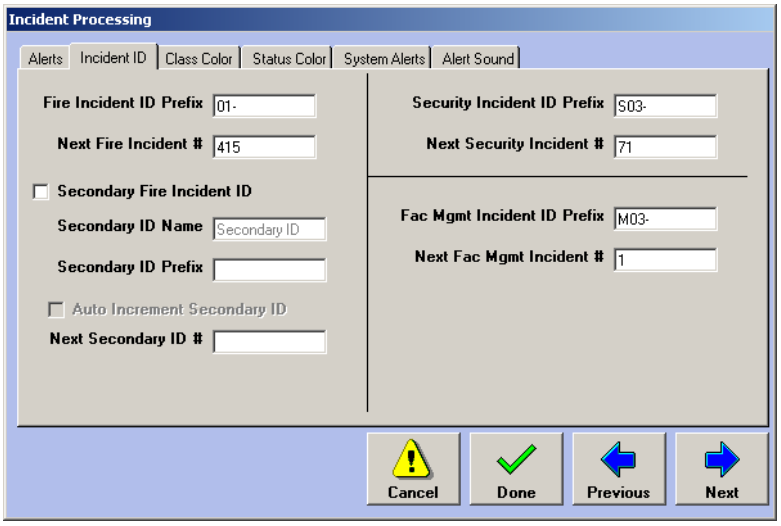


Figure 3-5 *Incident Processing dialog box with the Incident ID tab in the foreground*

- **Fire Incident ID Prefix** Enter the prefix you want used for fire incidents. You may enter up to ten characters.
- **Next Fire Incident Number** Enter the number you want used for the next fire incident. The value that appears in this box is dynamic, updating each time the next incident number is used.
- **Secondary Fire Incident ID** Select this option if you want to enable the use of a second numbering scheme for fire incidents. The text you enter in the Secondary ID Name field will be used to label this field in the D-21 Incident Client. A custom prefix is available with the secondary fire incident ID just as with the primary fire incident ID.
- **Security Incident ID Prefix** Enter the prefix you want used for security incidents. You may enter up to ten characters. This field is only available if the D-21 Security Client is installed.
- **Next Security Incident Number** Enter the number you want used for the next security incident. The value that appears in this box is dynamic, updating each time the next incident number is used. This field is only available if the D-21 Security Client is installed.
- **Fac Mgmt Incident ID Prefix** Enter the prefix you want used for Facility Management incidents. You may enter up to ten characters. This field is only available if the D-21 Facility Management Client is installed.

- **Next Fac Mgmt Incident Number** Enter the number you want used for the next Facility Management incident. The value that appears in this box is dynamic, updating each time the next incident number is used. This field is only available if the D-21 Facility Management Client is installed.

NOTE *The only way to lower the value of the number that appears in any of the Next Incident Number boxes is to change the Incident ID Prefix.*

To create secondary incident ID numbers

NOTE *You must have the Fire Client installed to create secondary incident ID numbers.*

1. Select **Options > Incident Processing**. The Incident Processing dialog box appears.
2. Click the Incident ID tab.
3. Check the Secondary Fire Incident ID checkbox option.
   - **Secondary ID Name** Type a name for the secondary incident number. This label is used through the D-21 Incident Client to identify the secondary number.
   - **Secondary ID Prefix** Type the prefix used to identify the secondary incident ID numbers. The prefix and a hyphen will be added to the start of each secondary incident ID number.
4. If you want your secondary incident ID number to be automatically incremented, check the Auto Increment checkbox option.
   - **Next ID Number** Enter the next secondary incident ID number you want to use.
5. Click **Done**.

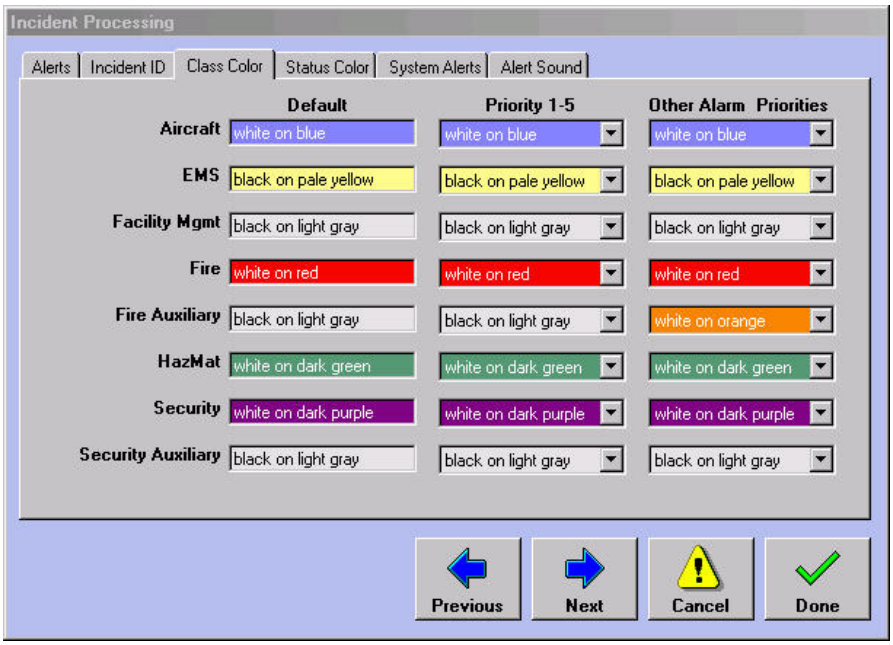
Customizing Incident Class and Status Colors

The Class Color and Status Color tabs in the Incident Processing dialog box provide drop-down lists for specifying the colors used for alert dialog boxes. You can specify different alert colors for each incident category, and for two sets of priority levels within each category. You can also change the colors used to display supervisory alerts.

To change the color of alerts

1 Select **Options > Incident Processing**.

2 Click the Class Color tab.



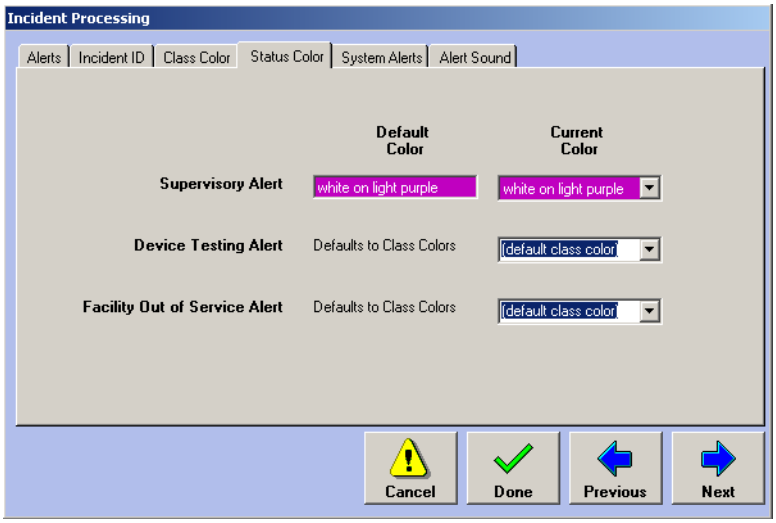
- **Default** Displays the default color coding for all alert classes.
- **Priority 1-5** Select a new color scheme for the alert when the alert's zone priority is set between 1 and 5. See "Zone Priority" on page 2-65 for more information.
- **All Other Priorities** Select a new color scheme for the alert class when the alert's zone priority is set at 6 or higher.

3 When you are finished, click **Done**.

To change the color of special status alerts

1 Select **Options > Incident Processing**.

2 Click the Status Colors tab.



The Status Color window allows Supervisory, Device Testing, and Facility out of Service alerts to be customized.

- **Default** Displays the default color coding for the alert. For instance, Supervisory Alert is set to white text on a light purple background.
- **Current** Select a new color scheme for the alert.

3 When you are finished, click **Done**.

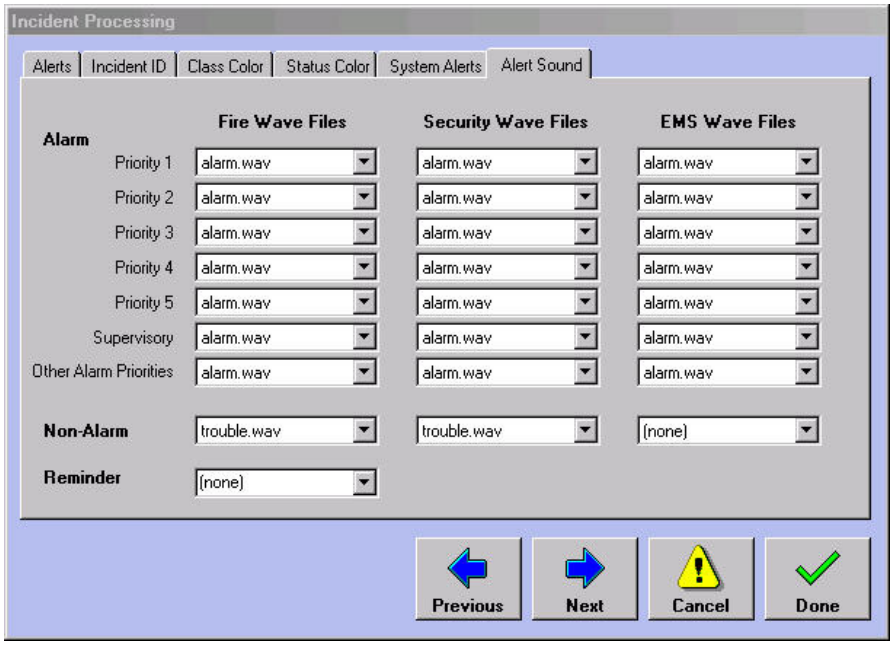
Setting Alert Sounds

The Alert Sounds are set to audibly notify operators of the class or severity of the trouble or alarm. The Alert Sound tab in the Incident Processing dialog box allows the administrator to set various sounds used to alert personnel.

To change alert sounds

1 Select **Options > Incident Processing**.

2 Click the Alert Sound tab.



- **Alarm** You can differentiate the class (fire, security, or EMS) of alarms based on sound. You can also assign different sounds to different alarm priorities within and across these classes.
- **Non-Alarm** You can assign a sound to normal and trouble alerts within and across classes.
- **Reminder** You can assign a sound to play when a scheduled reminder is activated. See "To create a Reminder action" on page 3-34 for more information on reminders.

3 Select the appropriate sound files as necessary.

NOTE *The sound files you want to assign must be located in* `C:\Program Files\D-21\Media\Sounds`.

4 Click **Done** when finished.

Resetting Incident Editing Controls

The D-21 "locks" an incident while it is being edited on one workstation so it cannot be edited by more than one operator at a time. The operator on the second workstation can view the information but cannot save any changes to the incident. If the D-21 informs you that an incident is already being edited by another operator, and you can verify the incident is not open on another workstation, the incident "lock" may need to be reset. Use the Reset Edit Incident Control command to reset the incident editing controls.

IMPORTANT *The Reset Edit Incident Control command is only available if the operator who is logged in is assigned data entry level 2 in the D-21 Admin Client. For more information on setting an operator's data entry level, see "To add an operator" on page 2-97.*

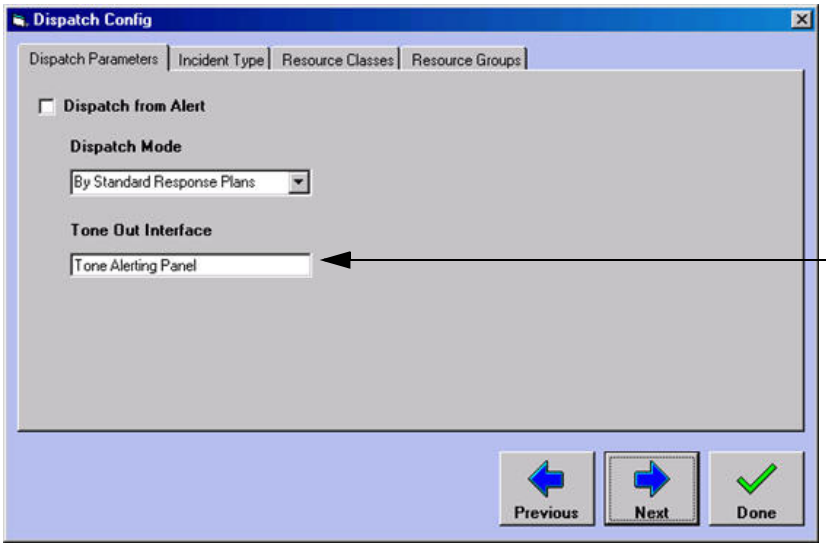
To reset the incident editing control in the D-21 Incident Client

NOTE *Monaco recommends all operators log out of the D-21 Incident Client before resetting incident editing control.*

1. Select **Commands > Reset Edit Incident Control**. A confirmation message appears.
2. Click **Yes**.

Dispatch Configuration

Once an incident is created, the most important and immediate duty of the D-21 Incident Client operator is often the dispatch of the appropriate resources to the incident. The D-21 administrator can simplify the selection of resources to dispatch by grouping resources together and setting up default resource assignments for typical situations. Select **Options > Dispatch Config** to view and configure dispatch options.



Displayed only when a tone alert interface has been added to the D-21. See Section 11, Configuring Tone Alerting.

The Dispatch Config dialog box is divided into four tabs:

- **Dispatch Parameters** Make basic decisions about when dispatching will occur and how default resource assignments will be assigned.
- **Incident Type** Make resource assignments for specific incident types.
- **Resource Classes** Customize the job types used to organize resources in the D-21.
- **Resource Groups** Group individual resources together for assignment.

Dispatch from Alert

By default, dispatching is performed in an incident's Dispatch viewer, which becomes available once the process of creating an incident has been completed. However, the D-21 administrator can enable the Dispatch from Alert option, which allows the D-21 Incident Client operator to notify resources as soon as an incoming alert has been acknowledged.

To enable dispatching from an alert

1. Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.
2. Click the **Dispatch from Alert** check box to check it.
3. If you are through configuring dispatch, click **Done** to close the dialog box.

Dispatch Modes

The D-21 provides three dispatch modes, which govern the way resources are pre-assigned to future incidents.

- **By Response Plan** Response plans are created by incident class and can be attached to sites, facilities, and zones. Response plans can include individual resource assignments, and the resources can be grouped as Priority 1 (first response), Priority 2 (second response), etc. When the dispatch mode is configured to be by response plan, the default resources assigned to an incident are the Priority 1 resources specified in the applicable response plan.

NOTE *See* *"To add dispatch instructions to a response plan" on page 3-9*.

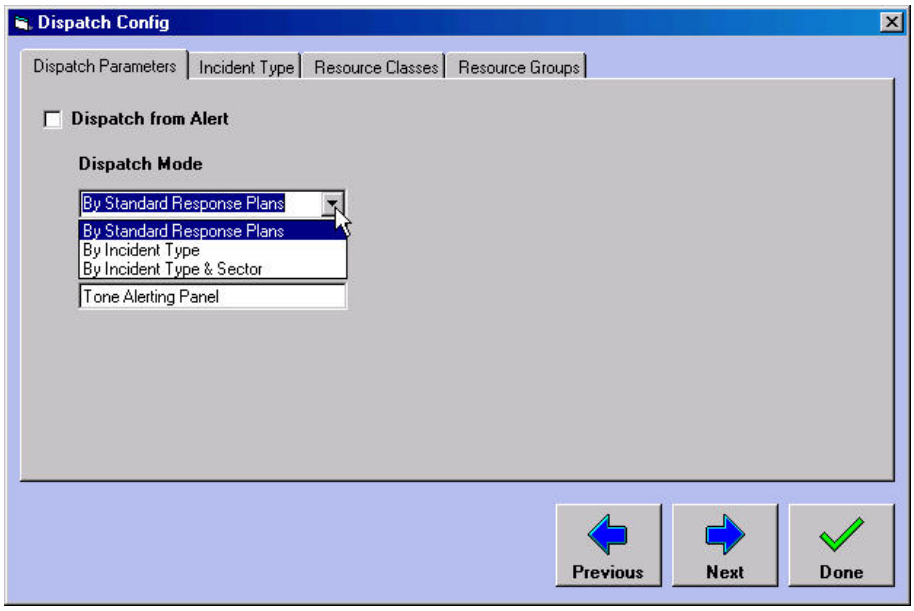
- **By Incident Type** Incident types are created to break down an incident class based on the resource group which should respond. When the dispatch mode is configured to be by incident type, the operator handling an incident can select an incident type as well as an incident class, and the default resources assigned to the incident are the members of the group associated with the incident type.
- **By Incident Type and Sector** For large installations, incident types can be further sub-divided to reflect the geographical areas covered by specific resource groups. When the dispatch mode is configured to be by incident type and sector, the operator handling an incident can

select an incident type and also a sector, if necessary. (The sector for facilities entered in the D-21 database is automatically populated.) The default resources assigned to the incident are the members of the group associated with the incident type and sector.

IMPORTANT *The D-21 Incident Client operator is always free to disregard default resource assignments and notify whatever resources are most appropriate, regardless of dispatch mode.*

To set the dispatch mode

1. Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.
2. Click the down arrow in the **Dispatch Mode** drop-down list to see all items in the list.



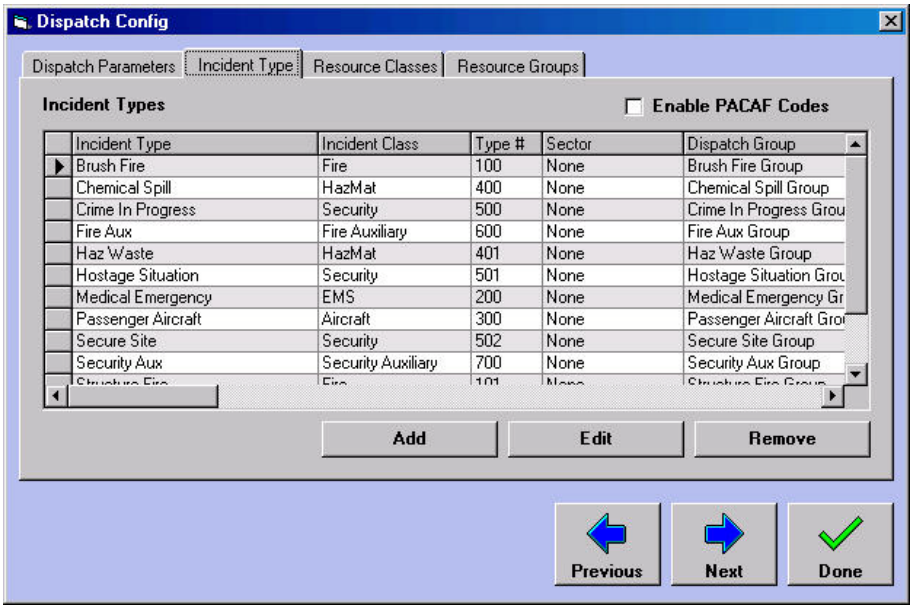
3. By default, dispatch mode is By Standard Response Plans. Select either By Incident Type or By Incident Type & Sector to change the dispatch mode. You will also need to create resource groups and incident types if you select one of these modes. See "Incident Types" on page 3-61 and "Resource Groups" on page 3-66.

Incident Types

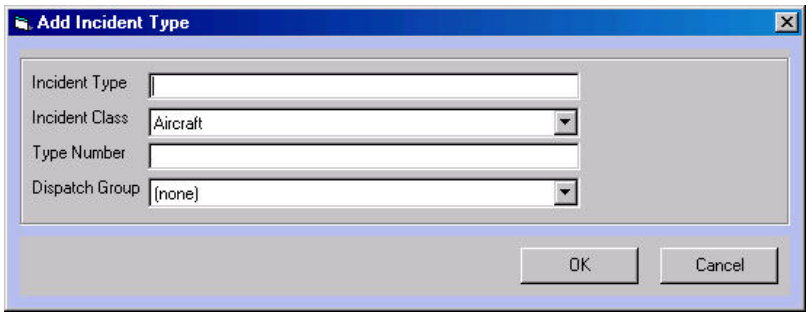
Incident types are sub-divisions within an incident class to which you can assign pre-defined groups of resources. When the D-21 Incident Client operator selects an incident type during the process of creating an incident, the pre-assigned resources are automatically selected.

To set up dispatching by incident type

1. Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.
2. Click the Incident Type tab.



3. Click **Add**. The Add Incident Type dialog box opens.



4. In the **Incident Type** text box provide a name for the Incident Type. This is what the D-21 Incident Client operator will select when processing an incident.
5. Select the incident class to which this incident type belongs from the **Incident Class** drop-down list.

6 In the **Type Number** text box provide an identifying code number for the incident type.

NOTE *If you have not yet created the resource group, you can skip the following step. Once you have created the resource group, return to the Incident Type tab, select the incident type in the grid, and click* **Edit** *to assign the resource group to the incident type.*

7 Select the resource group you want to associate with the incident type from the **Dispatch Group** drop-down list. (See "To add a resource group" on page 3-67 for instructions on creating resource groups.) When the D-21 Incident Client operator selects this incident type in the process of creating an incident, these resources will be automatically assigned to the incident.

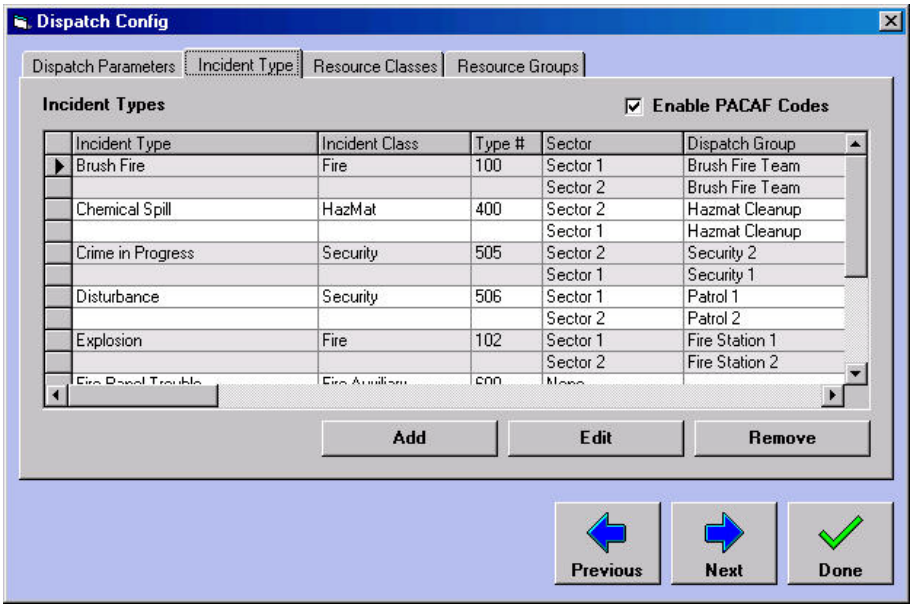
8 Click **OK** to save the new incident type.

To set up dispatching by incident type and sector

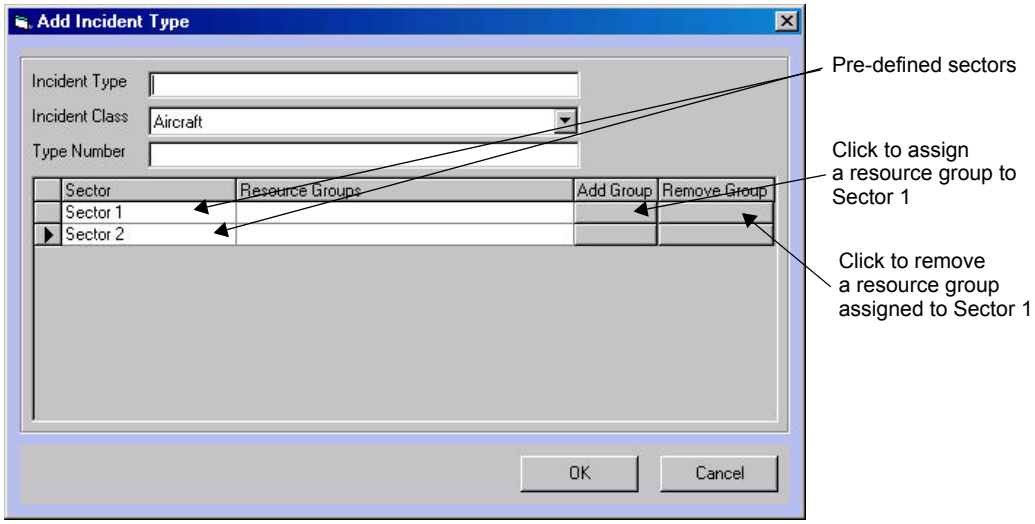
Sectors are geographical areas covered by specific resource groups. Sectors must be defined on the D-21 map before you set up dispatching by incident type and sector. Contact Monaco D-21 support for assistance with defining sectors.

1 Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.

2 Click the Incident Type tab.



3 Click **Add**. The Add Incident Type dialog box opens.

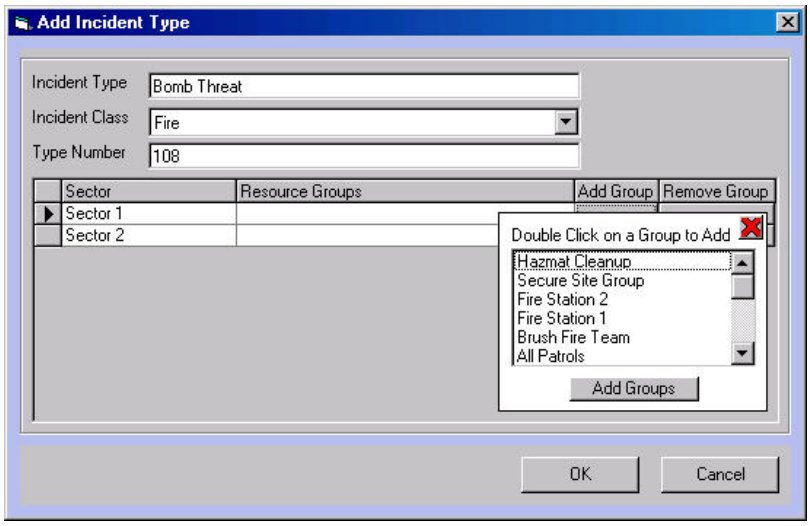


4 Type a name for the Incident Type in the **Incident Type** text box. This is what the D-21 Incident Client operator will select when processing an incident.

5 Select the incident class to which this incident type belongs from the **Incident Class** drop-down list.

6 Type an identifying code number for the incident type in the **Type Number** text box.

7 Click the button in the Add Group column for the first pre-defined sector in the grid. A list of groups available for assignment appears.



NOTE *If you have not yet created the resource group, you can skip the following step. Once you have created the resource group, return to the Incident Type tab, select the incident type in the grid, and click* **Edit** *to assign the resource group to the incident type.*

8 Double-click the resource group you want to associate with this incident type and sector. (See "To add a resource group" on page 3-67 for instructions on creating resource groups.) When the D-21 Incident Client operator selects this incident type in the process of creating an incident, these resources will be automatically assigned to an incident in this sector.

9 Repeat steps 7 and 8 for each pre-defined sector.

10 Click **OK** to save the new incident type.

To enable PACAF incident codes

1 Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.

2 Click the Incident Type tab.

3 Check the Enable PACAF Codes check box.

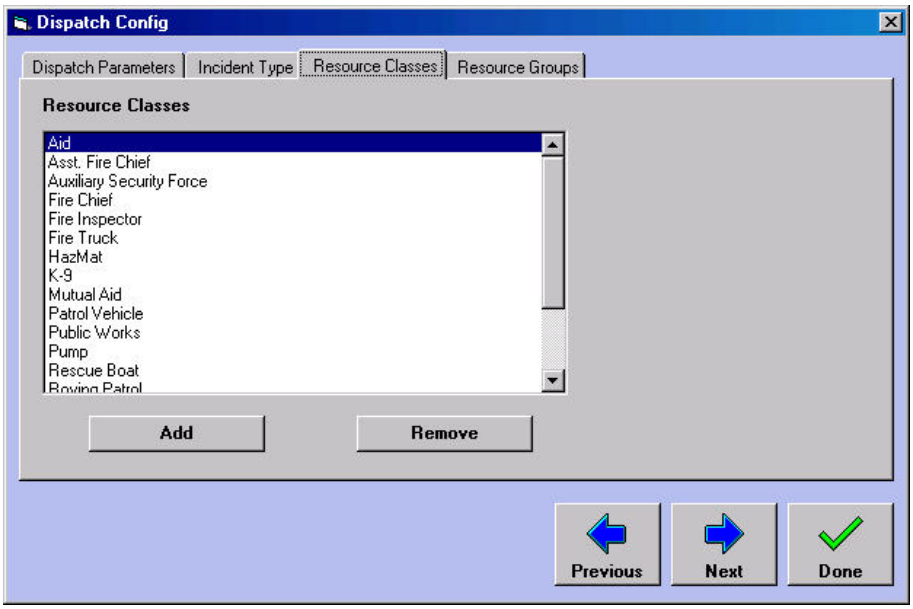
4 Click **Done**.

Resource Classes

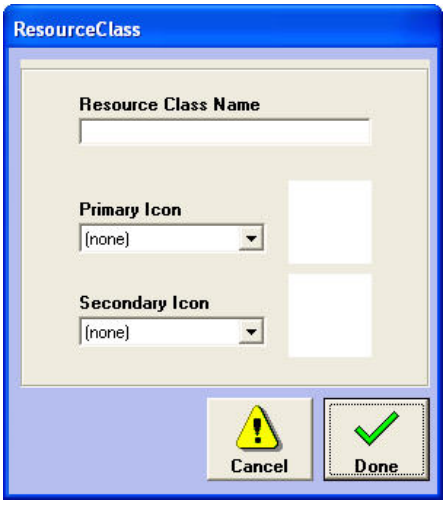
Resources added to the D-21 database are organized into resource classes, which represent emergency response roles or functions. The D-21 provides pre-defined resource classes for your use, which can also be deleted if they do not meet your needs. You can also add your own resource classes as necessary. For more information on resources, see "Resources" on page 2-103.

To add a resource class

1. Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.
2. Click the Resource Classes tab.



3. Click **Add** to add a new resource class to the list. A new entry dialog box appears.



4 Type the name of the new resource class.

5 If members of the new resource class will be equipped with Automatic Vehicle Location (AVL), select a primary and secondary icon to represent them on the map. See the D-21 Map Options User Guide (P/N 001-464-00) for more information about AVL.

6 When you are finished, click **Done**.

To delete a resource class

1 Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.

2 Click the resource class you want to delete in the Resource Classes list box.

3 Click **Remove**.

4 Click **Yes** in the confirmation dialog box that appears.

Resource Groups

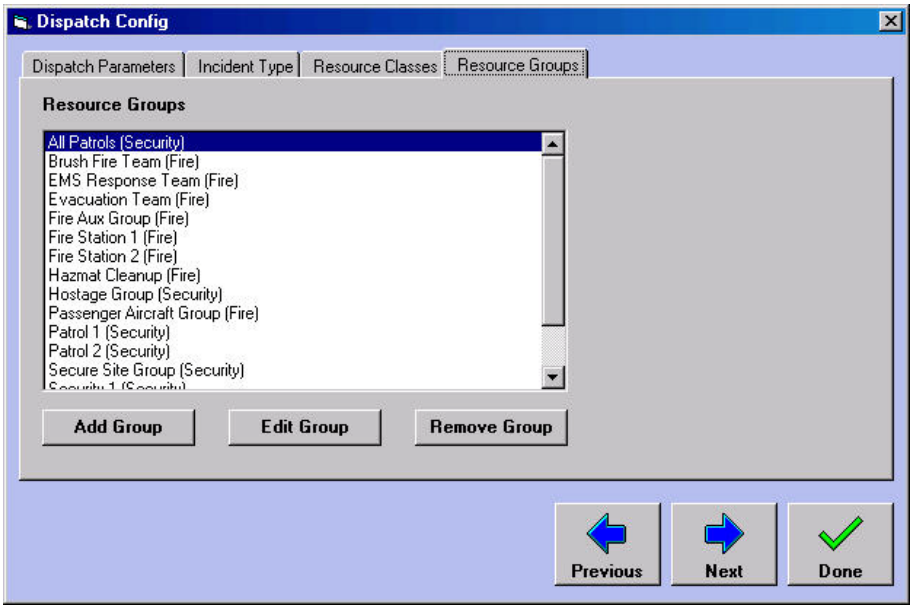
Resource groups allow you to handle multiple individual resources which are often dispatched together as one entity. You can group resources in any way that makes sense for your organization - by home location or by shift, for instance. You can make as many resource groups as you need, since each resource can be added to multiple groups.

NOTE *Resources added to resource groups can still be dispatched individually by the D-21 Incident Client operator.*

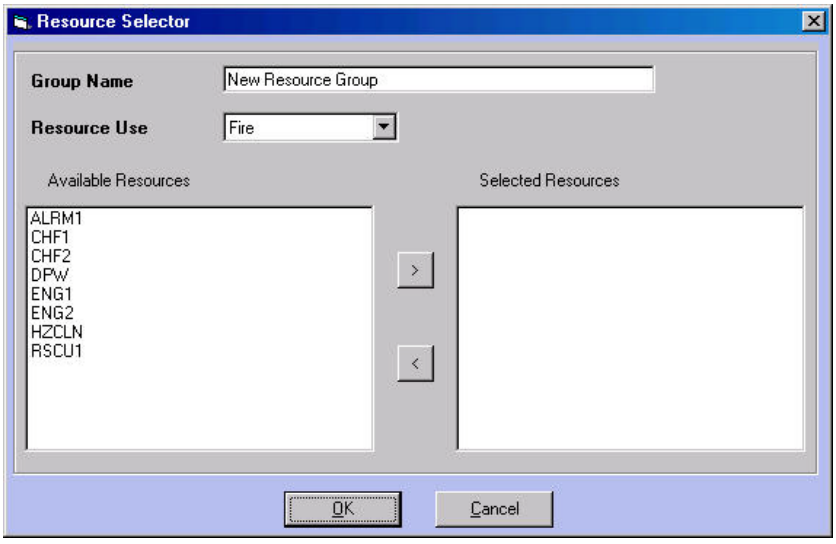
If you are using dispatch by incident type, or by incident type and sector, you will need to make resource groups to associate with the incident types. See "To set up dispatching by incident type" on page 3-61 and "To set up dispatching by incident type and sector" on page 3-62 for more information.

To add a resource group

1. Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.
2. Click the Resource Groups tab.



3. Click **Add Group**. The Resource Selector dialog box appears.



4. Enter a name for the new group in the **Group Name** text box.
5. Select the appropriate incident class for the group from the **Resource Use** drop-down list. The Available Resources list box displays all the resources defined for the incident class.

6 Click the resources you want to add to the group in the Available Resources list box. Then click the right arrowhead (**>**) button. The resources are removed from the Available Resources list box and added to the Selected Resources list box.

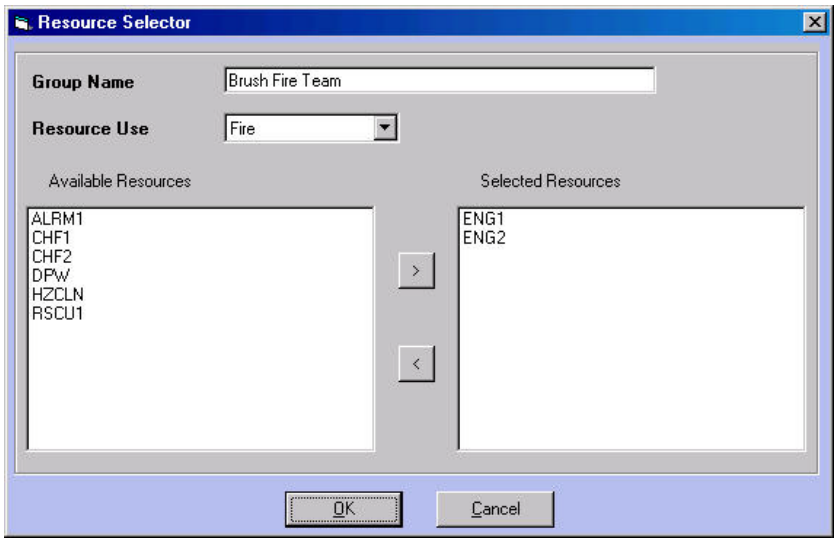
7 When you are finished, click **OK**.

To edit a resource group

1 Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.

2 Click the Resource Groups tab.

3 Select the group you want to edit in the Resource Groups list box and click **Edit Group**. The Resource Selector dialog box is displayed, along with the resources that are currently part of the group listed in the Selected Resources list box. Resources that are not currently part of the group are listed in the Available Resources list box.



4 To add a resource to the group, select it in the Available Resources list box and click the right arrowhead (**>**) button.

5 To remove a resource from the group, select it in the Selected Resources list box and click the left arrowhead (**<**) button.

6 When you are finished, click **OK**.

To delete a resource group

1 Select **Options > Dispatch Config**. The Dispatch Config dialog box is displayed, with the Dispatch Parameters tab selected.

2 Click the Resource Groups tab.

3 Select the group you want to delete in the Resource Groups list box and click **Remove Group**.

4 Click **Yes** in the confirmation dialog box that appears.

Section 4
Customizing the D-21

Read this section to learn how to customize D-21 look-up lists, map settings, and other workstation options.

Contents

Customizing Lists 4-2
- General Lists 4-2
- Fire Lists 4-12
- Security Lists 4-14
- Personnel Lists 4-23
- Permit/Work Order Lists 4-25

Setting Map Options (D-21 M) 4-33
- Configuring Shortest Routes 4-33
- Setting Road Closure Color 4-35
- Configuring Incident Relocating 4-36

Setting Hydrant Colors 4-37
Creating Rosters 4-38
Creating a Summary Statistics Log 4-46
Setting Workstation Options 4-49

Customizing Lists

You can customize many of the interface and database elements throughout the D-21 system. Use the General List dialog box to customize the information appearing in drop-down list boxes throughout the D-21 Admin Client and the D-21 Incident Client, that are not specific to either D-21 Fire Client or D-21 Security Client. For information specific to the Fire Client, see "Fire Lists" on page 4-12. For information specific to the Security Client, see "Security Lists" on page 4-14.

General Lists

This section provides the following customization procedures:

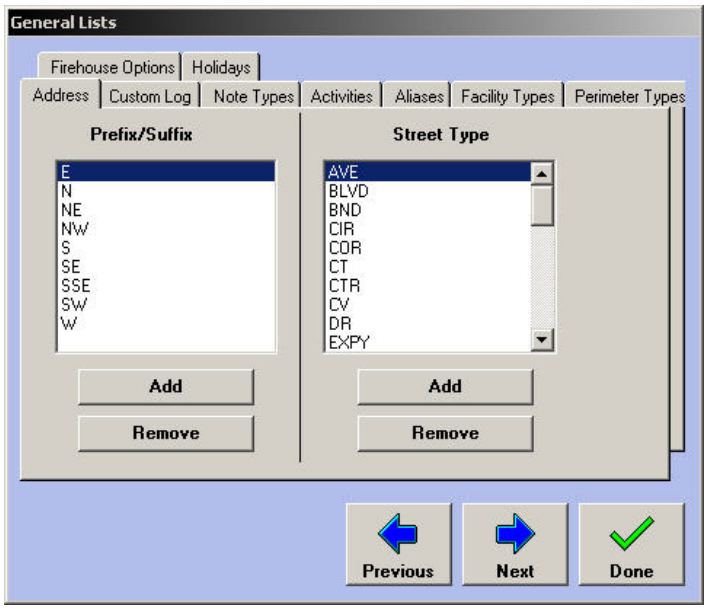
- "To enter address abbreviations" on page 4-3.
- "To create custom log entries" on page 4-4.
- "To create custom note types" on page 4-5.
- "To customize the D-21 Incident Client Daily Activity viewers" on page 4-6.
- "To customize the "Site" label" on page 4-7.
- "To create custom facility types and symbols" on page 4-8.
- "To customize perimeter types" on page 4-9.
- "To configure Firehouse options" on page 4-10.

NOTE *Firehouse options can only be configured when Firehouse software is installed.*

- "To schedule holidays" on page 4-11

To enter address abbreviations

1. Select **Options > General Lists**.
2. Click the Address tab.

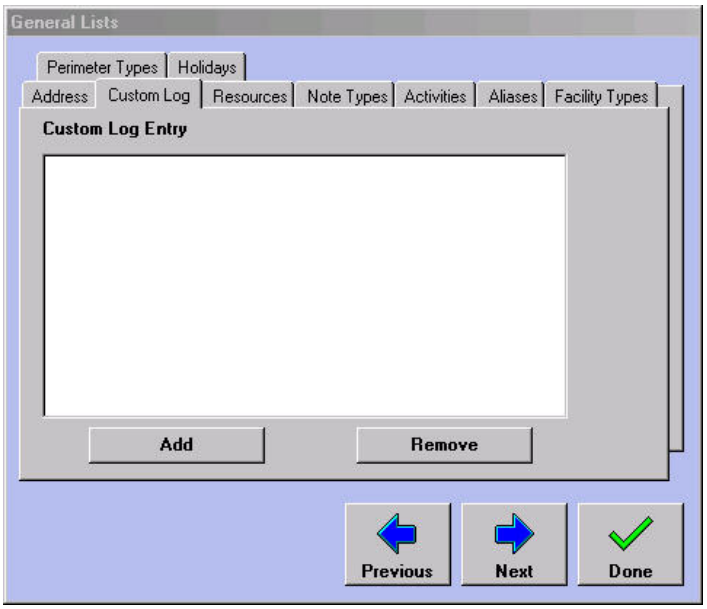


- **Prefix/Suffix** Enter directional prefixes or suffixes that are not included in the supplied list. You can select these entries wherever you enter address information in the D-21.
- **Street Type** Enter any street type labels that are not included in the supplied list. You can select these entries wherever you enter address information in the D-21.

3. Click **Add** beneath the list box to which you want to add an entry. A new entry dialog box appears.
4. Type the text of the new address abbreviation.
5. Click **OK**.
6. Click **Done**.

To create custom log entries

1. Select **Options > General Lists**.
2. Click the Custom Log tab.

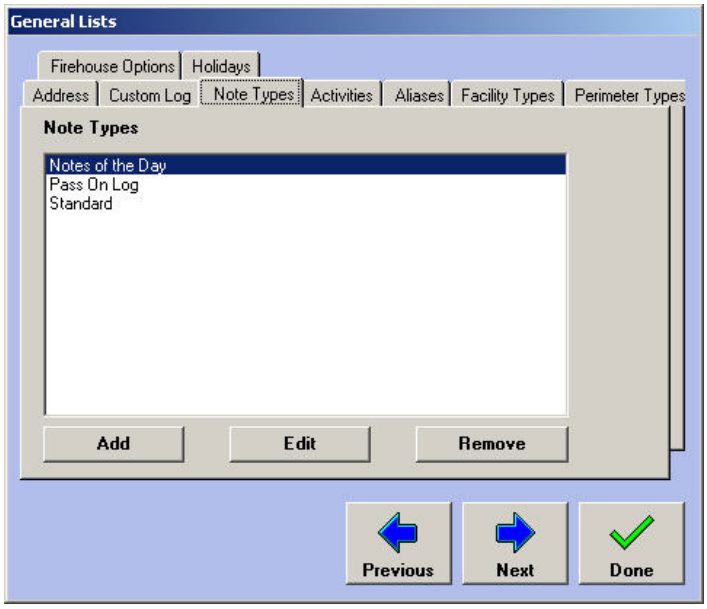


- **Custom Log Entry** Enter custom log entries in this field. These entries will be available in the Log Entry drop-down list boxes that appear when you click **Add Entry** in the D-21 Incident Client logs.

3. Click **Add** to add a new log entry. A new entry dialog box appears.
4. Type in the custom log entry text.
5. Click **OK**.
6. Click **Done**.

To create custom note types

1. Select **Options > General Lists**.
2. Click the Note Types tab.

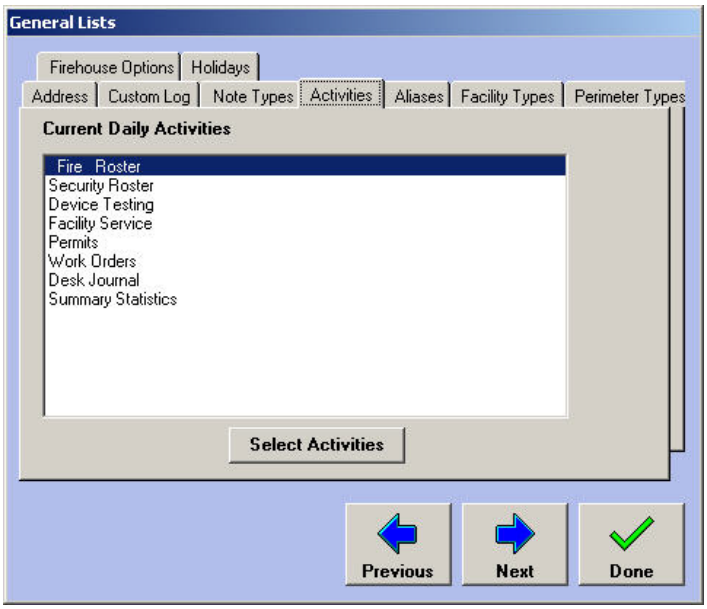


- **Note Types** Enter note types in this field you want to make available in the Notes viewer of Daily Activities in the D-21 Incident Client. Create note types for different categories of notes, such as notes to specific operators, workstations, or dispatch assignments. You can use note types to control the display of specific notes in the D-21 Incident Client. There are two default note types:
- **Standard** Use this type if you do not need additional note customizations.
- **Pass On Log** Use this note type to distinguish notes being passed from one shift to the next.

3. Click **Add** to add a new note type to the list. A new entry dialog box appears.
4. Type the name of the new note type.
5. Click **OK**.
6. Click **Done**.

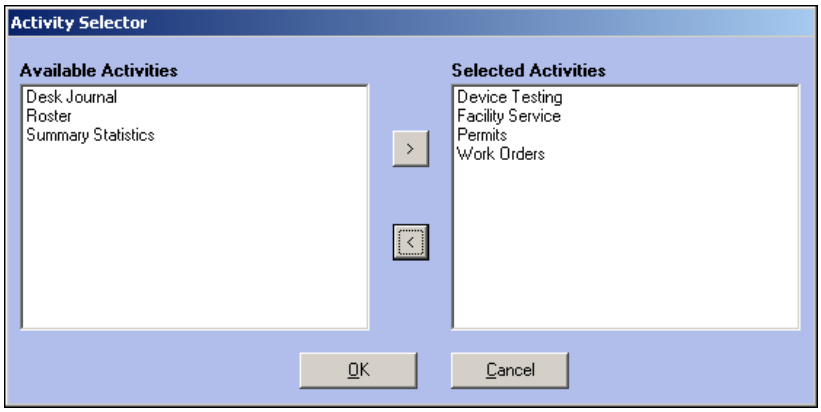
To customize the D-21 Incident Client Daily Activity viewers

1. Click **Options > General Lists**.
2. Click the Activities tab.



The Current Activities list shows the viewers available for selection as Daily Activities in the D-21 Incident Client.

3. Click **Select Activities**. The Activity Selector dialog box appears.



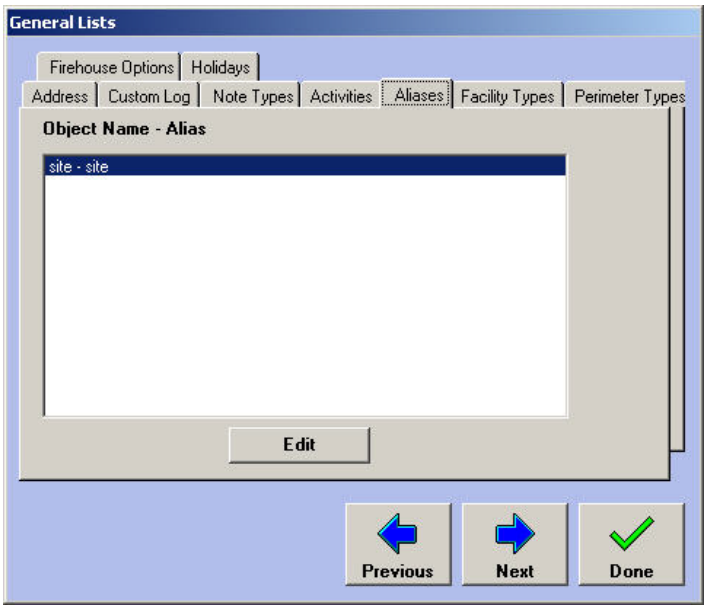
4. To add viewers to Daily Activities, select the viewer in the Available Activities list and click the right button (**>**) to move the viewer into the Selected Activities list. To remove viewers from the Daily Activity window, select the viewer in the Selected Activities list and click the left button (**<**) to move the viewer back into the Available Activities list.
5. Click **OK**.

To customize the “Site” label

Use the Aliases tab in the General Lists dialog box to customize the Site label. For example, if your site has multiple districts which each have their own facilities, you can change “Site” to “District.”

NOTE *You must be logged into the D-21 Admin Client, with administrator privileges, in order to rename the Site label.*

1. Click **Options > General Lists**.
2. Click the Aliases tab.

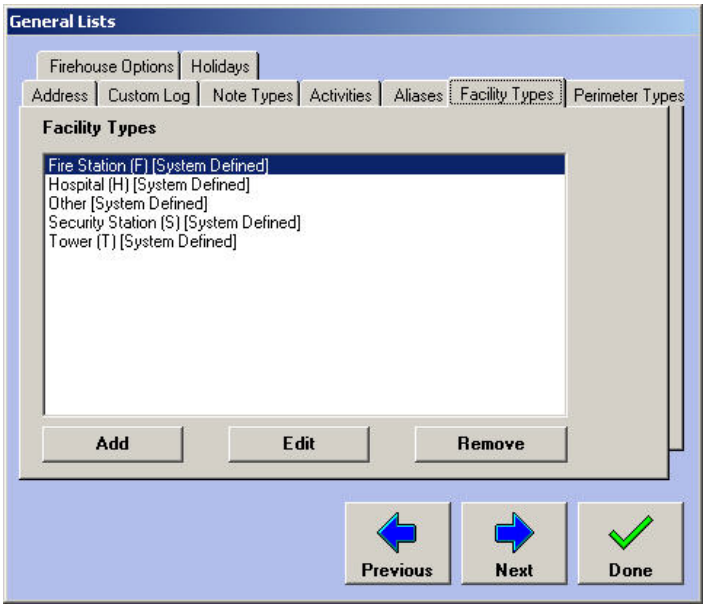


3. Select the site entry in the Object Name-Alias list.
4. Click **Edit**.

5. Type the new alias name.
6. Click **OK**.
7. Click **Done**.
8. Exit the D-21 Admin Client and log in again to view the change in the tree pane.

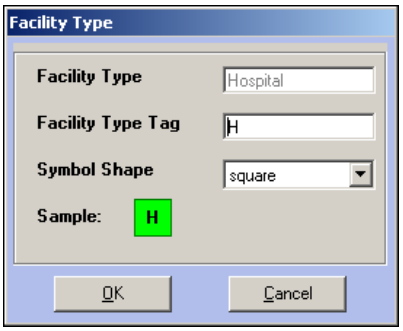
To create custom facility types and symbols

1. Select **Options > General Lists**.
2. Click the Facility Types tab.



- **Facility Type** Use the Facility Type tab to define new facility types on the map. Enter a name for the facility type and a single alphanumeric character in the Tag box. Select a symbol shape from the drop-down list. The character and symbol shape entered are displayed on the facility icon when it appears on the map in the D-21 Incident Client.

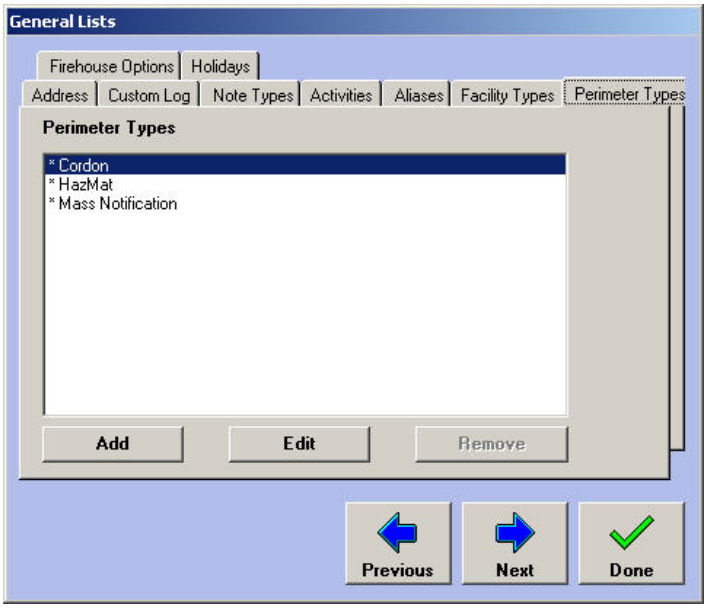
3. Click **Add** to add a new facility type to the list. A dialog box appears.



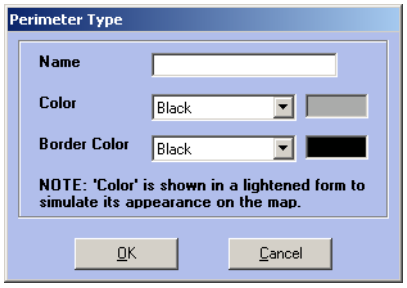
4. Enter the name, a tag letter, and a symbol shape.
5. Click **OK**.
6. Repeat the process until you have entered all the desired list items.
7. Click **Done**.

To customize perimeter types

1. Select **Options > General Lists**.
2. Click the Perimeter Type tab.
3. The Perimeter Types area shows the main Perimeter Types built into the D-21. The default perimeters cannot be deleted. Click **Add**.



4. The Add Perimeter dialog box appears



5. Fill in the Name field and change the color and border color to customize the new perimeter type. Click **OK**.
6. The new perimeter type will appear in the Perimeter Types area.

To edit a custom perimeter type

1. Select **Options > General Lists**.
2. Click the Perimeter Type tab.
3. Select the perimeter to be edited from the Perimeter Type area.
4. Click **Edit.**
5. Change the information in the perimeter type window.
6. Click **OK.**

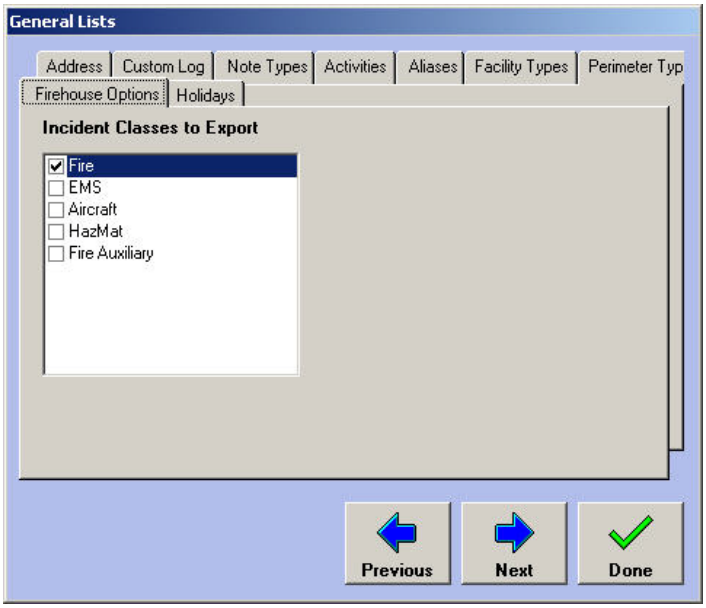
To remove a custom perimeter type

1. Select **Options > General Lists**.
2. Click the Perimeter Type tab.
3. Select the perimeter to be removed from the Perimeter Type area.
4. Click **Remove**, then click **Yes** when prompted to remove the perimeter.

To configure Firehouse options

1. Select **Options > General Lists**.
2. Click the Firehouse Options tab.

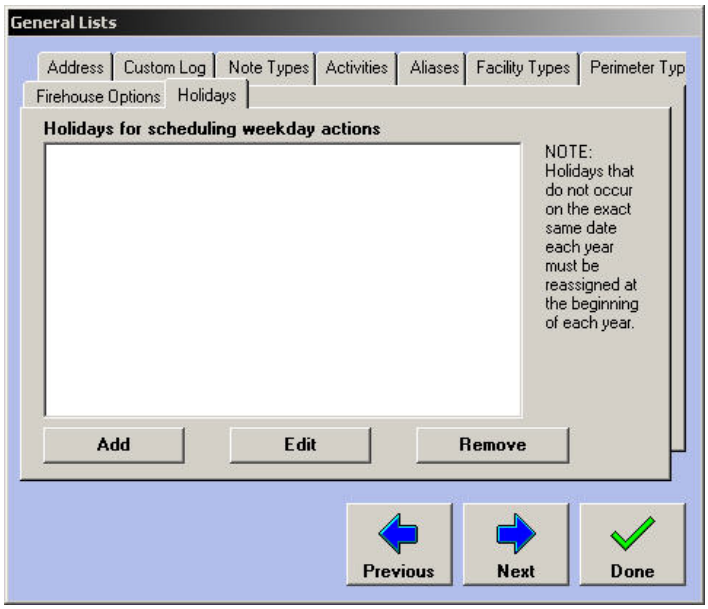
NOTE *The Firehouse Options tab will only appear when firehouse software is installed.*



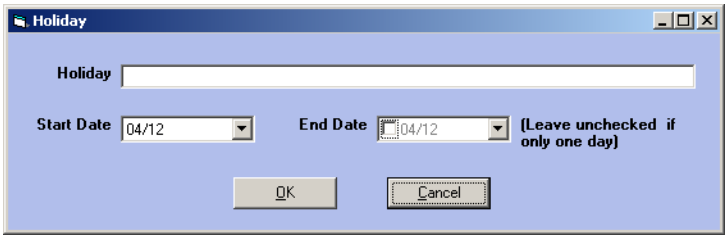
3. Select the incident class(es) you want the Firehouse software to export by selecting the checkbox for each class.
4. Click **Done**

To schedule holidays

1. Select **Options > General Lists**.
2. Click the Holidays tab.



3. To add a new Holiday click **Add**.



4. Type the holiday name into the Holiday field and select the Start and End dates from the date drop-down boxes. If the holiday is only one day, leave the End Date checkbox unchecked.

To edit a holiday

1. Select **Options > General Lists**.
2. Click the Holidays tab.
3. Select the desired holiday in the Holidays for scheduling weekday actions list.
4. Click **Edit.**
5. Change the information in the Holiday, Start Date, and/or End Date fields.
6. Click **OK.**

To remove a holiday

1. Select **Options > General Lists**.
2. Click the Holidays tab.

3 Select the desired holiday in the Holidays for scheduling weekday actions list.

4 Click **Remove**

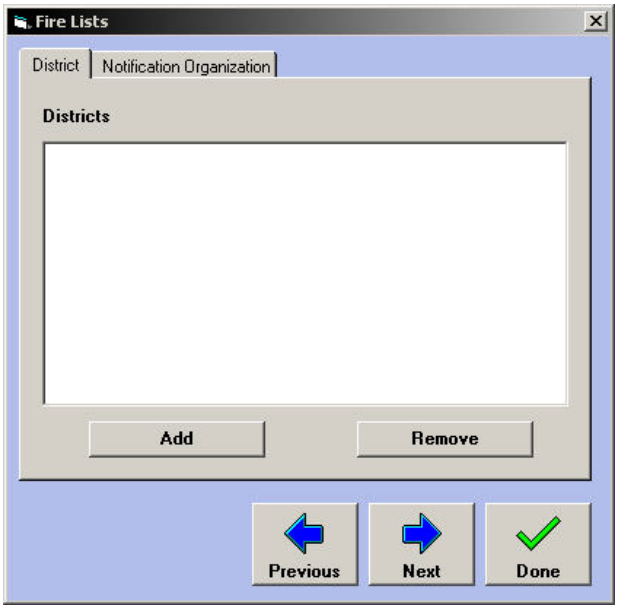
5 Click **Yes** when prompted to remove the selected holiday.

Fire Lists

This section includes procedures for customizing information that only appears when you are working with the D-21 Fire Client.

To create multiple fire districts for tracking incidents

1 Select **Options > Fire Lists**.



- **Districts** Use Districts to define geographical districts within a site. Incidents can be assigned to districts for incident reporting purposes in the D-21 Incident Client.

2 Click **Add**. A new entry dialog box appears.

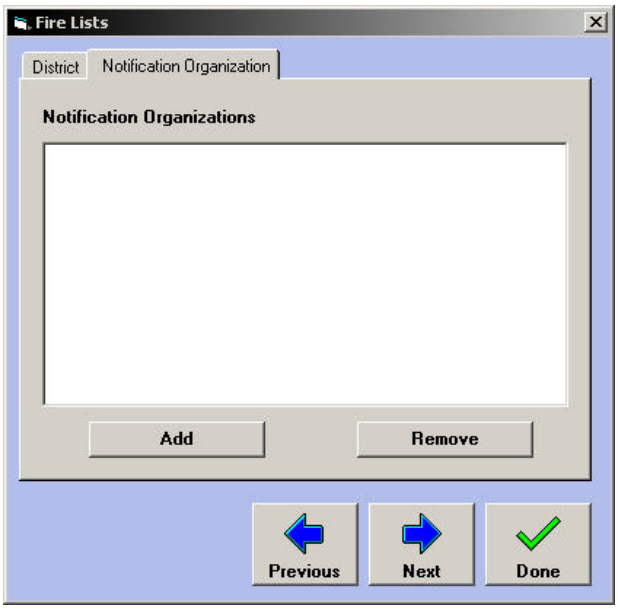
3 Type the name of the district. A district name can be up to five characters and include letters and numbers.

4 Click **OK**.

5 Click **Done**.

To add notification organizations

1. Select **Options > Fire Lists**.
2. Click the Notification Organization tab.



3. Click **Add**. A new entry dialog box appears.
4. Type the name of the Notification Organization.
5. Click **OK**.
6. Click **Done**.

Security Lists

This section includes procedures for customizing information that only appears when you are working with the D-21 Security Client.

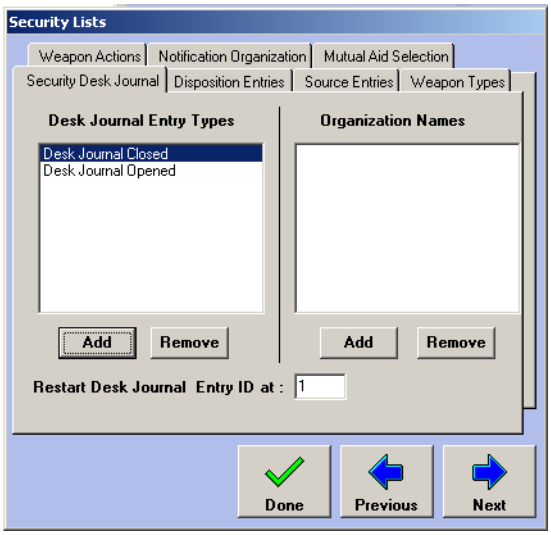
Setting Up Security Desk Journal Lists

The Security Desk Journal is a Daily Activity form in the D-21 Incident Client that is only available with the D-21 Security Client. The Desk Journal can be used to record security incidents and create reports customized for different organizations.

For more information on using the Security Desk Journal, contact Monaco Technical Support.

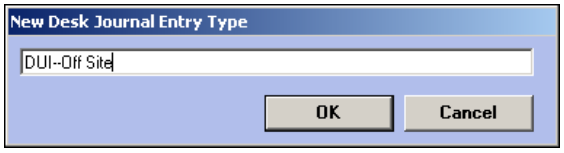
To add a new entry type to the Security Desk Journal

1. Select **Options > Security Lists**.
2. Click the Security Desk Journal tab.



- **Desk Journal Entry Types** Add the incident types you use to categorize each incident entry. The Desk Journal Opened and Desk Journal Closed entry types are default types that cannot be removed.
- **Organization Names** Add the names of administrative organizations that receive partial or complete copies of the Desk Journal report. When you enter an incident in the Desk Journal, you can list the organizations which you want to be able to view the incident. The Desk Journal report can then be filtered by the organizations involved, so you can control the incidents each organization sees.
- **Restart Desk Journal Entry ID at** Each entry in the Desk Journal is numbered. Enter the number you want the Security Desk Journal to use each time you open a new Desk Journal in the D-21 Incident Client.

3 Click **Add** under the Desk Journal Entry Types list. A new entry dialog box appears.



4 Type the new type in the entry box.

5 Click **OK**.

6 Click **Done**.

To delete Desk Journal entry types

1 In the Desk Journal Entry Types list, select the entry type you want to delete.

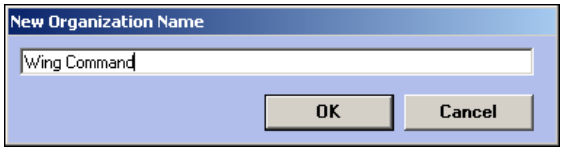
2 Click **Remove**.

To add Desk Journal organizations

1 Select **Options > Security Lists**.

2 Click the Desk Journal tab.

3 Click **Add** under the Organizations Names list. An entry dialog box appears.



4 Type the new organization name in the entry box.

5 Click **OK**.

To delete Desk Journal organizations

1 In the Organization Names list, select the organization name you want to delete.

2 Click **Remove**.

Setting Up Law Enforcement Lists

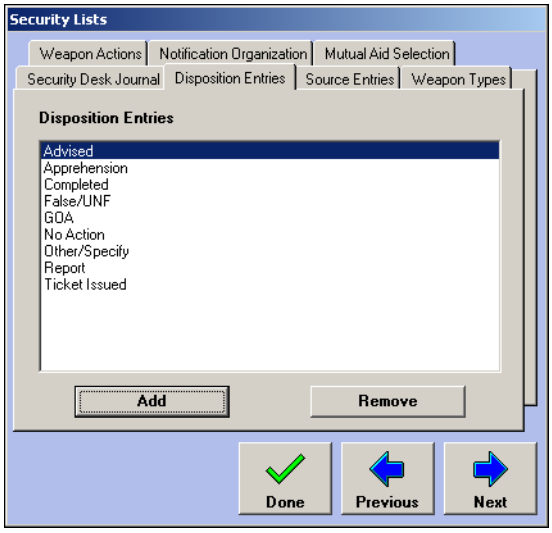
Law Enforcement is a D-21 Security Client option. If you have Law Enforcement installed, you can track and report law enforcement incidents in the D-21 Incident Client. You can use the general Security incident type to categorize law enforcement incidents, or you can create a list of custom law enforcement incident types using emergency cards. For example, you can set up emergency cards for "Vandalism" or "Domestic Disturbance" and then attach custom response plans to each. For more information, see "Emergency Cards" on page 3-20 and "Response Plans" on page 3-2.

You can customize the following information for law enforcement incidents:

- **Disposition** Use the Disposition field in law enforcement incidents to record the action taken by law enforcement officers for the incident, such as "Ticket Issued" or "No Action." See "To create a law enforcement incident disposition list" on page 4-17.
- **Mutual Aid** Use the Mutual Aid fields in law enforcement incidents to track the external organizations involved in the incident. For example, you can enter all of your ambulance companies and local hospitals and track which ones were part of the incident response. See "To create a list of law enforcement mutual aid" on page 4-20.
- **Notifications** Use the Notifications fields to track cooperating organizations that need to be contacted for an incident. When handling a law enforcement incident, you can record a contact person for the organization and the date and time when the contact was notified, arrived at the incident, and left the incident. See "To create a list of law enforcement notifications" on page 4-19.
- **Source** Use the Source field in law enforcement incidents to record if the incident originated due to a caller, walk-in report, regular patrol, etc. See "To create a list of law enforcement incident sources" on page 4-18.
- **Weapons** Use the Weapons fields in law enforcement incidents to record the type and firing action of weapons involved in an incident. See "To create lists of weapon types for Law Enforcement" on page 4-21.

To create a law enforcement incident disposition list

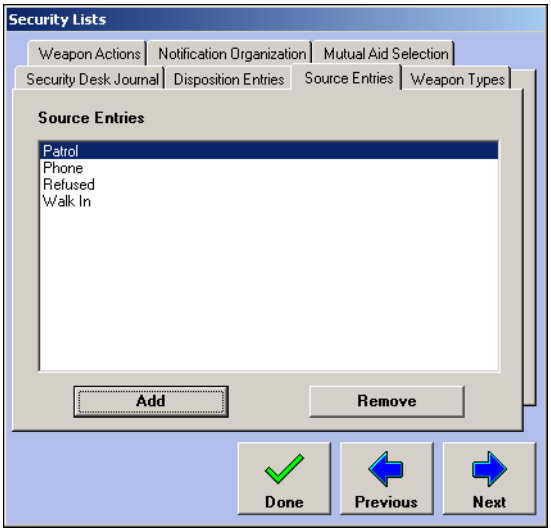
1. Select **Options > Security Lists**.
2. Click the Disposition Entries tab.



   - **Disposition Entries** Use Disposition Entries to track the type of incident response, such as Ticket Issued or No Action.
3. Click **Add**. A new entry dialog box appears.
4. Type a name for the new disposition type.
5. Click **OK**.
6. Click **Done**.

To create a list of law enforcement incident sources

1. Select **Options > Security Lists**.
2. Click the Source Entries tab.

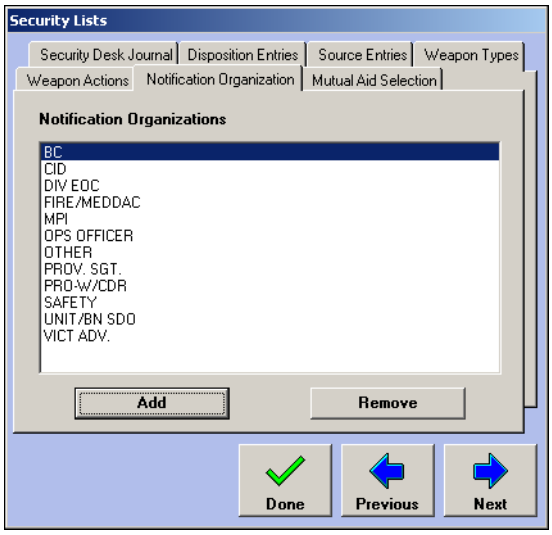


- **Source Entries** Use Source Entries to create a list of ways an incident was initiated, such as a phone call or report from a regular patrol.

3. Click **Add**. A new entry dialog box appears.
4. Type a name for the new type of incident source.
5. Click **OK**.
6. Click **Done**.

To create a list of law enforcement notifications

1. Select **Options > Security Lists**.
2. Click the Notification Organizations tab.

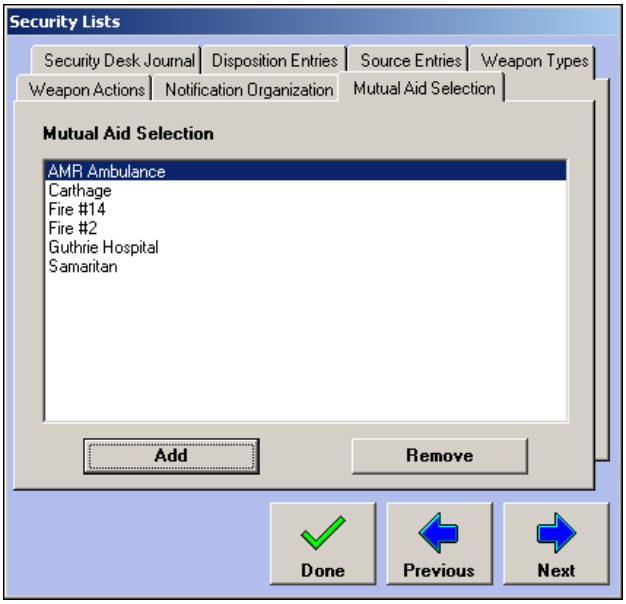


- **Notification Organizations** Use Notification Organizations to track notifications made to outside organizations or posts. For each notification entry, you can track a contact person, notified time, arrived time, and cleared time for each law enforcement incident created in the D-21 Incident Client.

3. Click **Add**. A new entry dialog box appears.
4. Type a name for the new organization.
5. Click **OK**.
6. Click **Done**.

To create a list of law enforcement mutual aid

1. Select **Options > Security Lists**.
2. Click the Mutual Aid Selection tab.

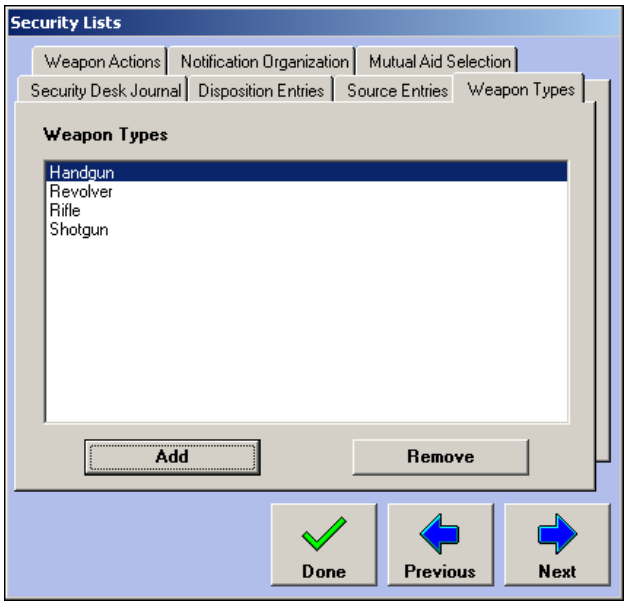


- **Mutual Aid Selection** Use Mutual Aid entries to track outside resources and agencies involved in responding to the incident. The D-21 does not track response times for Mutual Aid entries, and can only indicate whether or not Mutual Aid was involved in the incident. See the D-21 Incident Client User Guide (P/N 001-392-00) for more information.

3. Click **Add**. A new entry dialog box appears.
4. Type a name for the new entry.
5. Click **OK**.
6. Click **Done**.

To create lists of weapon types for Law Enforcement

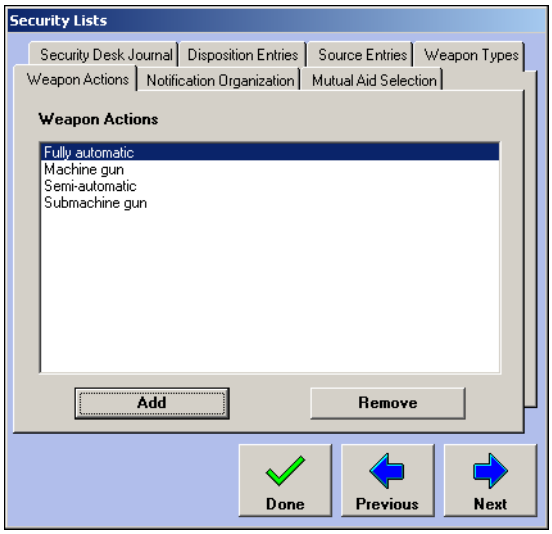
1. Select **Options > Security Lists**.
2. Click the Weapons Types tab.



   - **Weapon Types** Use Weapon Types to track what kind of weapon was involved in the incident.
3. Click **Add**. A new entry dialog box appears.
4. Type a name for the new entry.
5. Click **OK**.
6. Click **Done**.

To create a list of firing action types for Law Enforcement

1. Select **Options > Security Lists**.
2. Click the Weapons Actions tab.



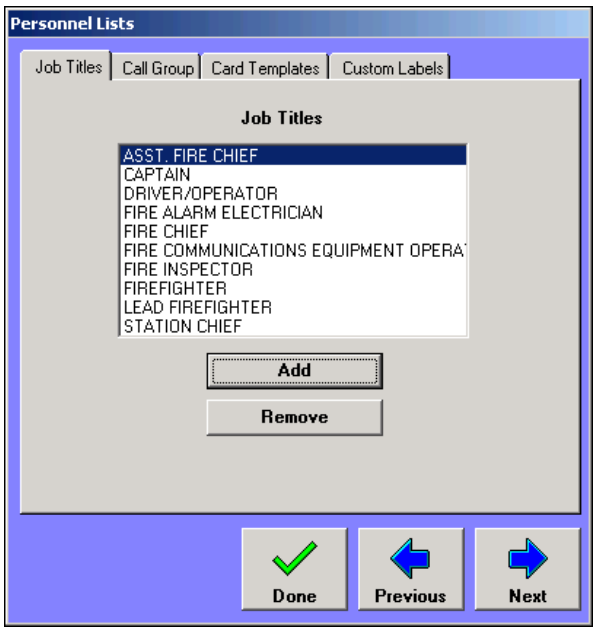
- **Weapon Actions** Use Weapon Actions to track the firing action of the weapons recorded with each incident.

3. Click **Add**. A new entry dialog box appears.
4. Type a name for the new entry.
5. Click **OK**.
6. Click **Done**.

Personnel Lists

Use the Personnel Lists dialog box to specify information that will appear in drop-down list boxes throughout the D-21 Admin Client and the D-21 Incident Client.

Figure 4-1 *Personnel Lists dialog box*



To add an item to a personnel list

1. Select **Options > Personnel Lists**.
2. Click the appropriate tab.
   - **Job Titles** The Job Titles tab allows the administrator to input job titles that can be used when entering or viewing personnel information, and when creating roster shift templates. For more information, see "Personnel" on page 2-85 and "Creating Rosters" on page 4-38.
   - **Card Templates** The Card Templates tab allows the administrator to create an entry for a card template.
   - **Call Group** The Call Group tab allows the administrator to create Call Groups for the Contact Info tab of the Person dialog box.
   - **Custom Labels** Use the Custom Labels tab to change the titles of the custom fields available in the Person dialog box in the D-21 Admin Client, including all the fields on the Custom tab. The Person dialog box is used when personnel is added or edited. These entries also appear in the personnel lists in the D-21 Incident Client. For more information, see "To create custom personnel fields" on page 4-24

To remove an item from a personnel list

1. Select **Options > Personnel Lists**.
2. Click the appropriate tab.
3. Select the item you wish to remove by clicking it.

4 Click the **Remove** button. A message will appear, asking whether you want to remove the item.

5 Click **Yes**.

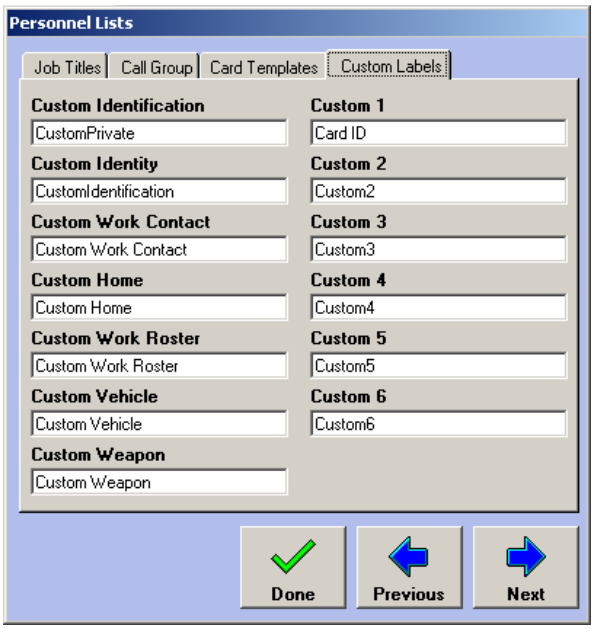
6 Repeat steps 2 through 5 until you have deleted all the items you want to remove.

7 Click **Done**.

To create custom personnel fields

1 Select **Options > Personnel Lists**.

2 Click the Custom Labels tab.



3 Edit the label entries. Entries in the left column are custom fields available on all the tabs in the Person dialog box (except the Name and Address tabs). Entries on the right are labels for each of the custom fields available on the Custom tab in the Person dialog box. These entries appear in the D-21 Admin Client when you add or edit personnel in the Person dialog box and in the D-21 Incident Client when you view a personnel list.

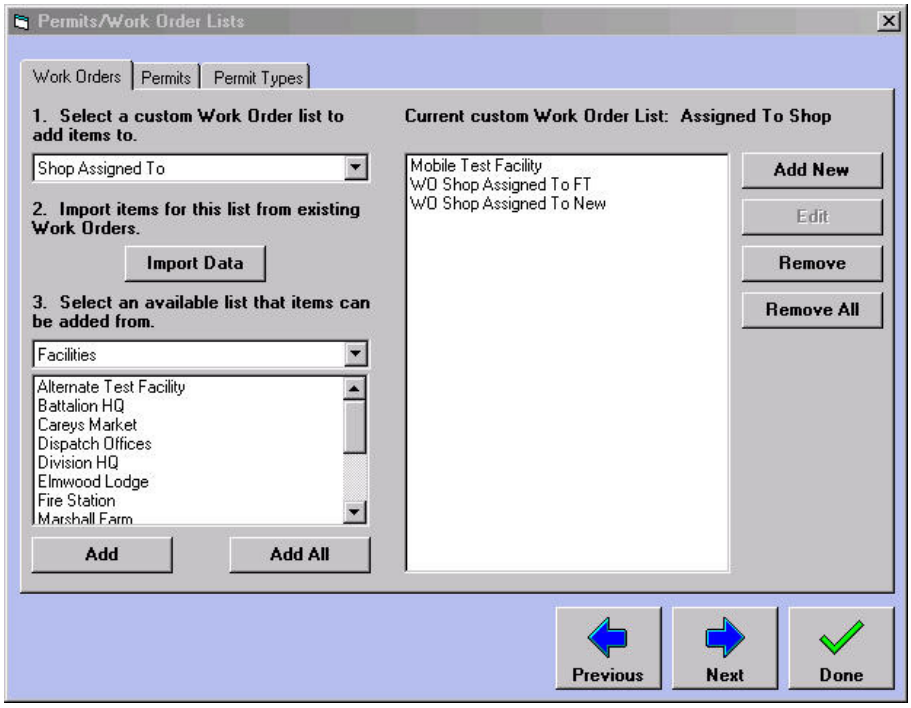
4 Click **Done**.

Permit/Work Order Lists

When users create permits and work orders in the D-21 Incident Client, pieces of information can be provided in one of two ways: by entering text, or by choosing an item from a drop-down list. Use Permit/Work Order Lists to define the list items on the permit- and work-order related drop-down lists used in the D-21 Incident Client, and to define permit types.

To populate a Work Order drop-down list

1 Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.



2 From the drop-down list marked **1. Select a custom Work Order list** select the Work Order list where items are being added. Available choices are: Shop Assigned To, Caller, Assigned To, and Completed By.

3 Click **Yes** in the confirmation dialog box.

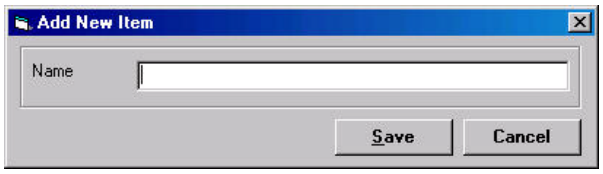
4 Click **Import Data** to see values that have already been entered in existing work orders. The Import List Items dialog box appears.

NOTE *If there are no existing work orders, the Import List Items list will be empty.*

5 Select any items that you would like to add to the current list. Holding down the **Ctrl** key and clicking non-adjacent individual items, or holding down the **Shift** key and clicking adjacent items allows the user to select multiple items from the list. When you are finished, click **Add**. Or, to simply add all the items to the list, click **Add All**.

6 You can also add items to the list you are working on from the D-21 Facilities, Personnel, and Resources lists. If you wish to do so, select the appropriate D-21 list from the drop-down list marked **3. Select an available list**. The box underneath the **3. Select an available list** heading displays the contents of the list selected from the drop-down list. Select any items that you would like to add to the list you are working on. Holding down the **Ctrl** key and clicking non-adjacent individual items, or holding down the **Shift** key and clicking adjacent items allows the user to select multiple items from the list. When you are finished, click **Add**. Or, to add all the items to the list, click **Add All**.

7 Click **Add New** to create items to add to the list you are working on. The following dialog box appears:



8 Type the name of the item you want to add to the list and click **Save**.

9 When you are finished adding items to the list, click **Done**. Or select a different Work Order list and repeat the process.

To modify a Work Order drop-down list

1 Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.

2 From the drop-down list marked **1. Select a custom Work Order list**, select the Work Order list you want to modify.

3 Click **Yes** in the confirmation dialog box. The current list items appear in the list box to the right.

4 To edit an item, select it in the list box and click **Edit**.

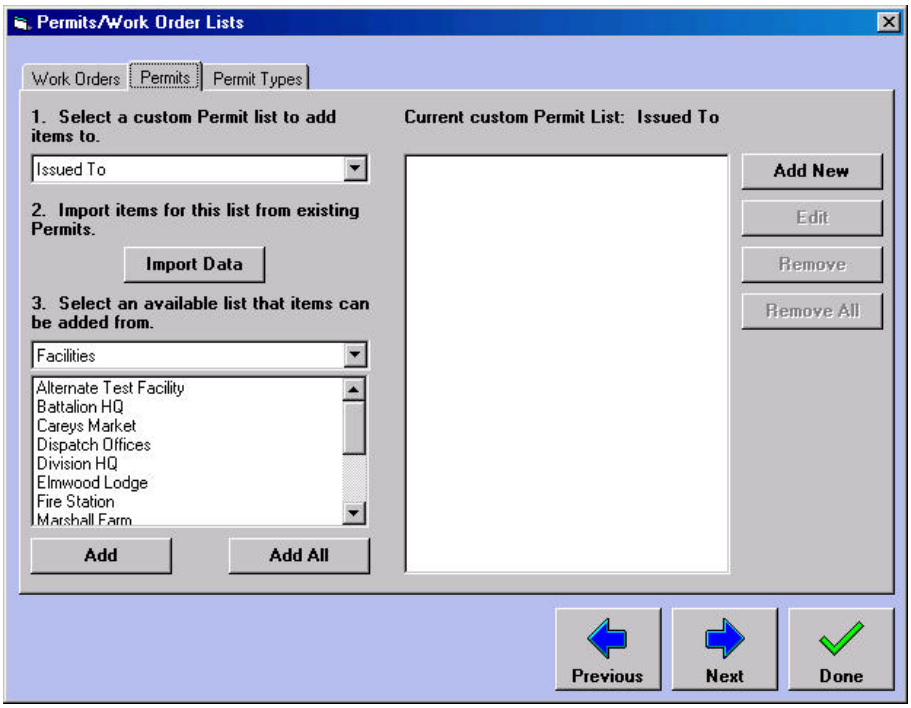
5 To remove an item, select it in the list box and click **Remove**.

6 To remove all the items, click **Remove All**.

7 When you are finished, click **Done**.

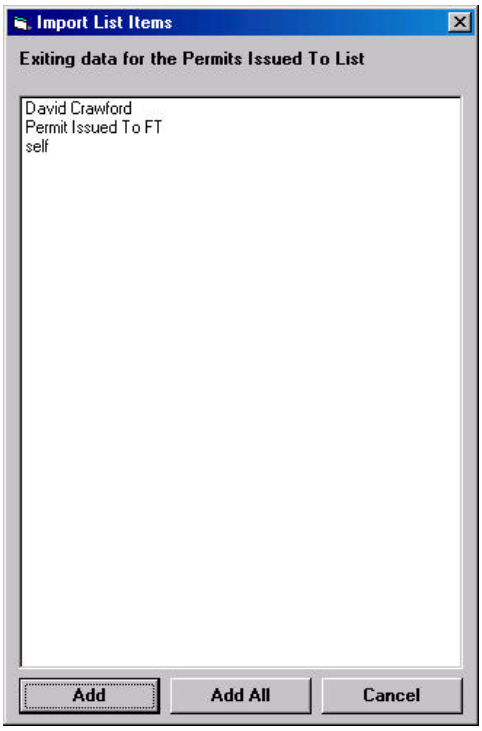
To populate a Permit drop-down list

1. Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.
2. Click the Permits tab.



3. Select the Permit list to add items to from the drop-down list marked **1. Select a custom Permit list**. The available choices are: Issued To, Caller, Issued By, Called In Complete By, and Completed By.
4. Click **Yes** in the confirmation dialog box.

5 Click **Import Data** to see values that have already been entered in existing work orders. The Import List Items dialog box appears.

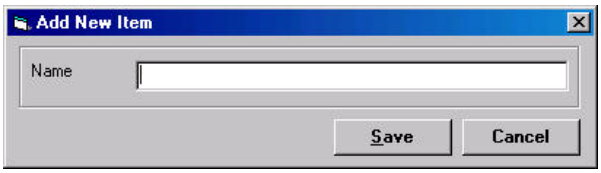


NOTE *If there are no existing permits, the Import List Items list will be empty.*

6 Select any items that you would like to add to the current list. Holding down the **Ctrl** key and clicking non-adjacent individual items, or holding down the **Shift** key and clicking adjacent items allows the user to select multiple items from the list. When you are finished, click **Add**. Or, to add all the items to the list, click **Add All**.

7 You can also add items to the list you are working on from the D-21 Facilities, Personnel, and Resources lists. If you wish to do so, select the appropriate D-21 list from the drop-down list marked **3. Select an available list**. The box underneath the **3. Select an available list** heading displays the contents of the list selected from the drop-down list. Select any items that you would like to add to the list you are working on. Holding down the **Ctrl** key and clicking non-adjacent individual items, or holding down the **Shift** key and clicking adjacent items allows the user to select multiple items from the list. When you are finished, click **Add**. Or, to add all the items to the list, click **Add All**.

8 Click **Add New** to add items to the list you are currently working on. The following dialog box appears:



9 Type the name of the item you want to add to the list, and click **Save**.

10 When you are finished adding items to the list, click **Done**. Or select a different Permit list and repeat the process.

To modify a Permit drop-down list

1 Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.

2 Click the Permits tab.

3 Select the Work Order list you want to modify from the drop-down list marked **1. Select a custom Work Order list**.

4 Click **Yes** in the confirmation dialog box. The current list items appear in the list box to the right.

5 To edit an item, select it in the list box and click **Edit**.

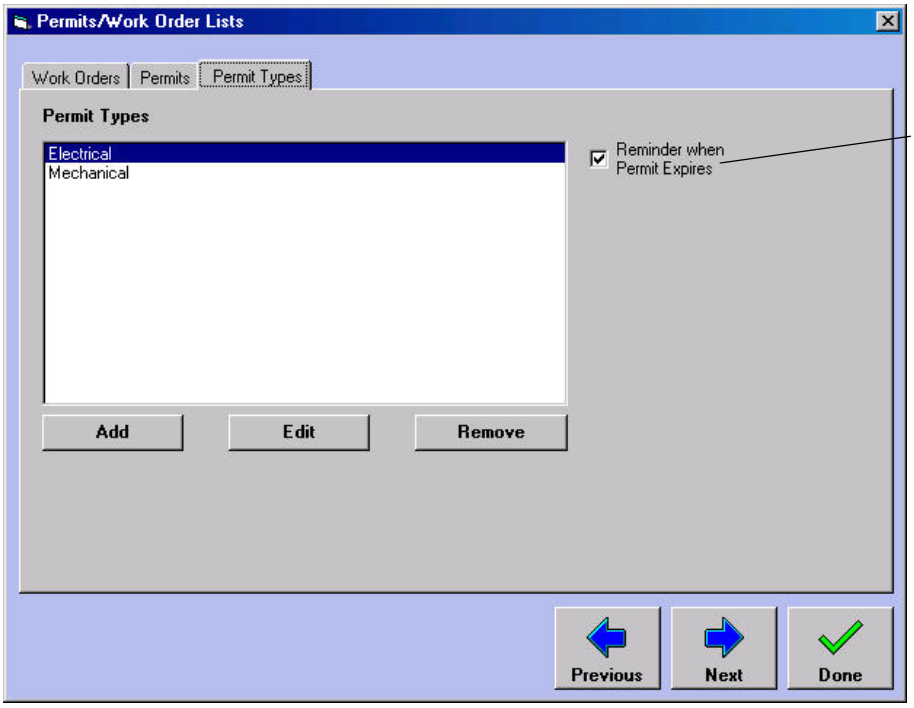
6 To remove an item, select it in the list box and click **Remove**.

7 To remove all the items, click **Remove All**.

8 When you are finished, click **Done**.

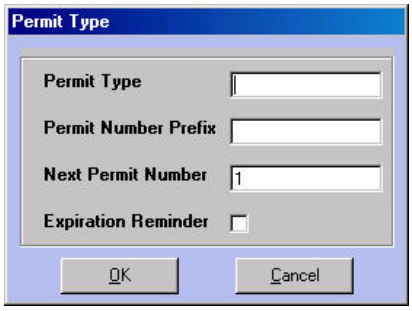
To add a Permit Type

1. Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.
2. Click the Permit Types tab.



Indicates whether the selected permit type is set to send a reminder when a permit expires

3. Click **Add**. The Permit Type dialog box appears.

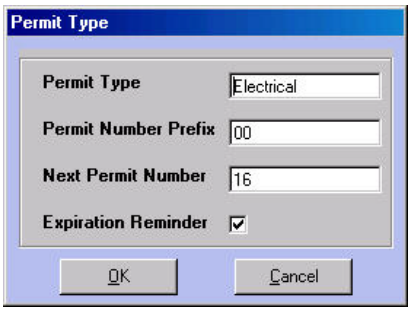


- **Permit Type** The name of the permit type.
- **Permit Number Prefix** The alphanumeric string, if any, to be added at the beginning of the permit number for all permits of this type (e.g. 'E-' for electrical permits).
- **Next Permit Number** The next number to be assigned when a new permit is issued. Subsequent permits will increase by an increment of one.
- **Expiration Reminder** When selected, indicates a reminder will be displayed in the D-21 Incident Client when a permit of this type expires.

4. Fill in the name of the new permit type and additional data as desired. When you are finished, click **OK**.

To edit a Permit Type

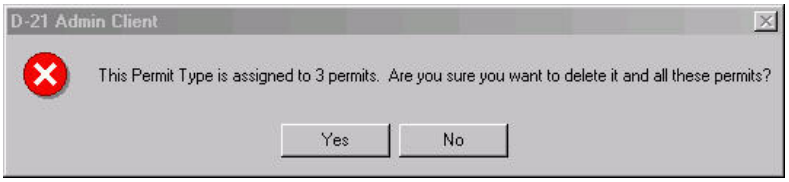
1. Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.
2. Click the Permit Types tab.
3. Select the permit type you wish to edit and click **Edit**. The Permit Type dialog box appears, populated with the values of the permit type you selected.



4. Make changes as necessary. When you are finished, click **OK**.

To remove a Permit Type

1. Select **Options > Permits/Work Order Lists**. The Permits/Work Order Lists dialog box appears.
2. Click the Permit Types tab.
3. Select the permit type you wish to remove and click **Remove**. A warning dialog box appears to inform you that any existing permits assigned to the permit type will also be deleted.



4. Click **Yes** to remove the permit type.

Setting Map Options (D-21 M)

The following options for the D-21 Map are configured in the D-21 Admin Client:

- Shortest routes colors and auto-routing (requires the Shortest Route map option).
- Closed road color (requires the Shortest Route map option).
- Default map location for incidents without map coordinates (requires either the Incident Relocating or Auto-Addressing map option).

NOTE *See the D-21 Map Options User Guide (P/N 001-464-00) for a full discussion of the D-21 Map and all of its options.*

Configuring Shortest Routes

When the Shortest Route map option is enabled, the D-21 Incident Client map can calculate and display the shortest route between two user-selected points. Shortest route calculations take into consideration detours made necessary by road closures, hazmat plumes, and perimeters as specified by the user.

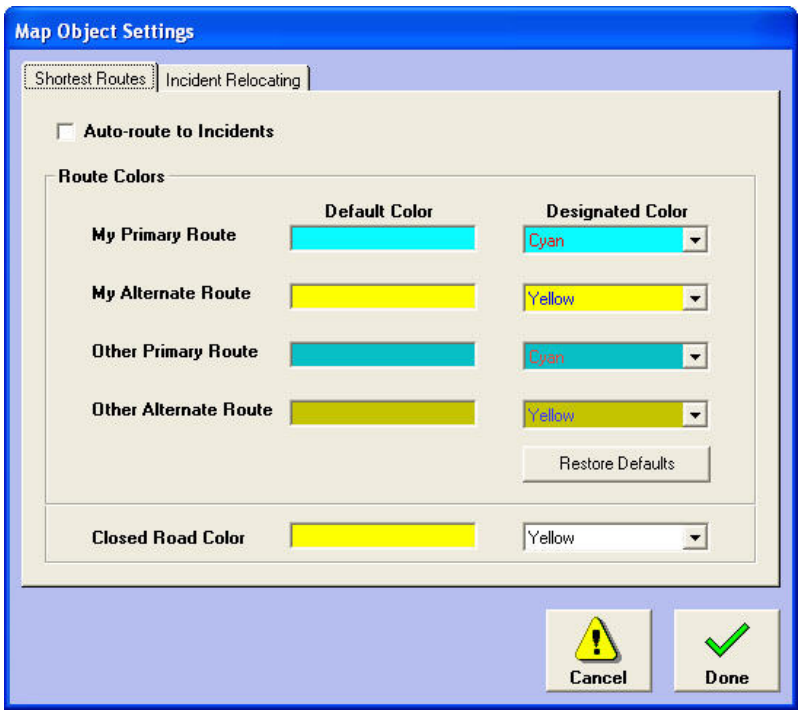
The D-21 Map can also automatically generate a route from a D-21 workstation location to an incident location whenever an incident is created, an option that is highly beneficial to systems that include Mobile Client workstations.

Follow these steps in the D-21 Admin Client to configure automatic shortest routes:

- Enable and configure the Automatic Shortest Route feature for the entire D-21 network. See "To enable automatic shortest routes" on page 4-34.
- Define the D-21 facility location for each D-21 workstation that will display automatic shortest routes. See "To configure workstation computer options" on page 4-49.
- If necessary, turn off automatic shortest routes for individual D-21 workstations. See "To configure workstation computer options" on page 4-49.

To enable automatic shortest routes

1 Select **Options > Map Object Settings**. The Map Object Settings dialog box appears with the Shortest Routes tab selected.



2 Click the checkbox labeled **Auto-route to Incidents** so a check mark appears.

3 Set **Route Colors** as desired.

- **My Primary Route** The color for a direct route between the incident and the D-21 workstation displaying the route. A primary route does not take into consideration road closures, hazmat plumes, and perimeters.
- **My Alternate Route** The color for a detoured route between the incident and the D-21 workstation displaying the route. An alternate route takes into consideration road closures, hazmat plumes, and perimeters.
- **Other Primary Route** The color for primary routes for other D-21 workstations.
- **Other Alternate Route** The color for alternate routes for other D-21 workstations.

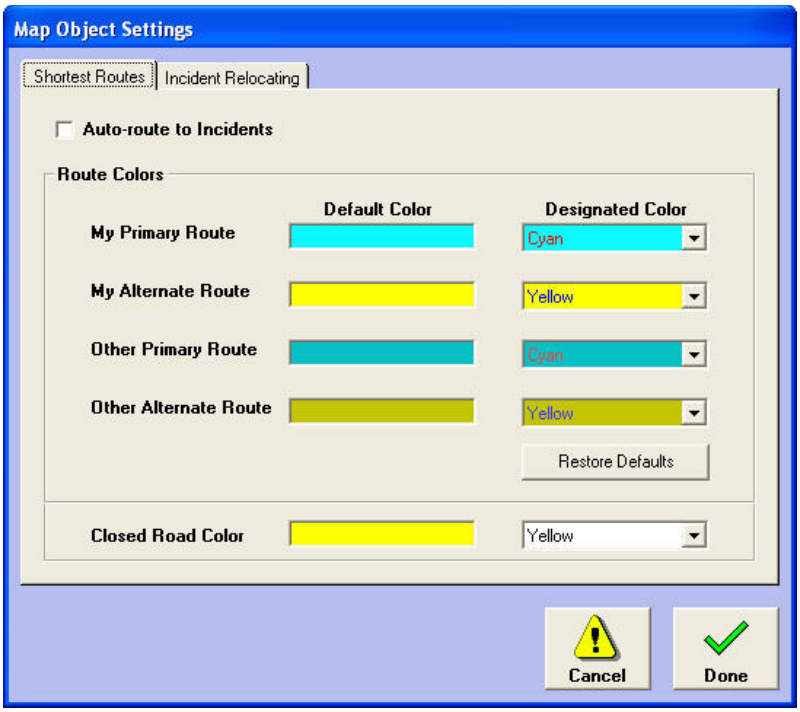
4 When you are finished, click **Done**.

Setting Road Closure Color

When a road segment is marked as closed on the D-21 Map, the segment is displayed in a different color. You can select a different color for closed road segments, if necessary.

To set the color for closed roads

1 Select **Options > Map Object Settings**. The Map Object Settings dialog box appears with the Shortest Routes tab selected.



2 Select the desired color from the drop-down list for **Closed Road Color**.

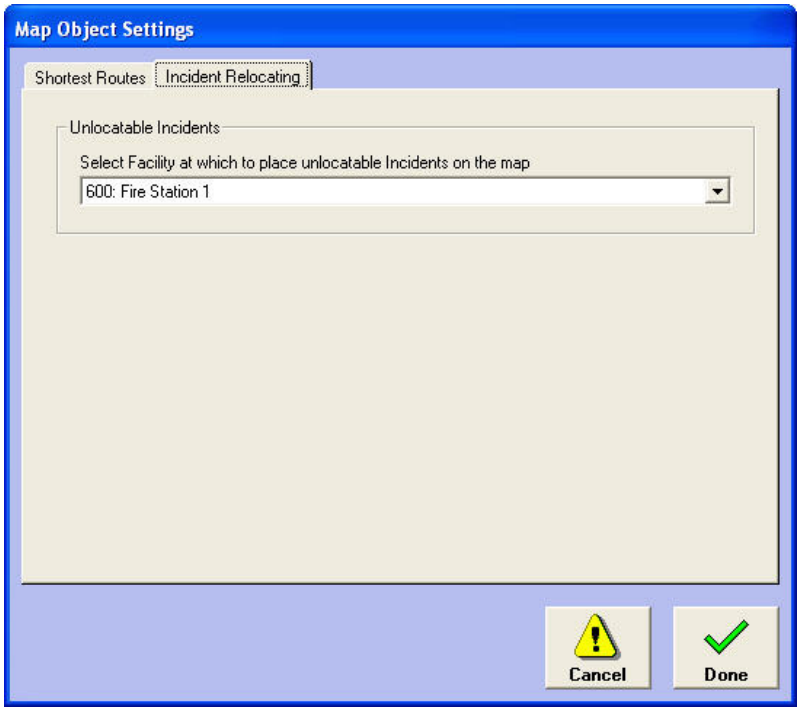
3 When you are finished, click **Done**.

Configuring Incident Relocating

When either the Incident Relocating or Auto-Addressing map option is enabled, all incidents are displayed on the D-21 map. Most incidents receive their map coordinates from the D-21 facility associated with the incident, but occasionally an incident can be created that does not have a map location. This type of scenario usually occurs when an alert comes in from a facility that has not yet been placed on the map. In such a situation, the D-21 places the incident icon at a default location on the map, displays a message saying that the incident icon should be manually moved to the correct location, and flashes the incident icon until the user moves it. You can select the facility to use as the default incident location for incidents without map coordinates in the D-21 Admin Client.

To set a default map location for incidents without map coordinates

1. Select **Options > Map Object Settings**. The Map Object Settings dialog box appears with the Shortest Routes tab selected.
2. Select the Incident Relocating tab.



3. From the drop-down list, select the facility you want to use as the default location. (You might select the facility containing the dispatch workstation.)
4. When you are finished, click **Done**.

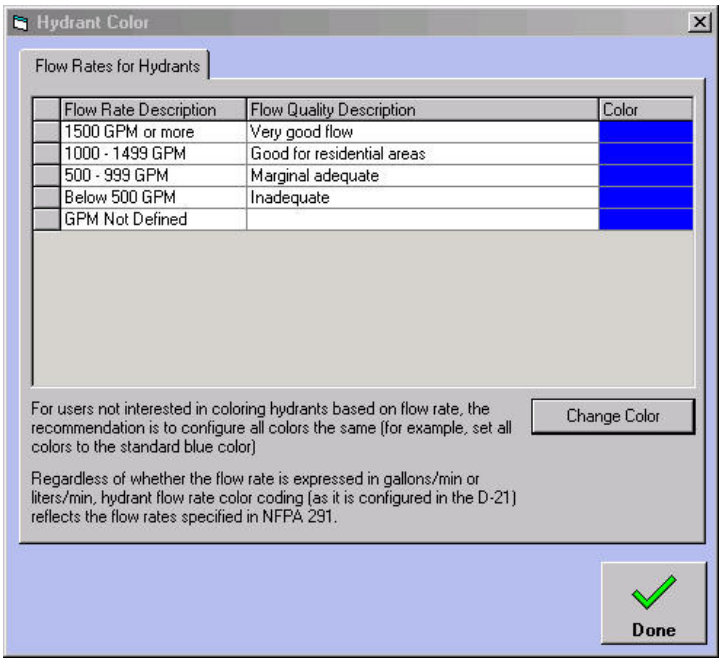
Setting Hydrant Colors

You can specify different colors for hydrants, based on hydrant flow rate, to be displayed on the D-21 Incident Client Map or in the D-21 Incident Client Hydrant Viewer. Five categories of flow rates are defined, based on NFPA 291:

- 1500 GPM or more: Very good flow.
- 1000 - 1499 GPM: Good for residential areas.
- 500 - 999 GPM: Marginal adequate.
- Below 500 GPM: Inadequate.
- GPM Not Defined.

To set hydrant colors based on flow rate

1 Select **Options > Hydrant Color**. The Hydrant Color dialog box opens.



2 Select the flow rate category for which you want to specify a color, and click **Change Color**. The color picker dialog box appears.

3 Click in a color box to select it, then click **OK**. The color picker dialog box closes, and the flow rate category's color in the Hydrant Color dialog box reflects the selection.

4 When you are finished selecting colors for the flow rate categories, click **Done**.

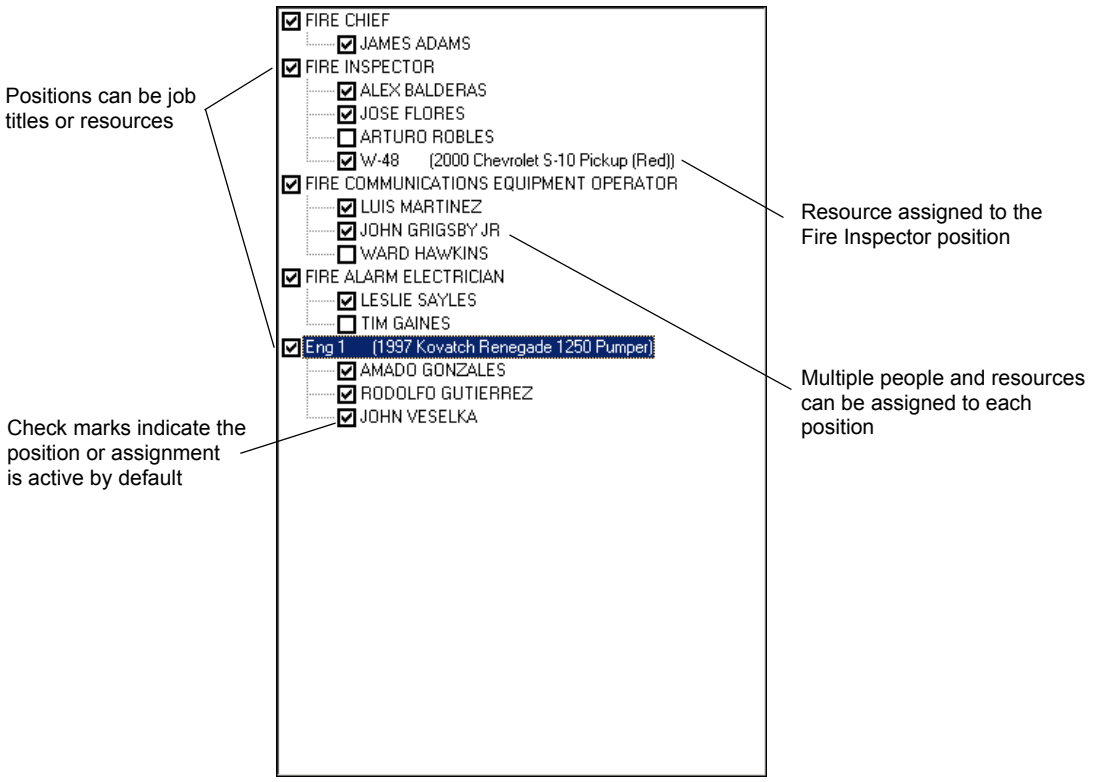
Creating Rosters

Use the Roster to create duty shift templates that assign personnel and resources to shift positions. Shift templates are created by defining positions using job titles and resources and then assigning personnel and resources to the shift positions. Shift templates created in the D-21 Admin Client are made available in the D-21 Incident Client for building daily rosters. You can build a roster using as many shift templates as you need to define your organization. Duty types can then be created for use in the D-21 Incident Client to track the status of personnel in the roster. See "To create roster duty types" on page 4-43.

Shift templates are classed as Fire, Security, or All. If the shift template is Fire, you can only add fire resources to the shift and the shift template will only be displayed on workstations that have the Fire Client enabled. If the shift template is Security, you can only build the shift

template using Security resources and you will only see the shift on workstations that have the Security Client enabled. If you want to build templates that use both fire and security resources, select All when specifying the class for the shift template.

Figure 4-2
Shift template



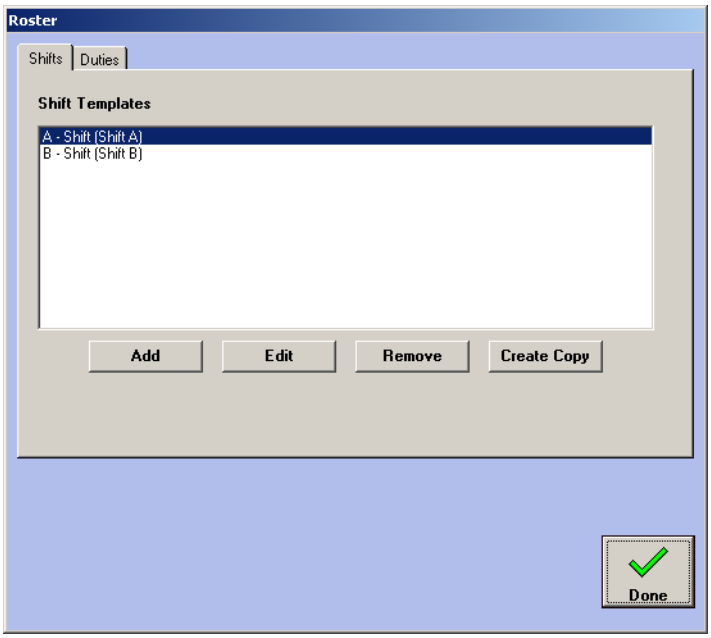
Before you begin

Create the job titles required to create the shift template. A job title can be an organizational position, a rank, or a task that must be performed during the course of the shift. See "Personnel Lists" on page 4-23.

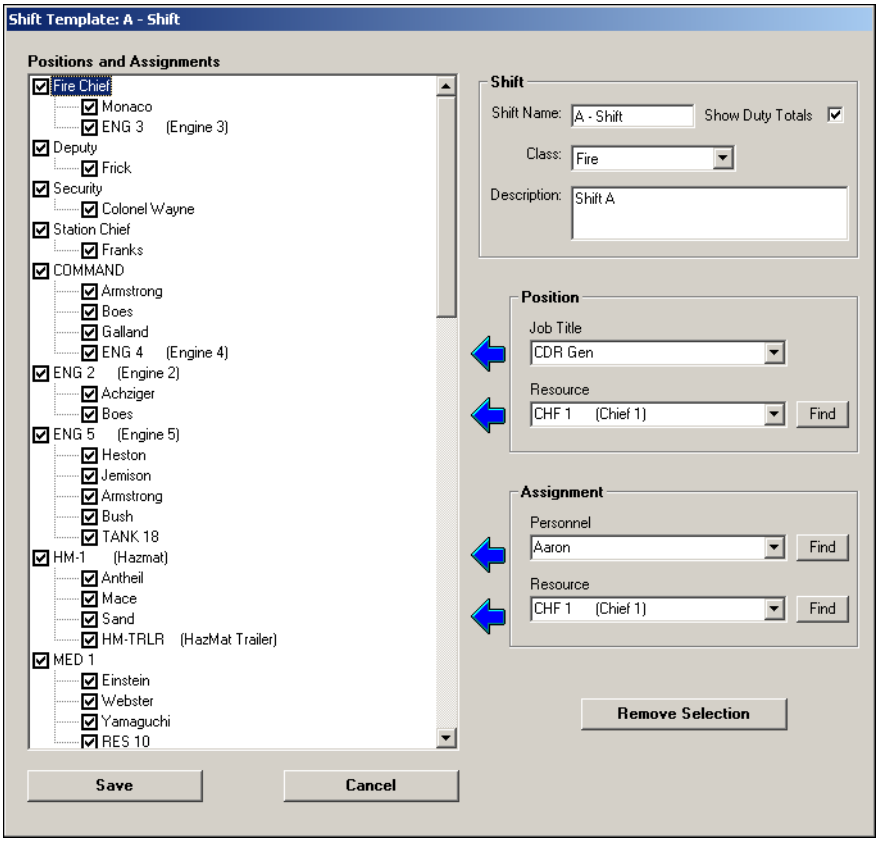
Create the resources you need to create the shift template. See "Resources" on page 2-103 for more information. Resources, such as fire trucks, can be used as shift positions when you want to assign and track personnel by resource.

To create a shift template

1 Select **Options > Roster**. The Roster dialog box appears.



2 Click **Add**. The Shift Template dialog box appears.



3 Type a name for the shift in the Shift Name box.

4 Select a class from the Class drop-down list.

- **All** All resources are available for creating the shift template and the shift template is available for building a roster on workstations with either the Fire or Security Client enabled.
- **Fire** Only fire resources are available for creating the shift template and the shift template is available for building a roster only on workstations with the Fire Client enabled.
- **Security** Only security resources are available for creating the shift template and the shift template is available for building a roster only on workstations with the Security Client enabled.
- **Facility Management** Only facility management resources are available for creating the shift template and the shift template is available for building a roster only on workstations with Facility Management enabled.

5 Type a description for the shift, such as the shift duration, in the Description box.

6 Click the Show Duty Totals check box if you want the shift to display the totals for each duty type when the roster is printed.

7 Build the organizational structure of the shift by adding positions.

a Select a job title in the Position Job Title drop-down list. See "Personnel Lists" on page 4-23 if the job titles you need are not available.

b Click the arrow to the left of the drop-down list to add the job title to the Positions and Assignments tree.

c Select a resource in the Position Resource drop-down list. See "Resources" on page 2-103 if the resources you need are not available.

d Click the arrow to the left of the drop-down list to add the resource to the Positions and Assignments tree.

e Continue adding jobs and resources until the shift template is complete.

8 Assign personnel and resources to the positions.

a In the Positions and Assignments tree, select the position (job title or resource) to which you want to make an assignment.

b Select the person or resource from the Assignments drop-down lists.

NOTE *If the person you want to assign does not appear in the Assignments list, make sure the Include in Roster personnel lists option is checkmarked in the person's database information. This option is located on the Name tab in the Person dialog box. See "To add a person" on page 2-86.*

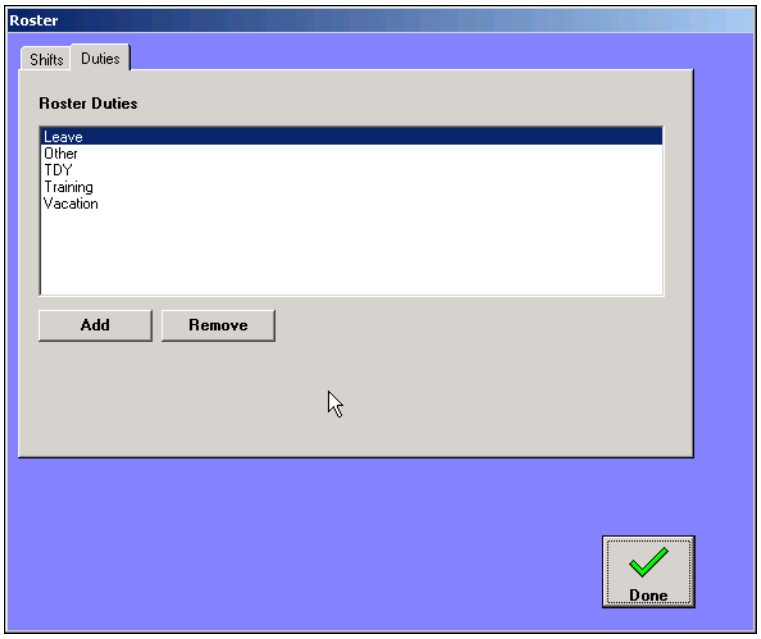
c Click the arrow to the left of the drop-down list item you want to assign.

9 When you are finished building the shift template, click **Save**.

NOTE *If you need a shift template similar to one you have already created, use the Create Copy button to create a copy and then make changes to the new template. See "To copy a shift template" on page 4-44.*

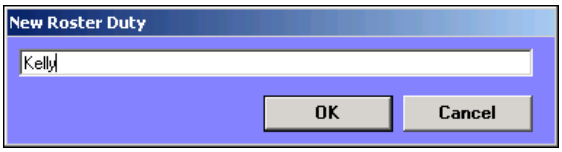
To create roster duty types

1. Select **Options > Roster**. The Roster dialog box appears.
2. Click the Duties tab.



NOTE *Duty types are used to track changes in personnel shift assignments in the D-21 Incident Client. When a person is assigned to a duty type, they are removed from the On Duty or active status. If Show Duty Totals is checked when creating the template, all duty type totals are tallied in the printed roster.*

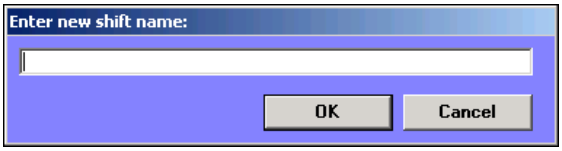
3. Click **Add**. The New Roster Duty dialog box appears.



4. Enter the name of the duty type. Typical duty types include: Leave, Vacation, Training, TDY, and On Leave.
5. Click **OK**.

To copy a shift template

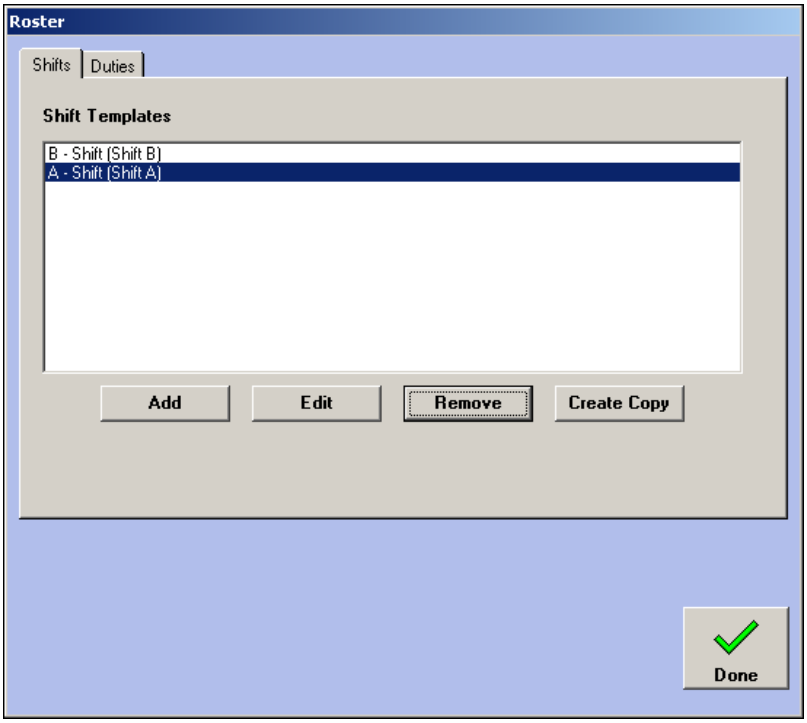
1. Select **Options > Roster**. The Roster dialog box appears.
2. Select the shift template you want to copy from the list on the Shifts tab.
3. Click **Create Copy**.



4. Type the name of the new shift template.
5. Click **OK**.

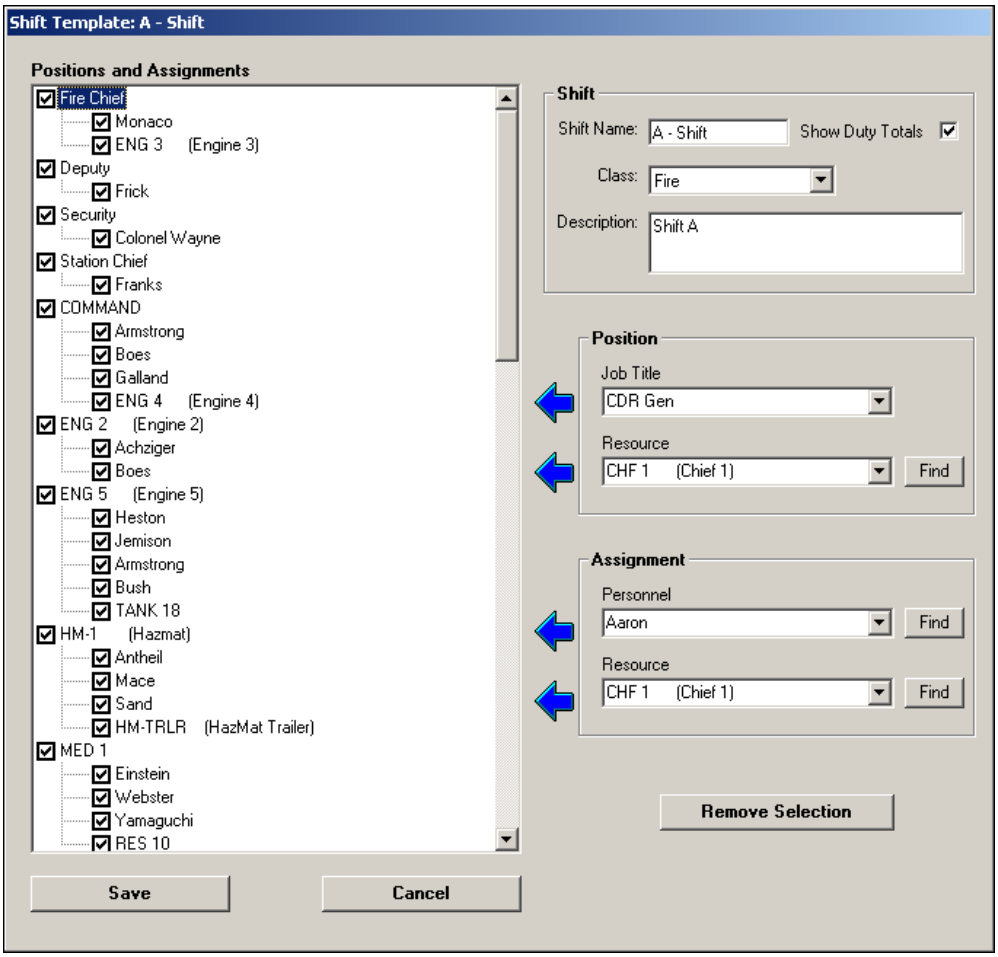
To edit a shift template

1. Select **Options > Roster**. The Roster dialog box appears.
2. Click the Shifts tab.



3. Select the shift you want to edit.

4 Click **Edit**. The Edit Shift dialog box appears.



- **Positions and Assignments** Clear the check box next to a position or assignment to temporarily remove it from the roster.
- **Shift** Enter a name and description for the shift. Click the **Show Duty Totals** check box to display the totals for each duty type when the roster is printed.
- **Position** Select a job title or resource you want to add to the shift and click the arrow. Click **Find** to locate a resource in the D-21's list of resources.
- **Assignment** Select the personnel or resources you want to add to a position and click the arrow. Click **Find** to locate personnel or resources.
- **Remove Selection** To delete a shift entry, select a position or assignment and click **Remove Selection**. Removing a position also removes all its associated assignments.

5 Click **Save**.

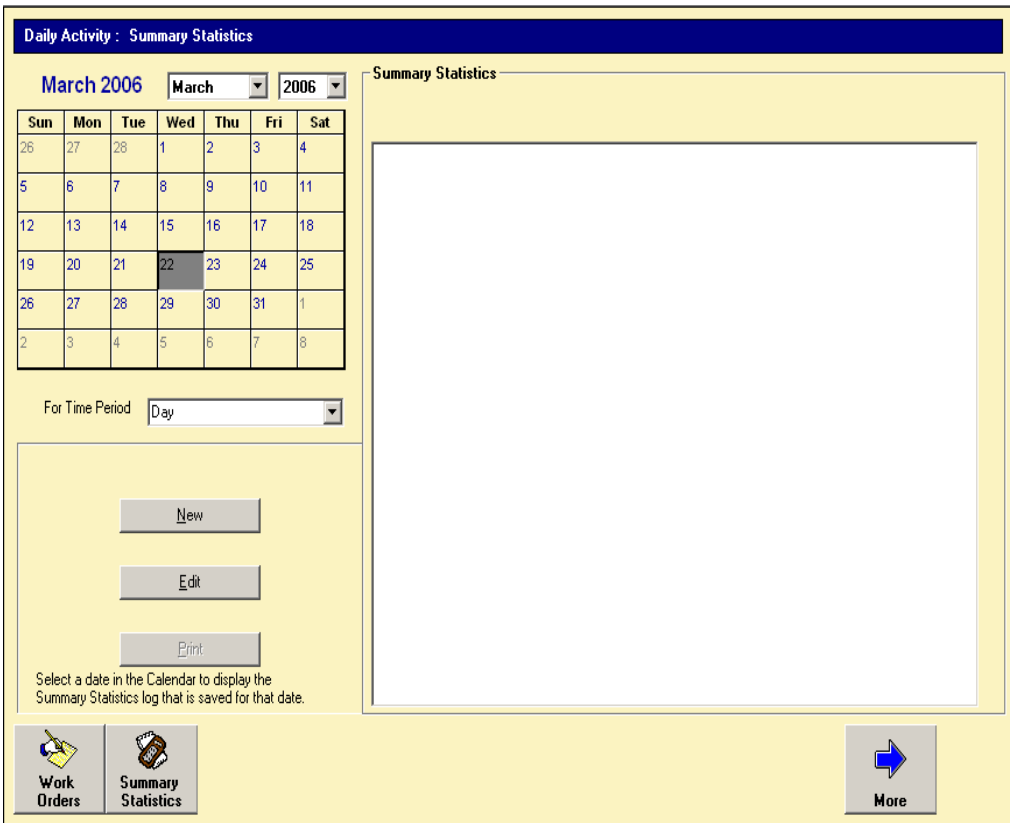
To delete a shift template

1. Select **Options > Roster**. The Roster dialog box appears.
2. Click the Shifts tab.
3. Select the shift you want to delete.
4. Click **Remove**.
5. Click **Yes** to confirm the selection.

Creating a Summary Statistics Log

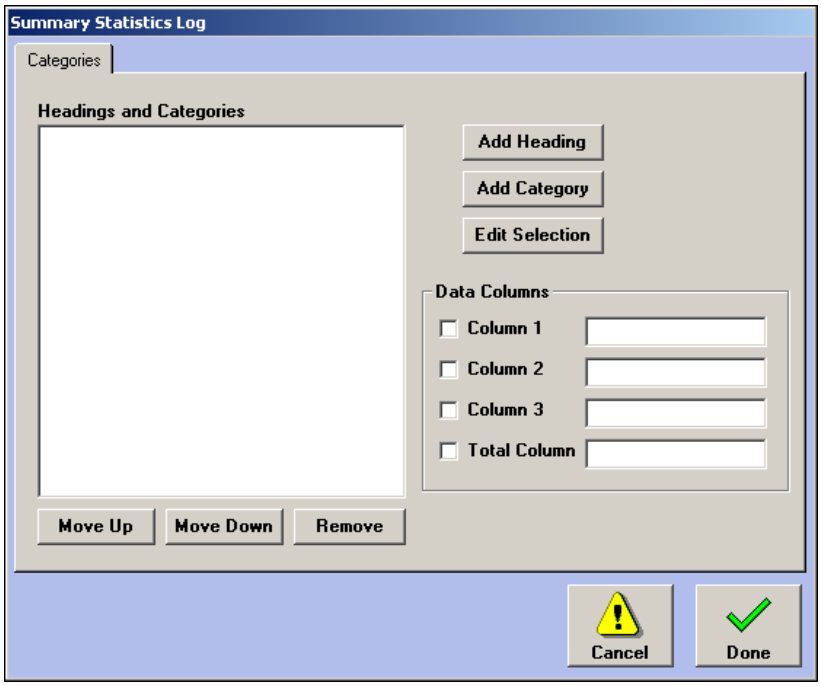
The Summary Statistics Log is a standard Daily Activity form that can be used to track non-critical administrative activities and tasks. For each item you want to track, you can add up to three fields for entering numbers. The numbers can then be tallied in a Total Column.

Figure 4-3
Summary Statistics Log sample



To create a Summary Statistics Log

1 Select **Options > Summary Statistics Log**. The Summary Statistics Log dialog box appears.

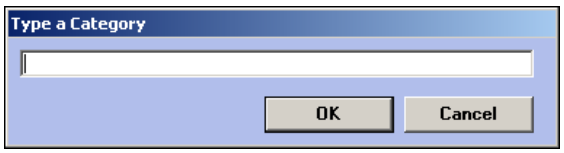


- **Heading** Use headings to create titles for groups of items. You cannot enter statistics for headings. If you want to group items under a heading, you must add the heading first.
- **Category** Use categories for the items that you want to track. You can track up to three sets of numeric data for each item.
- **Column** Use columns to specify how many numeric sets you want to track for each item. A name is required for each column you select. The Total Column, if selected, displays the sum of the numbers entered in all columns. The column names are used for all categories.

2 Click **Add Heading** to enter a heading for a group of categories. If you want to create a group of categories with a heading, you must create the heading first.

3 Select the heading in the Headings and Categories list under which you want to add a category.

4 Click **Add Category**. An entry dialog box appears.



5 Type the name of the category.

6 Click **OK**.

7 Continue adding headings and categories until the Headings and Categories list contains all the types of data you want to track.

NOTE *You can edit a heading or category by selecting it in the list and clicking* **Edit Selection**. *You can change the order of a category by selecting it and using* **Move Up** *and* **Move Down**.

8 Click the checkbox next to each column you want to create in the Summary Statistics Log.

9 Type a column heading name for each column. A column name is required for each selected data column.

10 Click **Done**.

For more information on how to use the Summary Statistics Log, see the D-21 Incident Client User Guide (P/N 001-392-00).

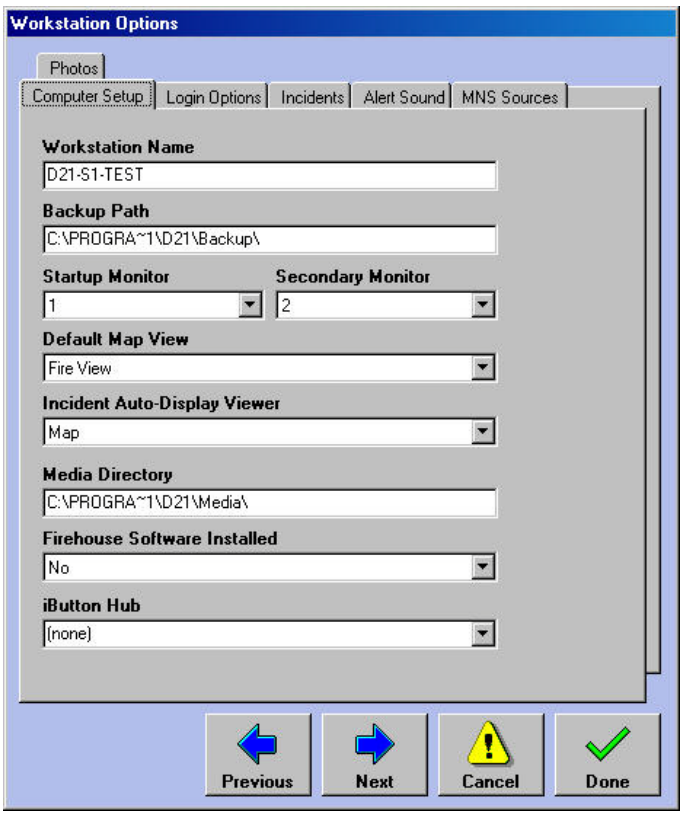
Setting Workstation Options

Use the Workstation Options dialog box to configure the D-21 Incident Client on the computer on which you are currently running the D-21 Admin Client. You must run the D-21 Admin Client and set the workstation options on each computer you want to configure.

NOTE *The Workstation Options available depend on the D-21 products and components installed.*

To configure workstation computer options

1 Select **Options > Workstation Options**.



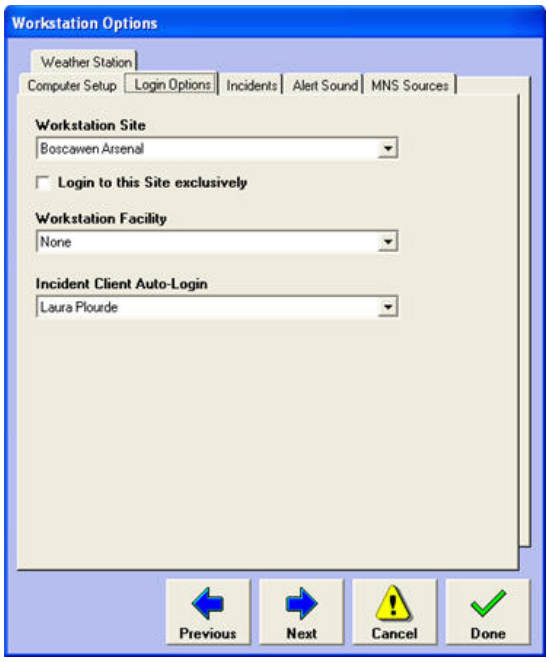
- **Workstation Name** Displays the computer name. Do not alter this value unless instructed to do so by a Monaco representative.
- **Backup Path** The location on the workstation where the D-21 backs up the D-21 database. Do not modify this path unless instructed to do so by a Monaco representative.
- **Startup Monitor** Select the monitor on which you want to start up and display the D-21 Incident Client. Select **1** if you want the application on the first monitor. Select **2** if you want the application on the second monitor. This option is only available if the workstation has been configured in Windows 2000/XP for dual monitors.

- **Secondary Monitor** Select the monitor on which you want to display the Incident Client map and graphics viewers. This option is only available if the workstation has been configured in Windows 2000/XP for dual monitors.
- **Default Map View** Select the map view that should be displayed when an operator logs in or re-logs in to the D-21 Incident Client from this drop-down list.
- **Incident Auto-Display Viewer** Select the viewer that you want to launch automatically on the second monitor when an incident is created in the D-21 Incident Client. This option is only available if the workstation has been configured in Windows 2000/XP for dual monitors.
- **Media Directory** The location on the workstation where the D-21 looks for all media files such as the map, floor plans, response graphics, icons, etc. Do not modify this path unless instructed to do so by a Monaco representative.
- **Firehouse Software installed** Select **Yes** if you are using Firehouse Software to export data from the D-21 to Firehouse Software. For more information on exporting to Firehouse, see the D-21 Maintenance Guide (P/N 001-399-02).
- **iButton Hub** Select the iButton hub you want this workstation to use for managing IDS iButtons and PINs. The iButton hubs displayed in this list were added to the database with the iButton Hub RID. See "IDS iButton and PIN Assignments" on page 9-24 for more information.

2. Make changes as necessary.
3. When you are finished, click **Done**.

To configure workstation login options

1 Select **Options > Workstation Options**. Click **Next** to advance to the Login Options tab.



- **Workstation Site** Select the site that workstation logs into by default.
- **Login to this Site exclusively** Select this option to limit operator logins at this workstation to the selected site only.
- **Workstation Facility** Select the facility in which this workstation is located. This value is required in order for this workstation to view automatic shortest routes. See "Configuring Shortest Routes" on page 4-33.
- **Incident Client Auto-Login** Select an operator name to automatically log in to the Incident Client each time the Incident Client is started at this workstation. Select None if you want to require an operator and password each time the Incident Client is started on this workstation.

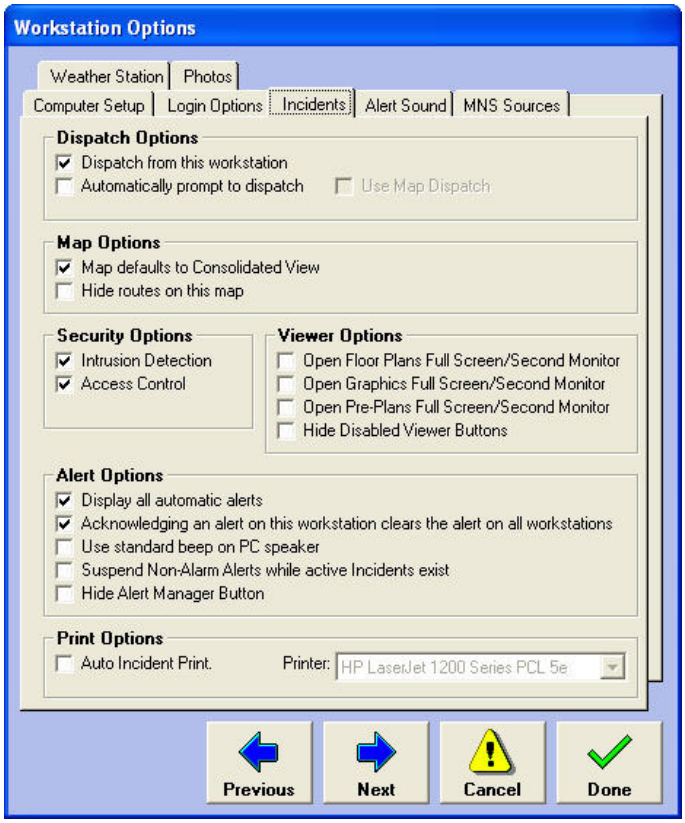
NOTE *When this option is selected, the D-21 Incident Client does not require a password for login.*

2 Make changes as necessary.

3 When you are finished, click **Done**.

To configure workstation incident processing options

1 Select **Options > Workstation Options**. Click the Incidents tab.



Dispatch Options

- **Dispatch from this workstation** Select this option to turn on the Dispatch viewer for all incidents at this workstation.
- **Automatically prompt to dispatch** Select this option to display the resource dispatch dialog box after an operator creates an incident at this workstation.
- **Use Map Dispatch** If you have enabled the automatic prompt to dispatch, select this option to use the Map-based dispatch when the automatic prompt is generated.

NOTE *See "Dispatch Configuration" on page 3-58 for more information about dispatch options.*

Map Options

- **Map defaults to Consolidated View** Select this option to use the Consolidated view on an incident's map. This view displays resources of any class (i.e. Fire or Security), and does not display facility icons for most facilities. See the D-21 Incident Client User Guide (P/N 001-392-00) or the D-21 Map Options User Guide (P/N 001-464-00) for more information about map views.
- **Hide routes on this map** Select this option if you do not want to see automatic shortest routes for all incidents at this workstation. For more information on shortest routes, see "Configuring Shortest Routes" on page 4-33.

Security Options

- **Intrusion Detection** Select this option to display Intrusion Detection alerts on this workstation.
- **Access Control** Select this option to display Access Control alerts on this workstation.
- **Law Enforcement** Select this option to record Law Enforcement information at this workstation.

Viewer Options

- **Open Floor Plans Full Screen/Second Monitor** Select this option if you want an incident's Floor Plan viewer to open full screen (for single-monitor workstations) or on the second monitor (for dual-monitor workstations), when it is selected, rather than within the Incident frame.
- **Open Graphics Full Screen/Second Monitor** Select this option if you want an incident's Graphics viewer to open full screen (for single-monitor workstations) or on the second monitor (for dual-monitor workstations), when it is selected, rather than within the Incident frame.
- **Open Pre-Plans Full Screen/Second Monitor** Select this option if you want an incident's Pre-Plan viewer to open full screen (for single-monitor workstations) or on the second monitor (for dual-monitor workstations), when it is selected, rather than within the Incident frame.
- **Hide Disabled Viewer Buttons** Select this option if you do not wish to display viewer buttons within the Incident frame when the viewers are not available for a particular incident (for example, when the Floor Plan button is disabled because no floor plan is available for the incident's facility).

Alert Options

- **Display All Automatic Alerts** De-select this option if you do not want to receive alerts at this workstation.

- **Acknowledging an alert on this workstation clears the alert on all workstations** Select this option to clear an alert on all workstations when it is acknowledged at this workstation.

NOTE *You must use the alert's Acknowledge button to clear the alert if you wish to clear it on all workstations. Using the Trouble, Nuisance, or Create Incident buttons will clear it only on the local workstation.*

- **Use Standard beep on PC speaker** Select this option if you are receiving alerts on this workstation and want each alert to be accompanied by a beep from the computer's internal speaker. If the D-21 Incident Client is configured to Auto Acknowledge trouble or normal alerts, no audible alert is sounded. If you are not receiving automatic alerts, this setting has no effect.
- **Suspend Non-Alarm Alerts while active Incidents exist** Select this option if you do not want non-alarm alerts (e.g. Trouble and Supervisory alerts) to be displayed on this workstation while an incident is open. When all incidents have been closed, then any pending non-alarm alerts will be displayed.
- **Hide Alert Manager button** Select this option if you do not want the Alert Manager button to appear in the alert pop-up window when a zone alarm is received. This option prevents the operator at this workstation from skipping a potentially serious alert by stacking it in the Alert Manager. See "To configure the Alert Manager" on page 3-50 for more information about the Alert Manager.

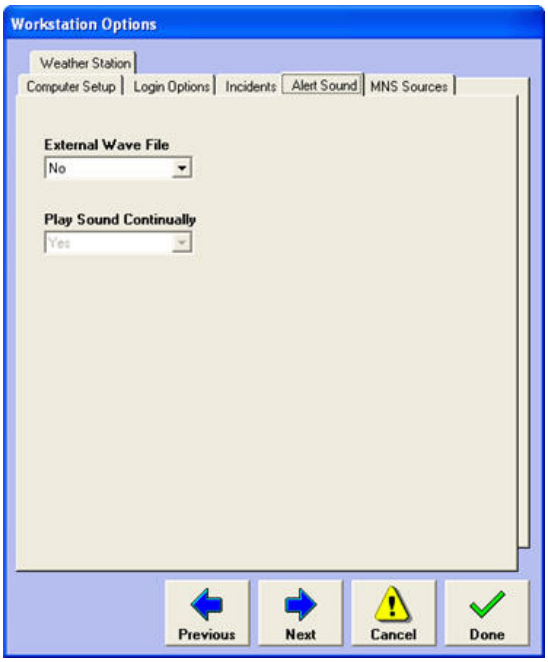
Print Options

- **Auto Incident Print** Select this option if you want a summary sheet to automatically print when an incident is created at this workstation.
- **Printer** Select the printer for the automatic incident summary sheet.

2. Make changes as necessary.
3. When you are finished, click **Done**.

To configure workstation alert sounds options

1 Select **Options > Workstation Options**. Click the Alert Sounds tab.



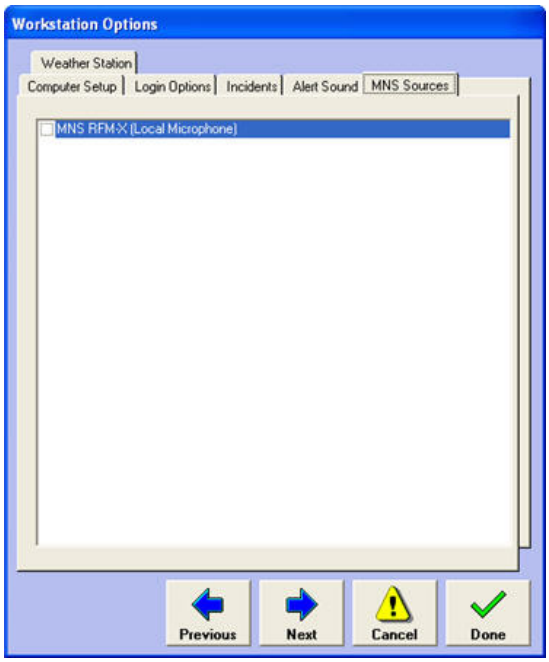
- **External Wave File** Select Yes from the drop-down list if you want to use a custom sound for the audible alert that accompanies alarm and trouble conditions.
- **Play Sound Continually** Select Yes from the drop-down list if you want the alert sound to play continuously.

2 Make changes as necessary.

3 When you are finished, click **Done**.

To configure workstation MNS live voice sources

1 Select **Options > Workstation Options**. Click the MNS Sources tab.



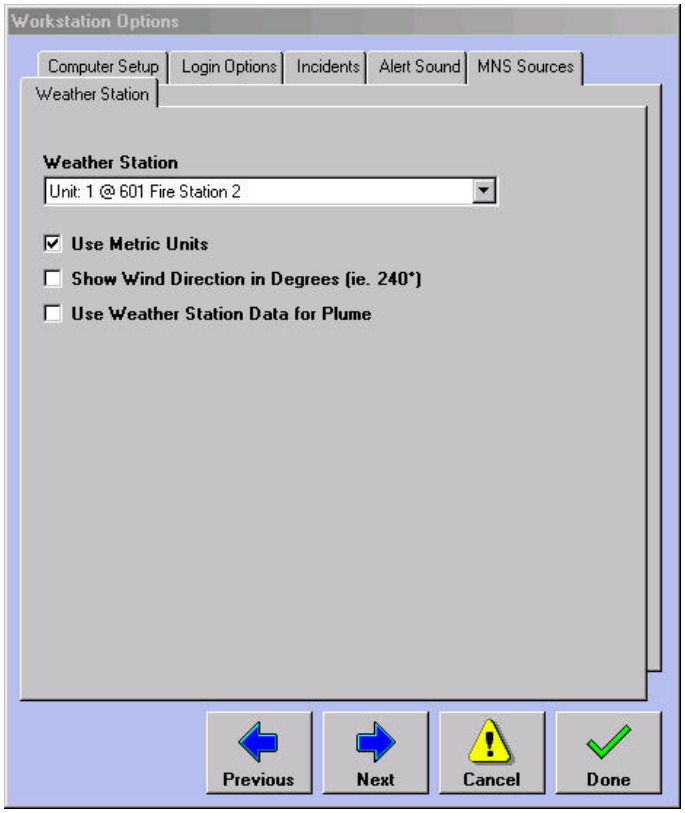
2 Select the MNS Sources available at this workstation by checking the appropriate check boxes.

NOTE *For information on configuring MNS sources for this workstation, see "Configuring Workstations for Multiple Live-Voice Sources" on page 7-16.*

3 Click **Done**.

To configure workstation weather station options

1 Select **Options > Workstation Options**. Click the Weather Station tab.



2 Select the weather station device from the **Weather Station** drop-down list.

NOTE *For information on adding a weather station RID and device, see the D-21 Remote Interface Driver Guide (P/N 001-399-01).*

3 Click in the check boxes as necessary to set display options for the Weather Data viewer in the D-21 Incident Client.

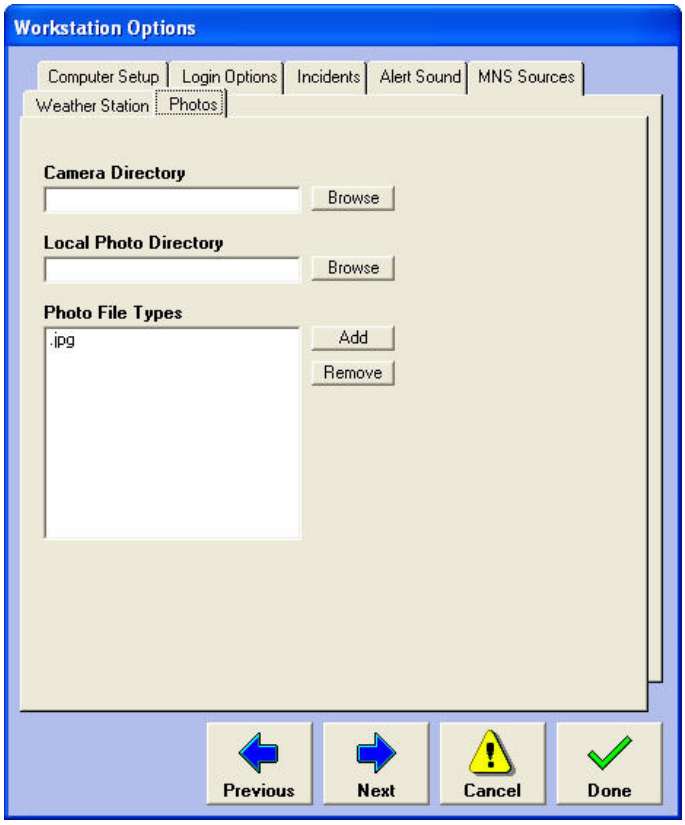
- **Use Metric Units** Display temperature in degrees Celsius, wind speed in meters per second, and barometric pressure in mb Hg (millibars of Mercury).
- **Show Wind Direction in Degrees** Display wind direction in degrees (0° - 360°) as opposed to compass directions. When this option is selected, an easterly wind direction is displayed as 90°.
- **Use Weather Station Data for Plume** When a hazmat plume has been created, this option allows its weather variables to be populated from the weather station data. This option is only available if the HazMat Plume component has been added to the D-21.

4 When you are finished, click **Done**.

To configure workstation photo options

If a digital camera will be attached to this D-21 workstation so photos can be uploaded, the required directory paths must be configured.

1 Select **Options > Workstation Options**. Click the Photos tab.



2 In the **Camera Directory** text box, enter the path to the photo storage area on the digital camera. If the camera is currently attached to the workstation, click the **Browse** button to navigate to and select the directory using a standard Windows file management dialog box instead of manually typing the path in the text box.

3 In the **Local Photo Directory** text box, enter the path to the folder on the local hard drive where uploaded photos will be kept. Use the **Browse** button to navigate to and select the directory using a standard Windows file management dialog box instead of manually typing the path in the text box.

4 Confirm the file type used by the digital camera for photos appears in the **Photo File Types** list box. If it does not, click the **Add** button to enter it in the list. To remove a file type, select it in the list and click the **Remove** button.

5 When you are finished, click **Done**.

Section 5
Adding Media Files

Read this section to learn how to add floor plans, icons, response graphics, and sound files to the Media folder.

Contents

Media Files 5-2
Programs for Generating Media Files 5-2
Floor Plans, Pre-Plans, and Response Graphics 5-3
    Conventions for Naming Media Files 5-4
    Importing Floor Plans, Response Graphics, and Pre-Plans 5-5
Icons 5-12
Sounds 5-12

Media Files

The Media folder is located at `C:\Program Files\D21\Media`, and contains graphics and audio files for use with the D-21. Since each D-21 workstation uses the media files in its own `\D21\Media` folder, it is important to periodically back up the contents of `\D21\Media` in case it is necessary to restore some or all of the media files. See the D-21 Maintenance Guide (P/N 001-399-02) for more information on backing up and restoring media files.

You can add image files to the following folders:

- `\FloorPlans`.
- `\PrePlans`.
- `\Icons`.
- `\ResponseGraphics`.
- `\Vehicles`.

You can add .wav sound files to the `\Sounds` folder.

NOTE *To add a map, contact Monaco. See Contact Information on page ii.*

Programs for Generating Media Files

Monaco provides Autodesk® AutoCAD LT® with the D-21G and D-21M for creating and editing floor plans and other graphics; for information on using AutoCAD LT, see the Autodesk documentation included with the product.

There are dozens of programs capable of generating media files in formats that can be used with the D-21.

IMPORTANT *Monaco neither endorses nor recommends programs for generating image graphics or sound files.*

Floor Plans, Pre-Plans, and Response Graphics

You can add graphics in the following formats to the FloorPlans, PrePlans, and Response Graphics folders when using the D-21G and D-21M:

IMPORTANT *If you are already using Monaco pre-plan templates to add pre-plans to your response plans, you cannot import pre-plans from another software application. See* *"Pre-Plans" on page 3-23* *for more information.*

File Format	File Name Extension	Programs that Make Files in this Format
Bitmap	.bmp	Paint programs such as Microsoft Paint and image editing programs such as Adobe® Photoshop®
CAD Zone Drawing	.czd	The Fire Zone by The CAD Zone
Drawing Web Format	.dwf	Autodesk AutoCAD LT (included with D-21G and D-21M)
Data Exchange File	.dxf	Autodesk AutoCAD LT (included with D-21G and D-21M)
Drawing	.dwg	Autodesk AutoCAD LT (included with D-21G and D-21M)
Graphic Interchange Format	.gif	Image editing programs such as Adobe Photoshop
JPEG (Joint Photographic Experts Group)	.jpg	Image editing programs such as Adobe Photoshop
Adobe Portable Document File	.pdf	Adobe Acrobat
Tagged Image File Format	.tiff	Image editing programs such as Adobe Photoshop
Windows Meta File	.wmf	Image editing programs such as Adobe Photoshop

To make a floor plan graphic available to the D-21 system

1 Save or copy the file to:
`C:\Program Files\D21\Media\FloorPlans`.

NOTE *Files in the *.pdf format cannot be used for D-21 floor plans.*

To make a response plan graphic available to the D-21 system

1 Save or copy the file to:
`C:\Program Files\D21\Media\ResponseGraphics`.

To make a pre-plan file available to the D-21 system

1 Save or copy the file to:
`C:\Program Files\D21\Media\PrePlans`.

NOTE *Files in the *.bmp, *.gif, *.jpg, *.tif, and *.wmf formats cannot be used for D-21 pre-plans.*

Conventions for Naming Media Files

Use the Import command to import large numbers of files and attach them to existing facilities by following the naming conventions described below.

IMPORTANT *The File > Import Pre-Plans command is not available if your database is set up to use Monaco pre-plan templates.*

- File names must start with the full facility number, including any prefix and suffix, exactly as entered in the D-21 database. Use an underscore (_) to separate the facility number from the rest of the file name. The import utility compares the characters that precede the underscore with facility numbers entered in the D-21 to match the file with a D-21 facility. The import utility also creates a label for the file within the D-21 that includes the facility name as entered in the D-21 database. If the image is a floor plan, the import utility includes that information in the label as well.
- The last characters before the period that separates the file name from the file extension must indicate the image type (floor plan, response graphic, or pre-plan) according to the following format:

Floor Plans	`FacilityNumber_fp.*` For example, `A-132_fp.dwg` is an AutoCAD floor plan for facility number A-132.
Response Graphics	`FacilityNumber_pic.*` For example, `8-Z-5_pic.jpg` is a photograph of facility number 8-Z-5.
Pre-Plans	`FacilityNumber_pp.*` For example, `12_pp.pdf` is a .PDF pre-plan for facility number 12.

- Include additional descriptive information about the file after the underscore, if necessary. The text will be included in the label for the file that is generated by the import utility. This is useful if there are multiple images to import for a single facility. For readability, you can include a space between the additional text and the final characters indicating the image type if you wish.

File Name	Label Attached by the D-21
132-A_fp.dwg	132-A FacilityName Floor Plan
132-A_1st Floor fp.dwg	132-A 1st Floor FacilityName Floor Plan
132-A_2nd Floor fp.dwg	132-A 2nd Floor FacilityName Floor Plan
45_pic.jpg	45 FacilityName
45_Electrical Panel pic.jpg	45 Electrical Panel FacilityName
190B_pp.pdf	190B FacilityName

NOTE *File names are not case-sensitive.*

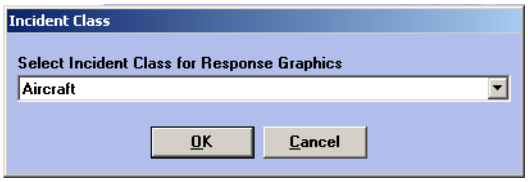
Importing Floor Plans, Response Graphics, and Pre-Plans

Use **File > Import** to import large numbers of response graphics, floor plans, and pre-plans. The Import command uses the file naming conventions described in "Conventions for Naming Media Files" on page 5-4 to import each graphic, floor plan, or pre-plan and attach it to the correct facility. Files must be located in the correct folder in the D-21 directory to import successfully. Floor plans must be in `C:\Program Files\D21\Media\FloorPlan`. Response graphics must be in `C:\Program Files\D21\Media\ResponseGraphics`. Pre-plans must be in `C:\Program Files\D21\Media\PrePlans`. For more information, see "Floor Plans, Pre-Plans, and Response Graphics" on page 5-3.

To import response graphics

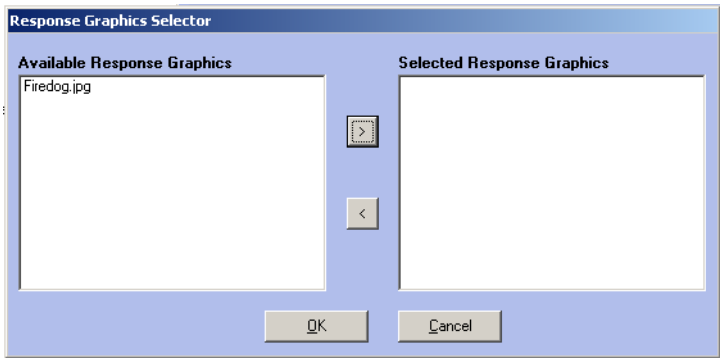
NOTE *Follow the file naming conventions for importing response graphics before using the Import command. See "Conventions for Naming Media Files" on page 5-4.*

1. Select **File > Import**.
2. Click **Import Response Graphics**. The following dialog box appears.



3. Select the Incident class being attached to the Response Graphic from the drop-down list.

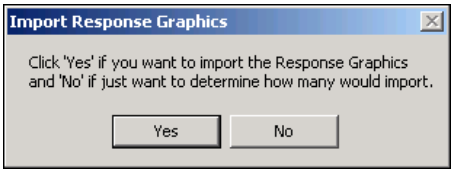
4 Click **OK**, and the Response Graphics Selector appears



5 Use the arrow buttons to move graphics between the Available and the Selected windows. Use the Shift or Ctrl keys to select multiple files. Graphics in the Selected window will be available for use by the D-21.

6 Click **OK.**

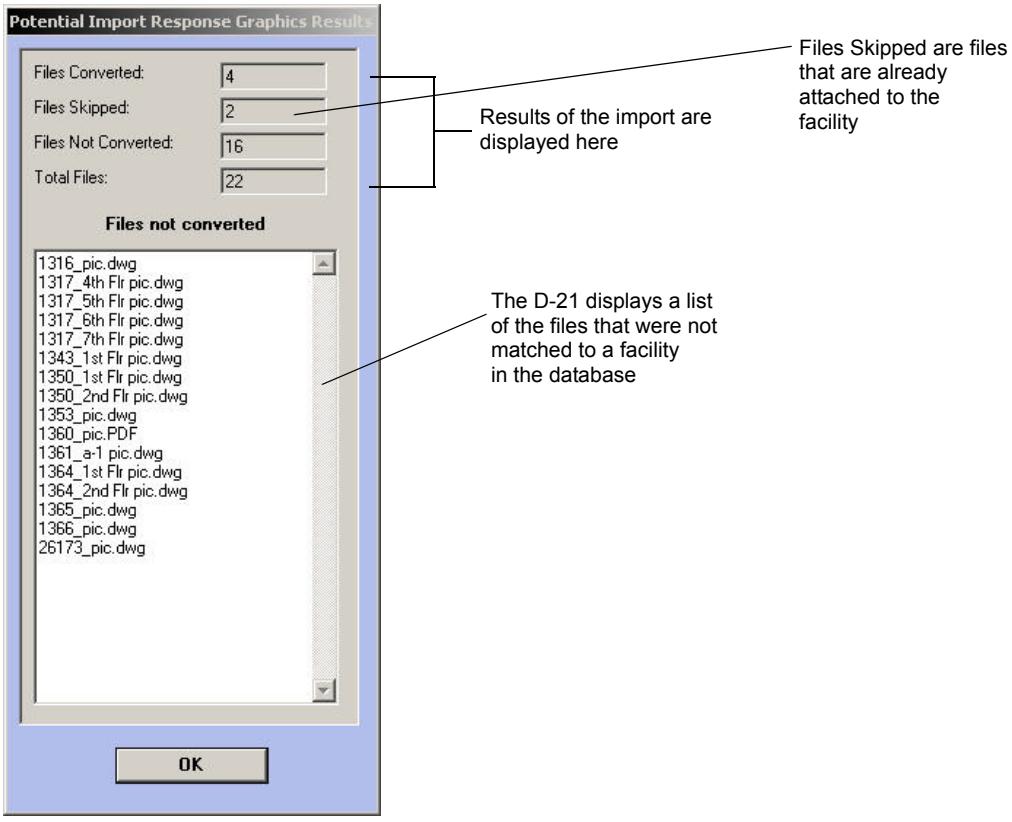
7 The following dialog box appears. Select **Yes** or **No**.



- Click **Yes** to import the response graphics. The D-21 imports the graphics and displays a dialog box with the actual results of the import.

OR

- Click **No** to view the potential results of using the Import command. The same dialog box is displayed without performing the import.



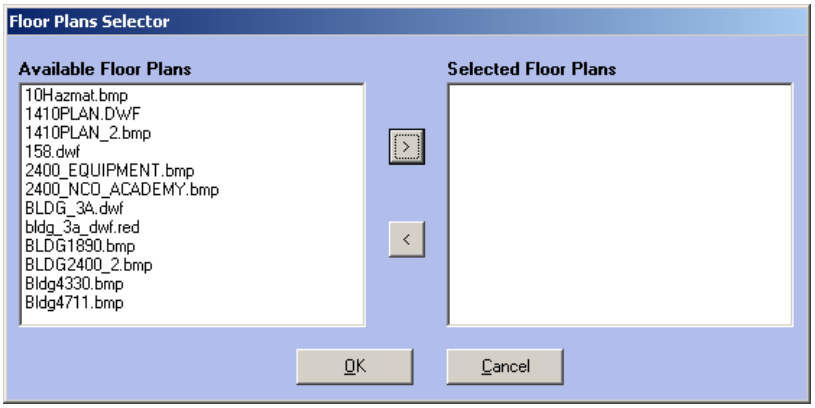
8 Click **OK**. Files that were not converted with the Import command can be manually added to response plans. See "To add graphics to a response plan" on page 3-12.

To import floor plans

NOTE *Follow the file naming conventions for floor plans before using the Import command. See "Conventions for Naming Media Files" on page 5-4.*

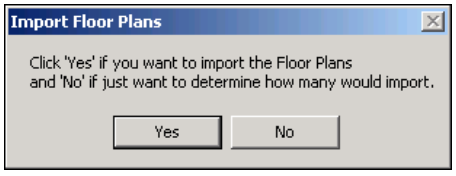
1 Select **File > Import**.

2 Click **Import Floor Plans**. The following dialog box appears.



3 Select files from the Available Floor Plans Section. Use the Shift or Ctrl keys to select multiple files. Click the right-hand arrow (**>**) to move them to the Selected Floor Plans section.

4 Click OK. The following dialog box will appear.

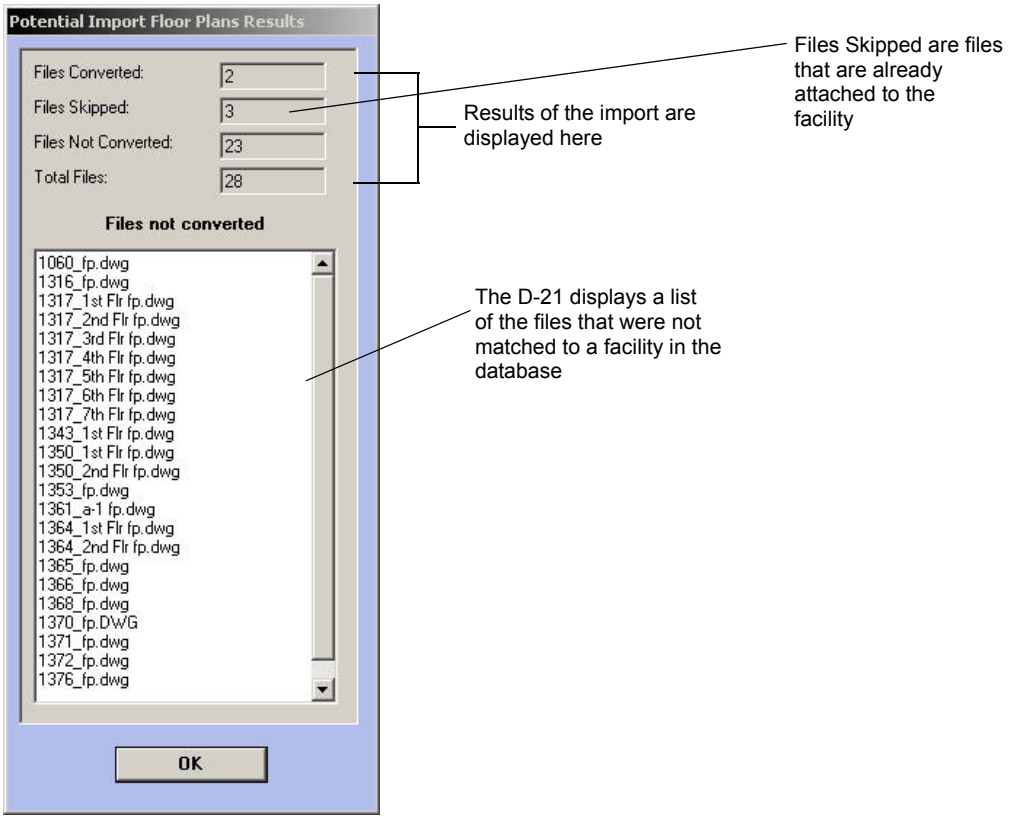


5 Do one of the following:

- Click **Yes** to import the floor plans. The D-21 imports the floor plans and displays a dialog box with the results of the import.

OR

- Click **No** to view the potential results of using the Import command. The same dialog box is displayed without performing the import.

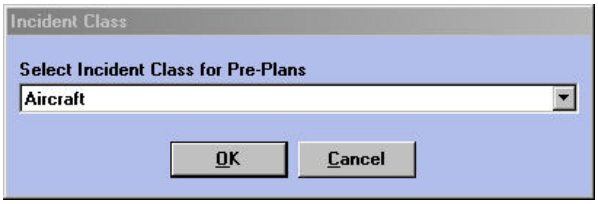


6 Click **OK**. Files that were not converted with the Import command can be manually attached to facilities. See "To add a floor plan to a facility" on page 2-27.

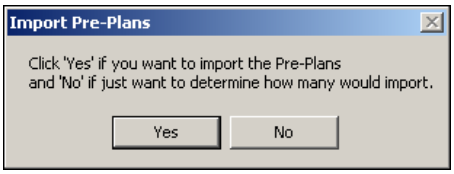
To import pre-plans

NOTE *You cannot import pre-plan files if you are already using Monaco pre-plan templates to create response plan pre-plans. In this case, the Import > Import Pre-Plans command will not be available.*

1. Select **File > Import**.
2. Click **Import Pre-Plans**. The following dialog box appears.



3. Select the Incident class being attached to the Pre-Plan from the drop-down list.
4. Click **OK**, and the Pre-Plans Selector appears. Select files from the Available Pre-Plans Section. Use the Shift or Ctrl keys to select multiple files. Click the right-hand arrow (**>**) to move them to the Selected Pre-Plans section.
5. Click **OK**. The following dialog box will appear.

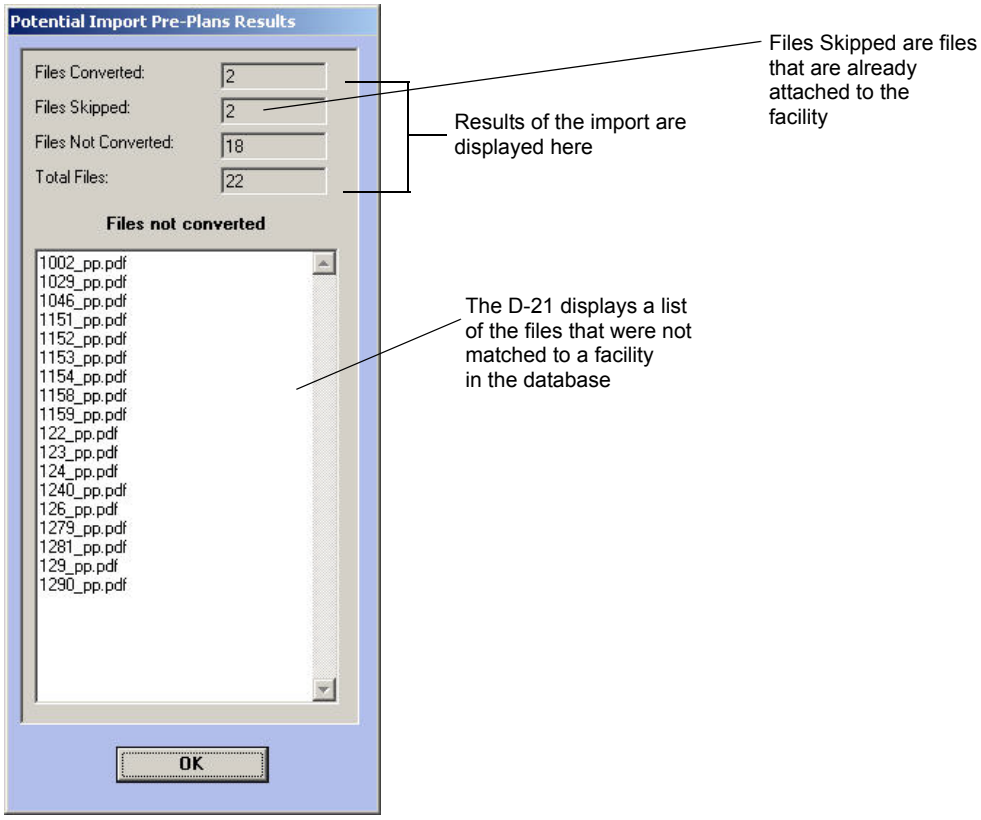


6 Do one of the following:

- Click **Yes** to import the pre-plans. The D-21 imports the pre-plan files and displays a dialog box with the results of the import.

  OR

- Click **No** to view the import results without actually attaching any pre-plans to response plans.



7 Click **OK**. Files that were not converted with the Import command can be manually attached to response plans. See "To add a pre-plan file to a response plan" on page 3-7.

Icons

You can add icons in the following formats to the Icons folder:

File Format	File Name Extension	Programs that Make Files in this Format
Bitmap	.bmp	Paint programs such as Microsoft® Paint and image editing programs such as Adobe® Photoshop®
Graphic Interchange Format	.gif	Image editing programs such as Adobe® Photoshop®
Icon	.ico	Any Windows icon editor program

To make an icon available to the D-21 system

1 Save or copy the file to:
`C:\Program Files\D21\Media\Icons`.

Sounds

You can add Windows wave files with the `.wav` filename extension to the Sounds folder. You can generate wave files from an audio editing application such as Goldwave Digital Audio Editor or Syntrillium Software Cool Edit.

To make a wave file available to the D-21 system

1 Save or copy the file to:
`C:\Program Files\D21\Media\Sounds`.

Section 6
Adding the BT-X Communicator

Read this section to learn how to add a multi-application BT-X to the D-21 database.

Contents

Adding the Multi-Application BT-X 6-2
Adding the BT-X Communicator 6-3
Adding the BT-X Communicator Plus 6-4
Configuring Dual Communication Channels. 6-4
Dual Communication Status 6-5
Dual Communication Testing 6-5

Adding the Multi-Application BT-X

Multi-application BT-X units (BT-X Communicator, BT-X Communicator Plus, BT-XF, BT-XS, BT-XS(M), BT-X/ACS(M), and BT-X/WAC+) can be configured with one or more different applications. An *application* is a combination of hardware and software that creates a specialized functionality in the D-21. Fire, intrusion detection, access control, and mass notification are all applications that can be configured when using the BT-X. One or more applications can be installed in the BT-X and configured for the unit at the D-21 depending on how the BT-X is configured by Monaco for your use.

IMPORTANT *When you finish programming the BT-X, print the List Configuration report to provide a list of remote units and zones that need to be added to the D-21 database.*

To add a multi-application BT-X to the D-21 database

1. Print the List Configuration report from the BT-X programming menu for the unit you are configuring. You will need to add each unit configured during the BT-X programming to the D-21 database.
2. Add a BT-X Communicator remote unit. Do one of the following:
   - **If the BT-X has MNS functionality installed** Add a BT-X Communicator unit using "To add a BT-X for in-building mass notification" on page 7-19.

   OR

   - **If the BT-X does not have MNS functionality** Add a BT-X Communicator unit using "To add the BT-X Communicator unit" on page 6-6.

   Add the onboard zones, if used, to the BT-X Communicator. See "To add a zone" on page 2-65.

   Add the relay outputs to the BT-X Communicator if the unit uses onboard relay drivers for activating relays from the D-21. See "To add an output" on page 2-74.
3. **If AIM reader interface modules are installed for ACS** Add the number of ACS application units indicated by the BT-X configuration report. Use the BT-X/ACS (M) remote unit type and assign the unit numbers calculated by the BT-X. "To add a BT-X/ACS (M) application unit" on page 8-12.
4. **If fire zone cards are installed for Fire reporting** Add the number of Fire application units indicated by the BT-X configuration report. Use the BT-XF (M) remote unit type and assign the unit numbers calculated by the BT-X. See "To add a remote unit" on page 2-55.
5. **If security zone cards are installed for IDS** Add an IDS Master unit and the number of IDS application units indicated by the BT-X configuration report. Use the BT-XS(M) remote unit type for the IDS Master unit and the IDS application units, and assign the unit numbers calculated by the BT-X. "To add an IDS application unit" on page 9-21.

Adding the BT-X Communicator

Each BT-X is represented in the D-21 database by the BT-X Communicator remote unit type and application-specific remote units that represent fire, mass notification, intrusion detection, and access control equipment. The BT-X Communicator unit is used to report BT-X operational conditions such as ac fail, battery fault, and enclosure tamper (if used).

The BT-X Communicator also supervises:

- **Mass Notification** If the BT-X is connected to a mass notification panel for pre-recorded and/or live-voice messages, the BT-X Communicator unit is used to configure MNS for the BT-X. See "Adding a BT-X with Mass Notification" on page 7-18.
- **Onboard zones** There are four onboard zones available on each BT-X Communicator unit that can be used for fire or auxiliary zone reporting. See "To add a zone" on page 2-65 after you have added the BT-X Communicator unit for more information on adding zones.
- **Relays** If the BT-X Relay Board is installed, the board's relays are configured in the D-21 as outputs attached to the BT-X Communicator remote unit. See "To add an output" on page 2-74 after you have added the BT-X Communicator unit for more information on configuring the relays. If the BT-X is used for mass notification, the BT-X relays drivers are used for activating and deactivating pre-recorded messages and cannot be used for output relays.
- **Dual communication channels** When the BT-X is configured for primary and secondary communication modes, either the BT-X Communicator or the IDS Master unit report an alarm on zone position 13 when the primary communication mode fails or the unit is manually switched to secondary communication mode. When the primary communication mode is restored, an end alarm condition is reported on zone 13. You must add zone 13 to each unit reporting communication status, in order for the D-21 to display status changes for the zone.

NOTE *Each dual communication BT-X with an IDS Master unit can be configured through BT-X programming in order to report the communication status on either the BT-X Communicator address or the IDS Master unit address. See the BT-X I-O-M Manual (P/N 001-398-00) for more information.*

- **Zone card failures** The BT-X Communicator reports a failure of one of the installed fire zone cards on zone position 14. The zone must be added to the Communicator unit in order for the D-21 to display status changes for this zone. The IDS Master unit reports a security zone card failure on its zone position 14.
- **Bad database** When the D-21 downloads to the BT-X and the configurations do not match, this condition is reported on zone position 16. This zone must be added to the Communicator unit in order for the D-21 to display the status change.

NOTE *Zone position 15 is not used on the BT-X Communicator unit.*

Each application (one or more fire cards, security cards, access control reader interface, etc.) is treated as an additional remote unit in the D-21 database. Each is numbered sequentially beginning with the unit number used for the Communicator. All unit numbers are determined

when the BT-X is programmed, and the programmed unit numbers should be entered into the D-21 so they match the programming at the BT-X. See the BT-X Installation Manual (P/N 001-398-00) provided with the BT-X for more information on programming the hardware and printing a List Configuration report (used when configuring the BT-X in the D-21).

Adding the BT-X Communicator Plus

The BT-X Communicator Plus is a firmware upgrade of the BT-X Communicator. Each BT-X Communicator Plus has the same basic functions of the BT-X Communicator, but has the following enhanced capabilities:

- Display of BT-X version information and Zone Card evaluation results.
- Global MNS activation or inactivation messages.
- Better control of keypad errors due to malfunctions.
- Selection of local or remote iButton bridge chips.
- Synchronizing of BT-X MNS pre-recorded messages.

For more information about the specifics of the BT-X Communicator Plus see the BT-X Communicator Plus Supplement (P/N 001-398-09).

BT-X Communicator Unit Classes

The BT-X Communicator and Communicator Plus units can be classified as Fire, Security, or Facility Management. Unit class is used to differentiate transceivers in the D-21 Incident Client, and allows the operator to efficiently communicate with different groups of units based on class. For instance, an operator can view unit status conditions and send commands to a fire BT-X Communicator on D-21 client workstations where the Fire Client is enabled.

The BT-X programming menus and the D-21 unit configuration must be set up so BT-X unit status is reported to the desired Client workstations. See the BT-X Basic IOM Manual (P/N 001-398-08) for more information on programming unit status reporting options on the BT-X.

Configuring Dual Communication Channels

Dual communication is enabled in the RFM 7000 RID configuration and in the BT-X remote unit configuration.

The dual communication option must be enabled in the RFM 7000 RID configuration dialog box for the RFM to communicate with one or more dual communication BT-X units. See "Dual Communication Testing" on page 6-5 for more information.

IMPORTANT *A dual communication BT-X communicates with the D-21 via the RFM-XHR. The RFM-XHR uses the RFM 7000 RID. See "Adding a RID for the RFM 7000 and RFM-X" on page 2-38.*

When dual communication is enabled, the RFM 7000 RID provides commands to:

- Switch from the primary to secondary channel.
- Switch from the secondary to the primary channel.
- Disable and enable either channel.
- Test the primary with fallback to secondary communication mode.

Each dual communication BT-X is programmed to report its status on either its BT-X Communicator address or IDS Master unit address (if intrusion detection equipment is installed). When these units are added to the D-21 database, the units programmed to report dual communication status to the D-21 must have the dual communication channel option enabled in their remote unit configuration.

The BT-X Communicator and IDS Master remote unit types each use a communication supervision zone (zone 13) to signal the fallback from primary to secondary communication and the subsequent return to primary communication. Zone 13 must be added to the remote unit configuration for units that will report dual communication channel status. See "To add the BT-X Communicator unit" on page 6-6 for how to configure the fallback zone (zone 13) on the BT-X Communicator unit. See "To add an IDS application unit" on page 9-21 for more information on configuring the IDS Master unit.

Dual Communication Status

Dual communication channel status is reported on zone 13. The Alarm and Normal/Secure status conditions reported on zone 13 of either the BT-X Communicator or the IDS Master unit indicate the following:

- **Alarm** The BT-X is in a fallback mode from the primary to secondary communication channel and is currently operating on its secondary channel.
- **Normal/Secure** The primary channel has been restored and the BT-X is operating on the primary communication channel. Zone 13 on the BT-X Communicator is Normal when the unit is on the primary channel. Zone 13 on the IDS Master unit status is Secure when the unit is on the primary channel.

When you enable dual communication channels on a BT-X Communicator or IDS Master unit, the D-21 gives you the option of automatically adding zone 13 to the remote unit configuration. The zone priority for zone 13 defaults to Supervisory. You can change this priority setting by editing the zone.

IMPORTANT *The zone priority is set to Supervisory so alarms from the unit do not appear on the system as higher priority Fire or Security Alarms.*

Dual Communication Testing

The Dual Communication Test tests the fallback to secondary channel and restore to primary channel operation of each dual comm BT-X unit that communicates with the RFM 7000 RID. The D-21 tests each dual communication unit by polling it, switching it to the secondary

channel, and then restoring it to the primary channel. If the unit fails the test at any point during the process, the testing stops, the reason is displayed in the Remote Activity window in RID Commands in the D-21 Incident Client, and the Dual Communication Test proceeds to the next dual communication unit.

IMPORTANT *Set the RFM 7000 RID polling mode to Continuous or Continuous/Timed when using the Dual Communication Test. See "Adding a RID for the RFM 7000 and RFM-X" on page 2-38.*

The Dual Communication Test fails to run if:

- The RFM is in communication failure.
- The RFM is currently operating in single-channel mode.
- There are no units attached to the RFM with dual communication enabled.

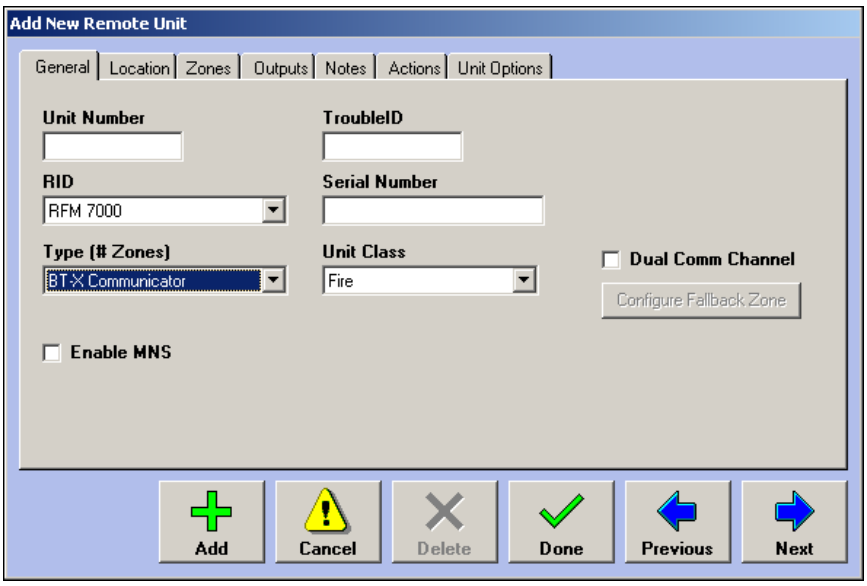
The Dual Communication Test skips a dual communication unit if:

- The dual communication unit is in a No Reply condition with the RFM.
- The dual communication unit is already operating on its secondary channel. Only units operating on their primary channel can be tested.

The Dual Communication Test can be set up to run automatically (at regular intervals) when you configure the RFM 7000 RID, or you can run the Dual Communication Test from the RID Commands window in the D-21 Incident Client. If you schedule the Dual Communication Test to run automatically, be sure to pick a test time that does not overlap other scheduled system activities, such as extended polls and automatic database backups. See "Adding a RID for the RFM 7000 and RFM-X" on page 2-38.

To add the BT-X Communicator unit

1 Select **Add > Remote Unit**.



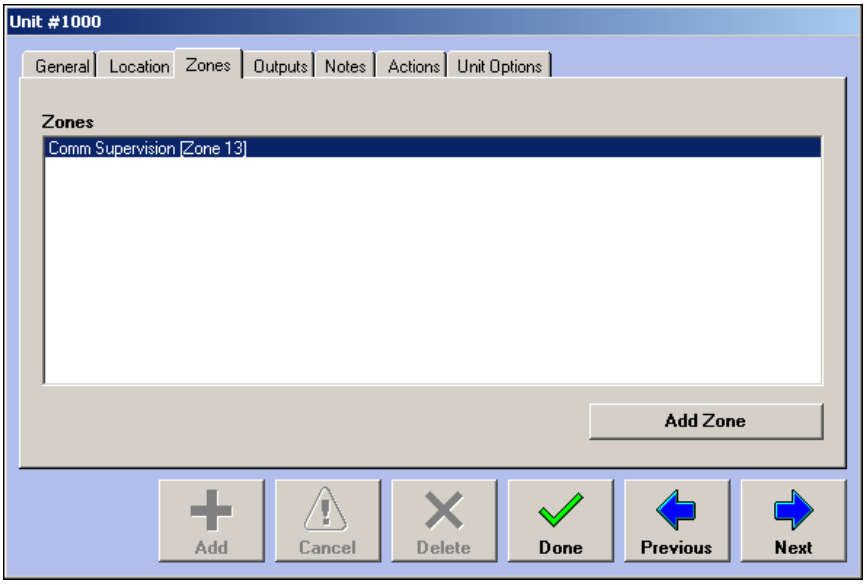
- **Unit Number** Enter the BT-X Communicator address.
- **RID** Select the RID that will be used to communicate with the BT-X.
- **Type (# Zones)** Select the BT-X Communicator remote unit type.
- **Trouble ID** For Monaco use only.
- **Serial Number** Enter the serial number for the remote unit hardware. This field is for informational purposes only and is not required.
- **Unit Class** Select Fire, Security, or Facility Management to specify which workstations and users can issue commands to this unit.
- **Enable MNS** Select this option if the BT-X is used for pre-recorded and/or live-voice mass notification. Checking this option enables MNS for the remote unit and adds the MNS tab to the dialog box. See "Configuring Mass Notification" on page 7-1 for more information.
- **Dual Comm Channel** Select this option if the BT-X is configured to communicate dual comm channel status with the D-21 on the BT-X Communicator address. See "Configuring Dual Communication Channels" on page 6-4 for more information.
- **Configure Fallback Zone** This option is only available if the Dual Comm Channel option is selected. The Configure Fallback Zone option automatically adds zone position 13 to the BT-X Communicator unit with the description: Comm Supervision.

2 Click **Next** to advance to the Location tab.

3 Select the site and facility where the remote unit is located from the drop-down lists. If desired, enter more specific information in the Location/Directions box.

NOTE *If the desired facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See "To add a facility" on page 2-13.*

4 Click **Next** to advance to the Zones tab. If you selected the Dual Comm Channel option and clicked **Configure Fallback Zone**, zone 13 is already added to the unit.



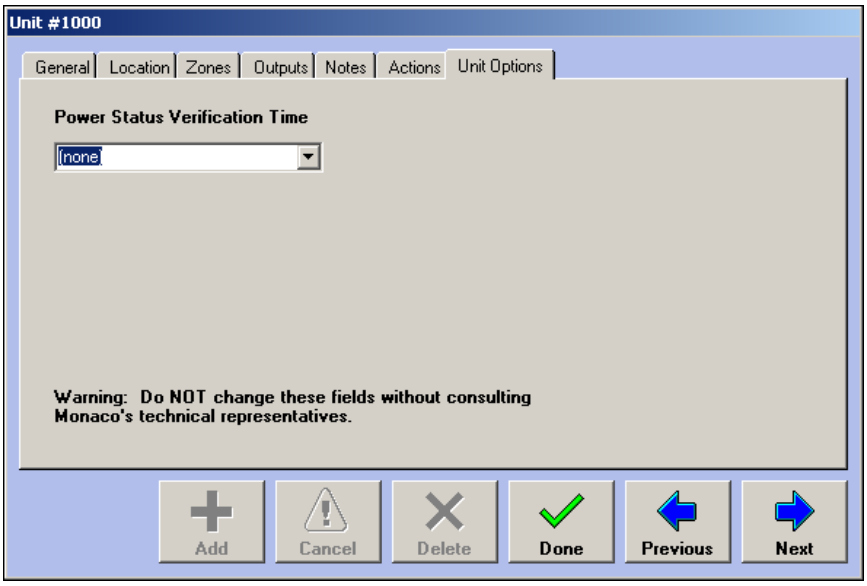
5 Click **Add Zone** to add the four onboard zones (Zones 1–4) and to add the BT-X status zones (Zones 14 and 16), if necessary. See "To add a zone" on page 2-65 for information on adding a zone. See "Adding the Multi-Application BT-X" on page 6-2 for more information on the zones available on the BT-X Communicator unit.

6 Click **Next** to advance to the Outputs tab when you are finished adding zones. Click **Add Output** to add the BT-X Communicator onboard relays, if used. See "To add an output" on page 2-74.

7 Click **Next** to advance to the Notes tab when you are finished adding outputs. Enter any descriptive information you would like saved with the unit record.

8 Click **Next** to advance to the Actions tab. Click **Add Action** to add an action to this unit when the unit status changes. You can add actions for Trouble and Normal status changes. For more information on actions, see "Actions" on page 3-27.

9 Click **Next** to advance to the Unit Options tab.

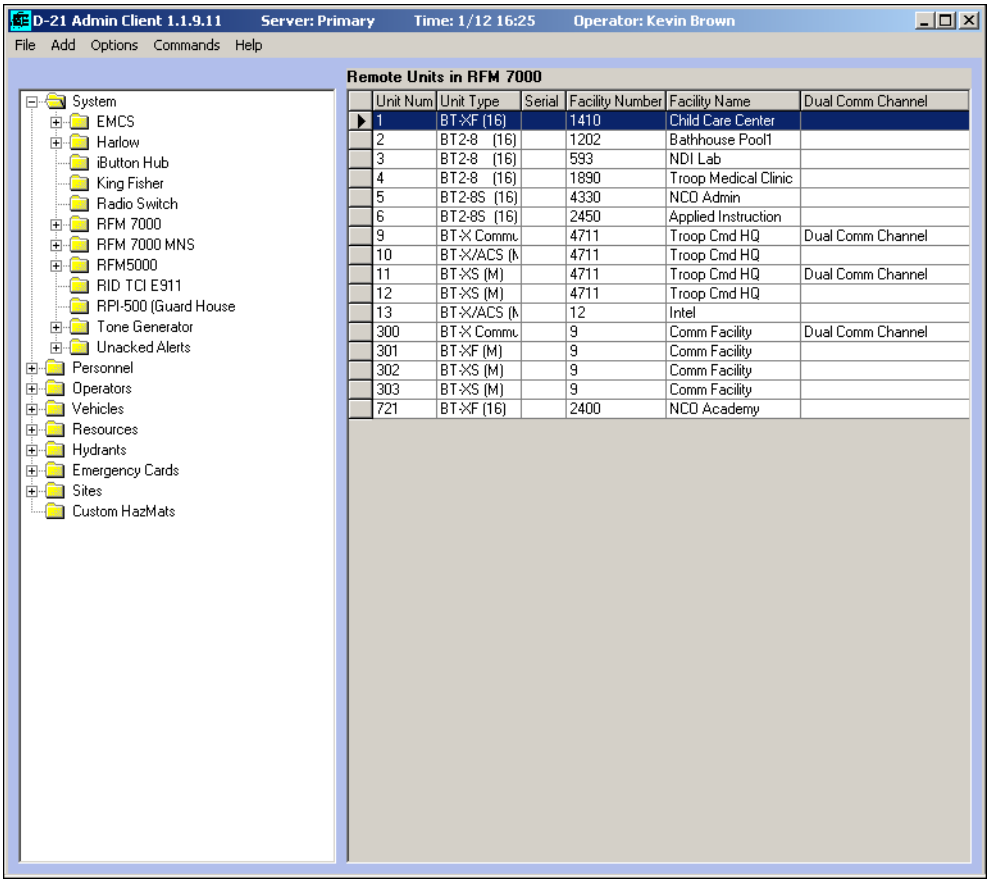


- **Power Status Verification Time** Select the length of time (the default selection is none) you want the D-21 to wait before generating a Battery Fault for the unit. Do not change this setting unless instructed to do so by a Monaco Help Desk representative.

10 Click **Done**. The BT-X Communicator remote unit is added to the System tree under the RID specified on the Remote Unit General tab.

To view remote units with dual communication enabled

1. Click the plus sign (**+**) next to System to expand the list of RIDs.
2. Click the RFM 7000 RID with the Dual Comm Channel option enabled. The Details pane displays all remote units communicating with the D-21 via this RFM.



NOTE *The Dual Comm Channel field lists which BT-X Communicator and BT-XS (M) IDS Master units have dual communication channels enabled.*

Section 7
Configuring Mass Notification

Read this section to learn how to configure remote units for in-building and wide-area mass notification.

Contents

Within-Building and Wide-Area Mass Notification 7-2
MNS Message Types. 7-2
Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts 7-3
Enabling the RFM 7000 RID for Mass Notification 7-4
Adding Pre-Recorded Messages 7-6
Creating Message Groups 7-7
Adding Broadcast Messages 7-11
Adding a RID for the ACU-1000 Radio Switch 7-13
Configuring Workstations for Multiple Live-Voice Sources 7-16
Adding a BT-X with Mass Notification. 7-18
Pre-Configuring MNS Messages 7-24
Configuring AutoMNS in the D-21 7-29

Within-Building and Wide-Area Mass Notification

The D-21 Mass Notification System (MNS) plays within-building and wide-area messages using a BT-X connected to mass notification equipment. The within-building MNS uses the BT-X Communicator to control a mass notification panel connected to speakers within a facility. Wide-area MNS uses the BT-X Wide-Area Communicator to control tower-mounted speakers. Both within-building and wide-area MNS systems can play multiple messages at different locations simultaneously.

Use the D-21 Admin Client to configure remote units for mass notification. Activate MNS messages in the Mass Notification command viewer in the D-21 Incident Client. See the D-21 Incident Client User Guide (P/N 001-392-00) for more information.

MNS Message Types

The D-21 MNS supports three types of messages, as described below.

- **Pre-recorded** Pre-recorded messages are built in to the mass notification panel controlled by the BT-X unit. The messages cannot be changed without modifications to the panel firmware.
- **Live voice** Live voice messages are created by speaking into a microphone source. The live voice source can be the local microphone at the RFM or a handset, desk microphone, or telephone connected to an ACU-1000 radio switch.
- **Broadcast** Broadcast messages are .wav files installed on the D-21 primary server. Additional broadcast message files can be easily added at any time. Broadcast messages utilize the same technical implementation as live voice, so live voice must be configured on the RFM and all units playing broadcast messages. Additionally, an external sound card must be installed on the D-21 primary server and connected to an ACU-1000 radio switch.

Notes on Configuring the Within-Building BT-X Communicator

A BT-X Communicator connected to a within-building mass notification panel can be set up to send pre-recorded messages, live-voice messages, or both. The within-building MNS D-21 configuration of the BT-X varies depending on the program chip:

- **A.9** The BT-X with program chip A.9 installed is a fire-only unit that incorporates MNS functionality into the fire remote unit configuration. If the BT-X only has one type of message mode (pre-recorded or live-voice), that message mode is configured on the first BT-XF (16) remote unit. If the BT-X supports both message modes, pre-recorded messages use the first BT-XF (16) remote unit and live-voice messages use a second BT-XF (16) remote unit, even if there are no additional expansion fire zones.
- **B.8 or higher** The multi-application BT-X Communicator incorporates all MNS functionality into the BT-X Communicator unit address.

To configure within-building and wide-area mass notification

1. Set global timeouts for pre-recorded, live-voice, and keep alive. See "Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts" on page 7-3.
2. Enable mass notification on the RFM 7000 RID. See "Enabling the RFM 7000 RID for Mass Notification" on page 7-4.
3. Add pre-recorded messages to the database. See "Adding Pre-Recorded Messages" on page 7-6.
4. Add broadcast messages to the database. See "Adding Broadcast Messages" on page 7-11.
5. Add mass notification remote units to the database.
   - "To add a BT-X for in-building mass notification" on page 7-19.
   - "To add a BT-X for wide-area mass notification" on page 7-22.
6. Add the ACU-1000 Radio Switch to the database, if its being used as a live-voice input source. See "To add the ACU-1000 RID for broadcast and live-voice sources" on page 7-14.
7. Configure each workstation with available live-voice input sources. See "To configure live-voice sources at a workstation" on page 7-17.

Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts

Timeout settings are used to terminate pre-recorded and live-voice message broadcasts after a user-defined period of time (0 - 60 minutes). Timeout settings are programmed into the MNS remote units by Monaco personnel during installation. The timeout settings entered at the D-21 should be synchronized with the timeout settings programmed at the MNS remote units.

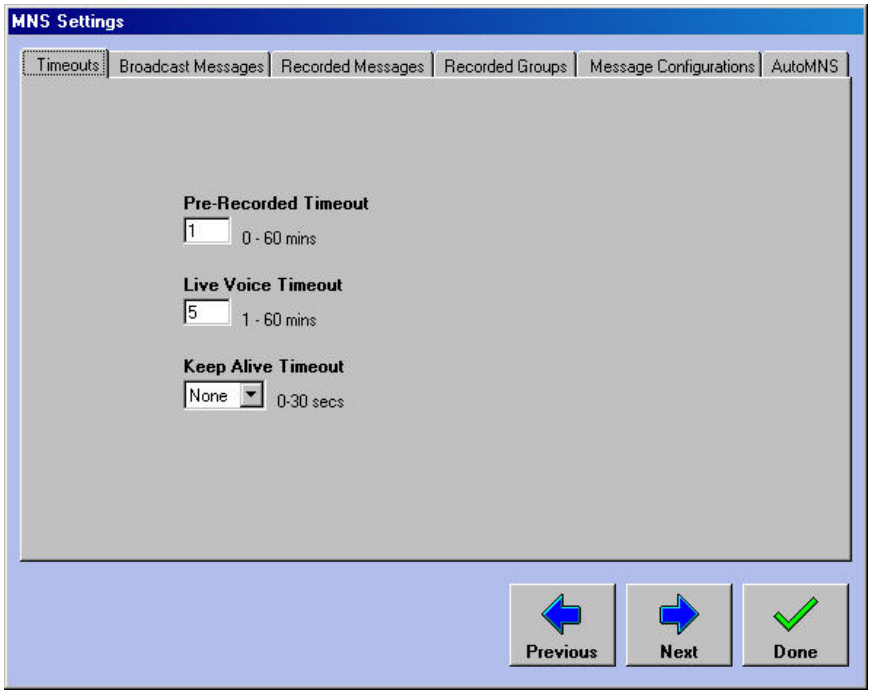
The Keep-Alive signal is a coded transmission that the D-21 sends along with live-voice messages to the BT-X. The Keep-Alive signal "chirps" at regular intervals equivalent to the Keep-Alive timeout. If the BT-X does not receive the Keep-Alive signal, the BT-X turns off the mass notification speakers and stops sending the live-voice transmission to the mass notification equipment.

CAUTION *Fire alarms and other device status changes are not displayed while a live-voice message is activated. The live-voice timeout should be set to the shortest reasonable length of time to ensure prompt notification of device status changes.*

Timeout settings are used globally throughout the D-21 system. All MNS remote units should use the same timeout settings, and if more than one RFM 7000 RID for MNS is configured each RID uses the same timeout settings.

To set up timeouts for mass notification

1 Select **Options > MNS Settings**. The MNS Settings dialog box appears with the Timeouts tab displayed.



- **Pre-Recorded Timeout** Specifies the time interval after which pre-recorded messages, which have not been deactivated by the D-21 operator, will time out at the remote unit. The default is 5 minutes. All pre-recorded messages deactivate automatically after the time specified.
- **Live Voice Timeout** Specifies when the open voice input for live voice is shut off. The default is 5 minutes. If the Keep Alive time is turned on at the BT-X, the live-voice timeout at the BT-X is set at 0. However, you must set the Live Voice timeout to a value greater than 0 in the D-21 for live voice to function correctly.
- **Keep Alive Timeout** Specifies the time interval between signals sent by the D-21 to the BT-X. If the BT-X does not receive the Keep Alive signal at the specified interval, it deactivates the live-voice connection to the mass notification equipment. The default is None.

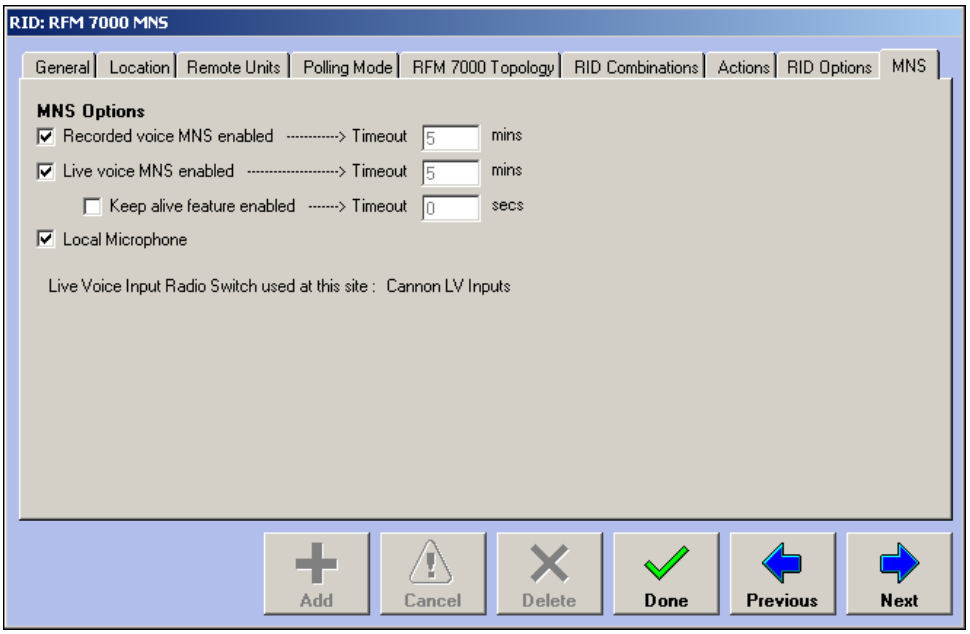
2 Enter the appropriate timeout settings and click **Done**.

Enabling the RFM 7000 RID for Mass Notification

Use the MNS tab in the RFM 7000 RID dialog box to enable and disable MNS options. The MNS tab is only available when the D-21 Mass Notification Client is installed. You must enable pre-recorded and live-voice message modes in the RID configuration in order to see the MNS options in the BT-X Communicator and BT-X/WAC+ remote unit configuration dialog boxes. You must enable the local microphone on the RID MNS tab in order to have the option to select the microphone when configuring live-voice input sources for MNS workstations.

To enable mass notification for the RFM 7000 RID

1. In the tree pane, right-click the RFM 7000 RID that communicates with the BT-X remote units configured for mass notification.
2. Click the MNS tab.



- **Recorded Voice MNS enabled** Select this option if you will be playing pre-recorded messages on units attached to this RID. The timeout displayed to the right of the check box option is set in the Timeout tab in the MNS Settings dialog box. See "Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts" on page 7-3.
- **Live voice MNS enabled** Select this option if you will be using the live-voice mode on units attached to this RID. The timeout displayed to the right of the check box option is set in the Timeout tab in the MNS Settings dialog box. See "Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts" on page 7-3.
- **Keep alive feature enabled** This option is only available if live voice is enabled. Select this option if you have enabled the Keep Alive signal that prevents messages from unauthorized sources. The timeout displayed is set in the Timeout tab in the MNS Settings dialog box. See "Setting Pre-Recorded, Live-Voice, and Keep Alive Timeouts" on page 7-3.
- **Local Microphone** Select this option if the RFM 7000 RID is used to communicate with an RFM-X connected to a local microphone. When this option is selected, the RFM-X local microphone is added to the list of available live-voice input sources. The RFM-X revision must be F.9 or newer to use local microphone for live-voice input. If you enable the local microphone for an RFM-X version that does not support the local microphone, the RID generates an Invalid Configuration message when it is loaded.

3. Click **Done**.

Adding Pre-Recorded Messages

Pre-recorded messages are recorded and stored in the mass notification panel or wide-area controller connected to the BT-X. The mass notification panel that connects to the BT-X Communicator for within-building messages can store up to eight pre-recorded messages. The BT-X Wide-Area Communicator connects to a wide-area controller that stores up to 15 pre-recorded messages. For more information on recording messages, see the documentation provided with your mass notification equipment.

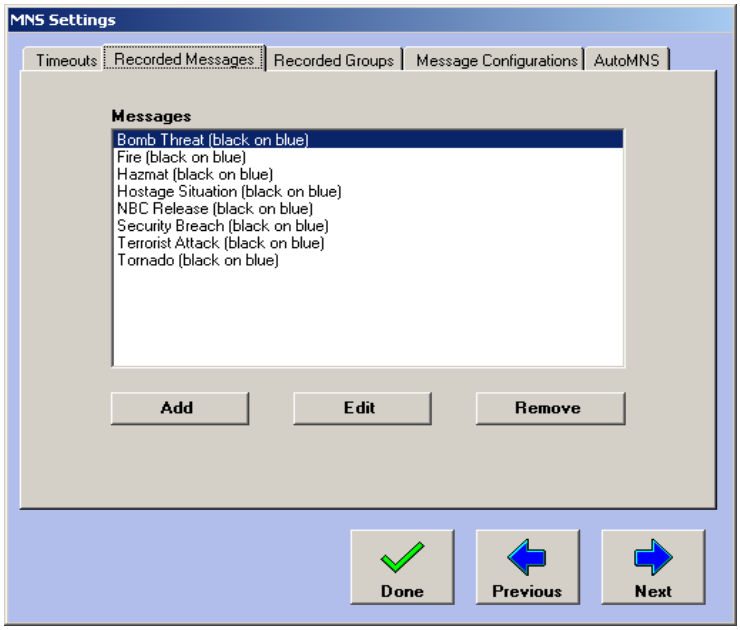
Configuring pre-recorded messages consists of the following tasks:

- Add all pre-recorded messages that are recorded on the mass notification equipment. If a message is repeated on multiple units, add it only once to the database. See "Adding Pre-Recorded Messages" on page 7-6.
- Add a message group for each unique set of messages and message ID pairings. Message groups pair the message name with the ID number used to activate the message by the mass notification equipment. See "Creating Message Groups" on page 7-7.

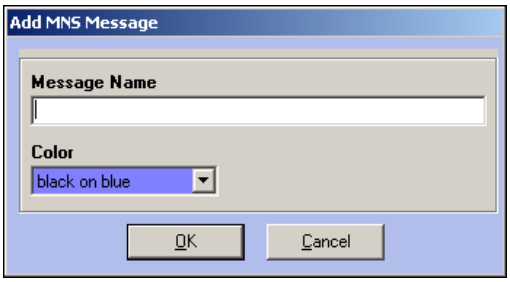
IMPORTANT *Message groups are attached to the BT-X remote unit used to control the mass notification equipment. The message name/number pairings in the message group assigned to the BT-X must match the pairings recorded and stored in the mass notification equipment.*

To add pre-recorded messages

1 Select **Options > MNS Settings** and click the Recorded Messages tab.



2 Click **Add** to add a new pre-recorded message.



3 Enter a descriptive name for the message in order to select it quickly when broadcasting a pre-recorded message from the D-21 Incident Client.

4 If you wish, select a color combination for the message's display in the D-21 Incident Client.

5 Click **OK**.

6 Click **Done**.

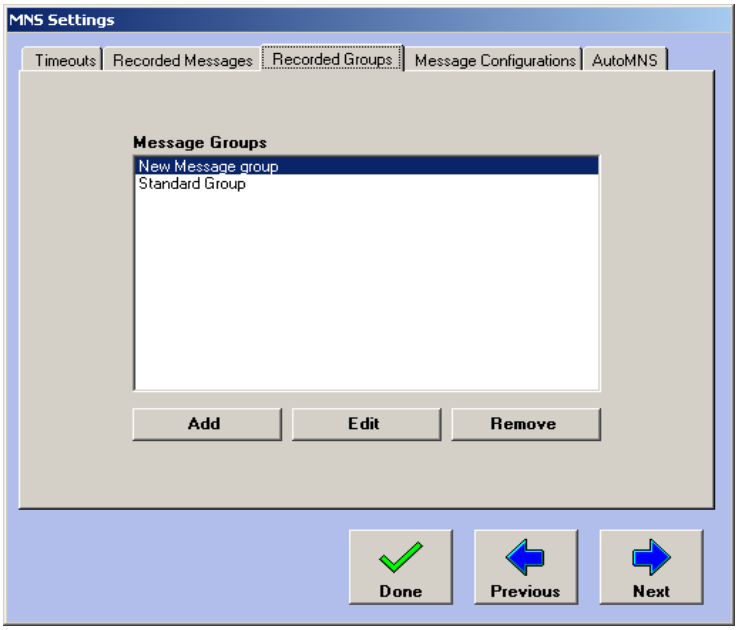
Creating Message Groups

Message groups pair individual pre-recorded messages with the message ID numbers used to activate the message at the mass notification equipment. Within-building MNS panels use eight dry contact inputs to activate up to eight messages. Wide-area MNS panels support up to 15 message IDs. When you create a group, specify whether it is an in-building group (for use with the BT-X Communicator) or a wide-area group (for use with the BT-X/WAC+).

IMPORTANT *The D-21 sends the message ID number, not the message name, to the BT-X when broadcasting pre-recorded messages. The message ID equals the dry contact input on within-building MNS panels or the ID number sent through the serial connection to the wide-area controller.*

To create a message group

1. Select **Options > MNS Settings**.
2. Click the Recorded Groups tab.

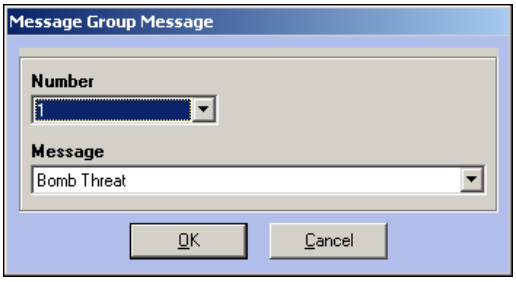


3 Click **Add Group.** The New Message Group dialog box appears.

- **Message Group Name** Enter a name for the group.
- **Use** Select the type of MNS equipment that will use this message group. In-building message groups have up to eight messages and can be attached to the BT-X Communicator remote unit. Wide Area message groups can have up to 15 messages and are used with the BT-X/WAC+ remote unit type.
- **Messages** Lists the messages that are part of the message group.

4 Click **Add Message**. The Message Group Message dialog box appears.

IMPORTANT *The number and message selected in the Message Group Message dialog box must match the number and message assigned in the mass notification equipment.*



5 Select the desired message number from the Number drop-down list.

6 Select the desired message from the Message drop-down list. You can add messages to the list using the Messages tab. See "To add pre-recorded messages" on page 7-6.

7 Click **OK**.

8 Repeat these steps for each message you want to add to the group.

9 Click **OK** in the New Message Group dialog box.

10 Click **Done** in the Groups dialog box.

To edit a message group

1 Select **Options > MNS Settings**.

2 Click the Recorded Groups tab.

3 Select the desired group, then click **Edit**. The Message Groups dialog box appears.

4 Do one of the following:

- To change the group name, edit the text in the Message Group Name box.

OR

- To add a message, click **Add Message**. The Message Groups dialog box appears, from which you can specify the message being added. For more information, see "To create a message group" on page 7-8.

OR

- If you want to remove a message from the group, select it and click **Remove Message**.

5 Click **OK** in the Message Groups dialog box.

6 Click **Done** in the Groups dialog box.

To remove a message group

1 Select **Options > MNS Settings**.

2 Click the Recorded Groups tab.

3 Select the desired group, then click **Remove.** A confirmation message asks if you want to delete the group.

4 Click **Yes**.

5 Click **Done** in the MNS Settings dialog box.

Adding Broadcast Messages

In order to play a .wav file stored on the D-21 primary server as a broadcast message, the following configuration steps must be carried out:

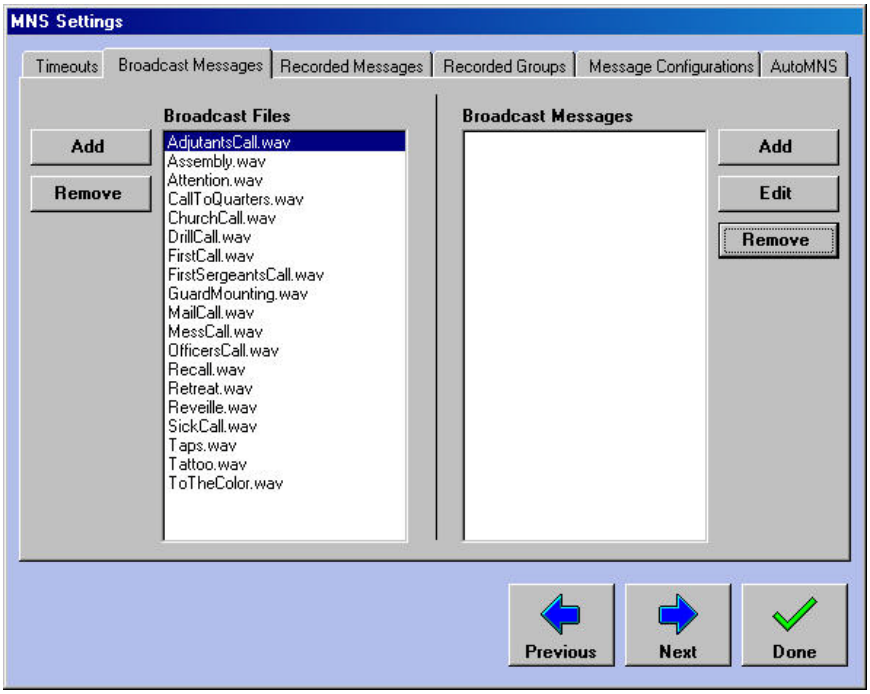
- The file name must be added to the D-21 database.
- The file must be copied to the correct location in the primary server's directory structure.
- A broadcast message name must be added and associated with the file name.

The following instructions describe how these steps are carried out.

NOTE *By default, a number of commonly used broadcast .wav files are automatically copied to the primary server and added to the D-21 database when broadcast message functionality is installed on the D-21. To use these files, it is necessary to add a broadcast message name.*

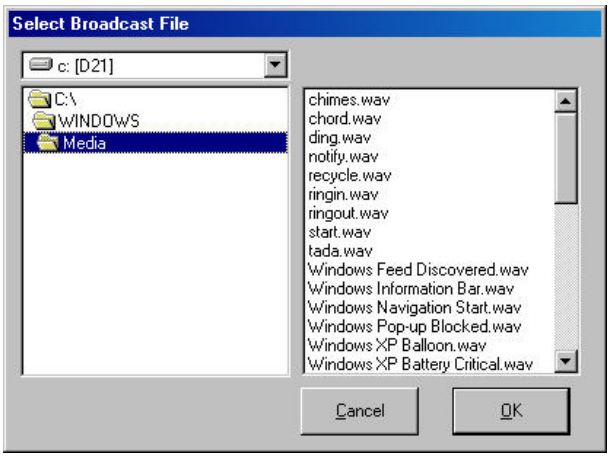
To add a broadcast file

1 Select **Options > MNS Settings** and display the Broadcast Messages tab.



The **Broadcast Files** list box on the left displays all the .wav files that have been added. **The Broadcast Messages** list box on the right displays any broadcast message names that have been associated with a broadcast file.

2 Click the **Add** button on the left side of the dialog box. The Select Broadcast File dialog box is displayed.

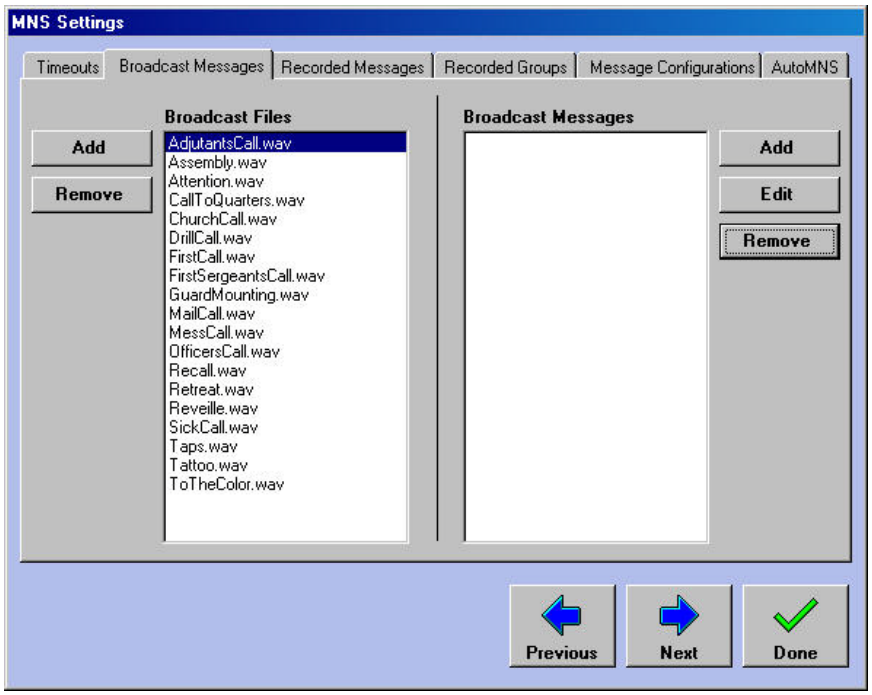


3 Navigate the directory tree on the left until the new file is displayed in the list on the right.

4 Select the file and click **OK.** The file is automatically copied to the correct directory on the primary server. The dialog box closes and the file name is displayed in the **Broadcast Files** list box.

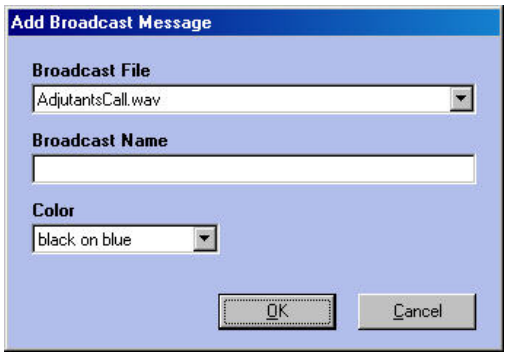
To add a broadcast message

1 Select **Options > MNS Settings** and display the Broadcast Messages tab.



The **Broadcast Files** list box on the left displays all the .wav files that have been added. **The Broadcast Messages** list box on the right displays any broadcast message names that have been associated with a broadcast file.

2 Click the **Add** button on the right side of the dialog box. The Add Broadcast Message dialog box is displayed.



3 Select the .wav file to be associated with the new broadcast message from the **Broadcast File** drop-down list. This list contains the same files displayed in the Broadcast Files list box on the Broadcast Messages tab.

4 Enter a name for the new message in the **Broadcast Name** text box.

5 If desired, change the color scheme used to display the broadcast message in the D-21 Incident Client by selecting it from the **Color** drop-down list.

6 Click **OK**. The dialog box closes and the new message is displayed in the Broadcast Messages list box.

Adding a RID for the ACU-1000 Radio Switch

The ACU-1000 Radio Switch provides multiple input sources for live-voice and broadcast messages. Channel 0 is reserved for the ACU-1000 handset. Channels 1 & 2 are reserved for use by the RFM-X. Channels 3 through 12 are user-configurable and their usage depends on the hardware configuration of the radio switch.

Each radio switch requires a unique RID in the D-21 database. The radio switch channels are added to the radio switch RID. The names you give to the channels in the RID configuration are the names you will use to select the input source for each live-voice and broadcast message you play in the D-21 Incident Client.

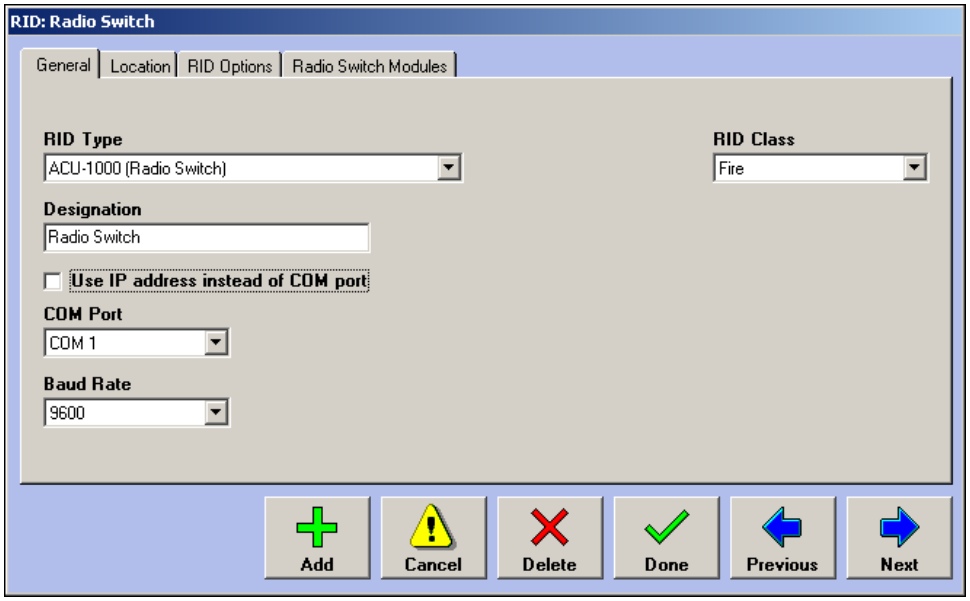
Radio switch channels, as well as the RFM-X local microphone, are only available for use at workstations where they have been added to the list of available input sources. An operator can only select input sources that have been added to the workstation. See “Configuring Workstations for Multiple Live-Voice Sources” on page 7-16.

Setting Up Live-Voice Sources for Multiple Sites

If you are configuring live-voice input sources for more than one site, a separate radio switch and radio switch RID are required for each site. Each site playing live-voice messages must also have its own RFM-X and RFM 7000 RID. The D-21 pairs the radio switch with the RFM-X by matching their respective sites.

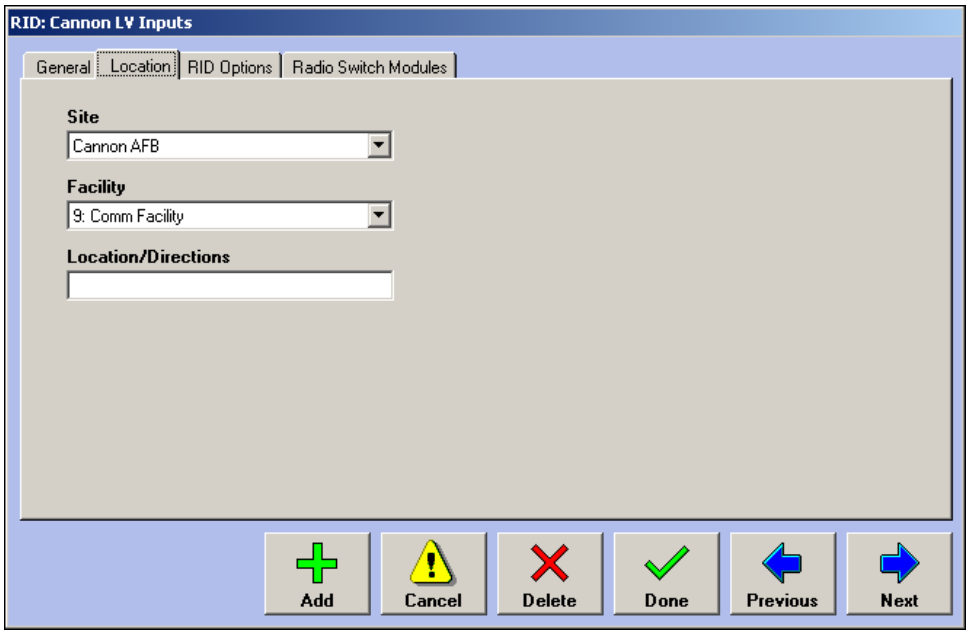
To add the ACU-1000 RID for broadcast and live-voice sources

1 Select **Add > RID**. The Add New RID dialog box appears.



- **RID Type** Select ACU-1000 (Radio Switch).
- **RID Class** Select either Fire, Security, or Facility Management to specify if this RID receives commands from Fire, Security or Facility Management workstations and users.
- **Designation** Type a name for the RID.
- **Use IP address instead of COM port** Check this option if the radio switch uses the network to communicate with the D-21 server workstation. You will need to enter an internet protocol (IP) address, port, and port timeout for the switch.
- **COM Port** Select a COM port from the list if the radio switch is connected directly to a COM port on the back of the D-21 server workstation.
- **Baud Rate** Select 9600 for optimal operation with the D-21 if you are using a COM port connection for communications.

2 Click the Location tab.

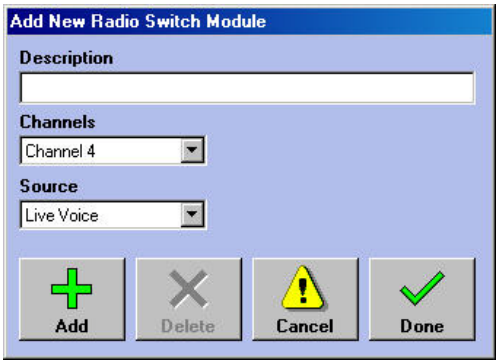


- **Site** Select the site that will have access to this radio switch. See "Setting Up Live-Voice Sources for Multiple Sites" on page 7-13 for more information.
- **Facility** Select the facility you want to associate with the location of the radio switch.
- **Location/Directions** Enter additional information that describes the location of the radio switch.

NOTE *Make changes to the RID Options tab only if instructed to do so by Monaco technical representatives.*

3 Click the Radio Switch Modules tab.

4 Click **Add Module**. The RID will be loaded before you can add a radio switch module.



- **Description** Enter the name of the input source device. This is the name operators will use when selecting this input source for a live-voice or broadcast message.
- **Channels** Select the radio switch channel through which the input source will be routed when a live-voice or broadcast message is initiated at the D-21. Channel 0 is reserved for the radio switch handset. Channels 1 and 2 are reserved for use by the RFM-X.
- **Source** Select the type of message for this module, either Live Voice or Broadcast.

5 Add a module for each channel being used for live-voice or broadcast messages at the D-21.

6 Click **Done**.

7 In the RID dialog box, click **Done**.

Configuring Workstations for Multiple Live-Voice Sources

Each workstation can be configured with a custom list of live-voice input sources, including the local microphone (controlled from the RFM 7000 RID) and live-voice input radio switch modules. See the Live Voice Input Radio Switch Manual (P/N 001-444-00) for more information.

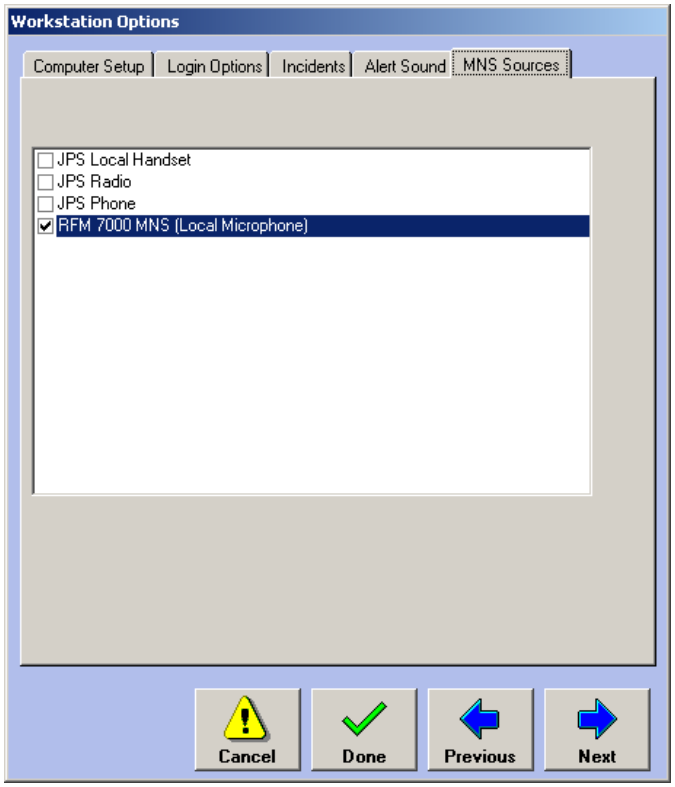
Use the following procedure to configure the available live-voice sources for each MNS workstation that will broadcast live-voice messages. See "Adding a RID for the ACU-1000 Radio Switch" on page 7-13 for more information on configuring the radio switch in the D-21.

To configure live-voice sources at a workstation

1 Select **Options > Workstation Options**. The Workstation Options dialog box appears.

NOTE *You must enable the local microphone in the RFM 7000 RID and add the ACU-1000 Radio Switch RID and input modules before these input sources can be assigned to a workstation.*

2 Click the MNS Sources tab.



If there is more than one radio switch, the name of the channel is preceded by the name of the radio switch RID

3 Select the live-voice input sources available for use at this workstation. The RFM-X local microphone is enabled at the RFM 7000 RID that is used for the RFM-X. See "Enabling the RFM 7000 RID for Mass Notification" on page 7-4. The other input sources are from one or more live-voice input radio switches. See "Setting Up Live-Voice Sources for Multiple Sites" on page 7-13 for more information.

4 Click **Done**.

Adding a BT-X with Mass Notification

There are two remote unit types used to configure a BT-X with mass notification equipment:

- **BT-X Communicator** Used to configure BT-X remote units connected to In Building mass notification panels. When you enable MNS on this unit type, the eight onboard relay drivers are reserved for activating the dry contact inputs on the mass notification panel, and the Outputs tab is not available. You can add four onboard zone inputs to the unit (zones 1 - 4) and four status reporting zones (13 - 16). See "To add a BT-X for in-building mass notification" on page 7-19.

IMPORTANT *When configuring a BT-X with a program chip (P/N 325-305-00 revision A.9 or older), the MNS functionality shares the base transceiver address with the BT-XF fire transceiver that uses the BT-XF(16) unit type.*

- **BT-X/WAC+** Used to configure the BT-X Wide Area Communicator that broadcasts pre-recorded and live-voice messages from tower-mounted speakers via a wide-area controller. The BT-X/WAC activates messages in the wide-area controller via serial connections and does not support output relays. Add the following three zones that report the status of the wide-area controller:

Zone	Description	Status Conditions
12	**Bad database**	Off normal condition on this BT-X/WAC+ zone indicates a problem with the local message database at the BT-X Wide Area Communicator. When zone 12 is off normal, the unit will not reply to the Initiate Message command from the D-21.
14	**Communication failure with the wide area controller**	Off normal condition on this BT-X/WAC+ zone indicates a communications failure between the BT-X and the wide-area controller. When zone 14 is off normal, the unit will not reply to the Initiate Message command from the D-21.
15	**Amplifier fault**	An alarm condition on this zone indicates an amplifier fault on the output side of the amplifier. When zone 15 is in alarm, the unit will not reply to the Initiate Message command from the D-21.
		A trouble condition on this zone indicates an amplifier fault on the input side of the amplifier. When zone 15 is in trouble, the unit will attempt to reply to the Initiate Message command from the D-21.

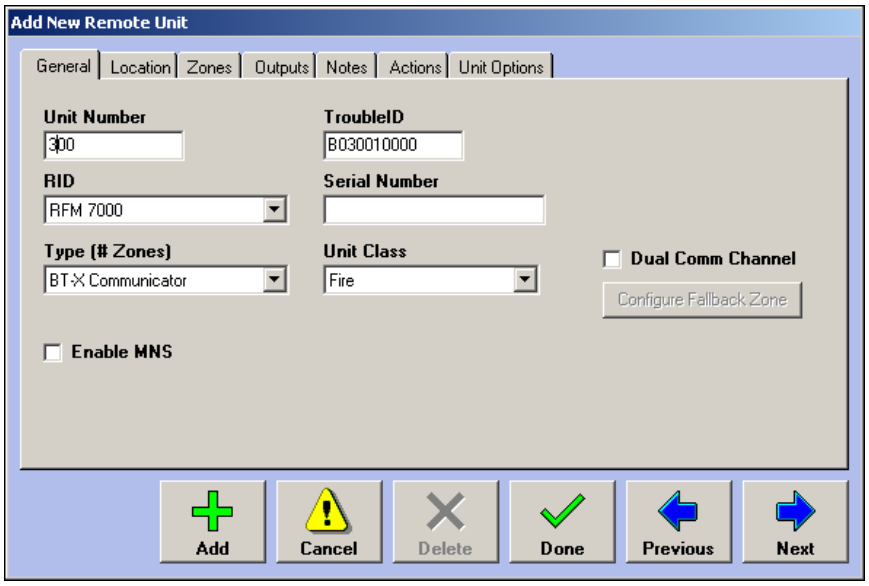
For more information, see "To add a BT-X for wide-area mass notification" on page 7-22.

Before you begin

If you are adding a remote unit for broadcasting pre-recorded messages, see "Adding Pre-Recorded Messages" on page 7-6 and "Creating Message Groups" on page 7-7 before adding the remote unit.

To add a BT-X for in-building mass notification

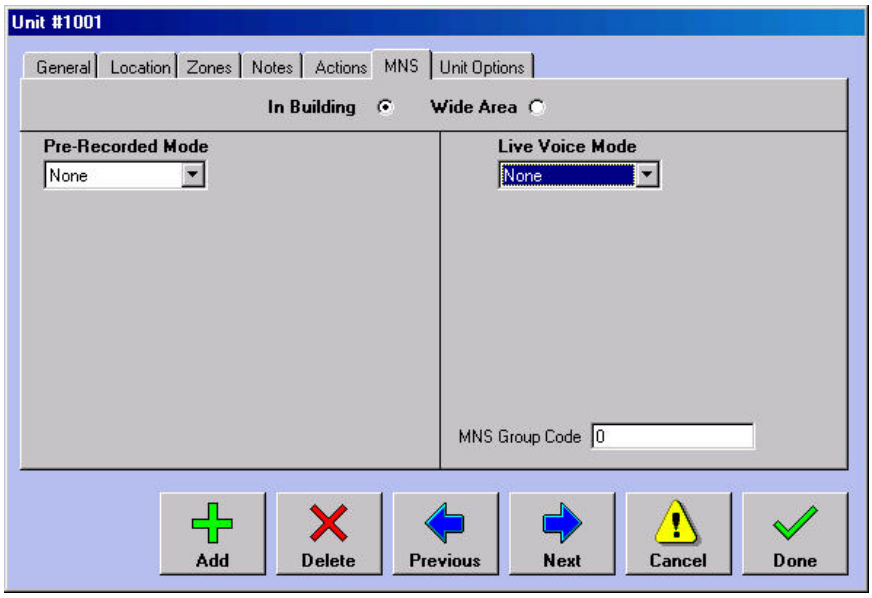
1 Select **Add Remote Unit**. The Add New Remote Unit dialog box appears.



- **Unit Number** Enter a unit number between 1 and 2040 that is unique from other units assigned to the same RID. Use the unit number assigned to the BT-X Communicator when the unit was programmed locally at the BT-X.
- **RID** Select the RFM 7000 RID the BT-X will use to communicate to the D-21.
- **Type (# Zones)** Select BT-X Communicator or BT-X Communicator+, as appropriate. The Enable MNS, Unit Class, and Dual Comm Channel options appear in the dialog box.
- **Enable MNS** Select this option to enable MNS functionality on this remote unit.

For more information regarding the fields on the General tab, or for information adding zones, actions, and outputs to the BT-X Communicator unit, see "To add the BT-X Communicator unit" on page 6-6.

2 Click the MNS tab.

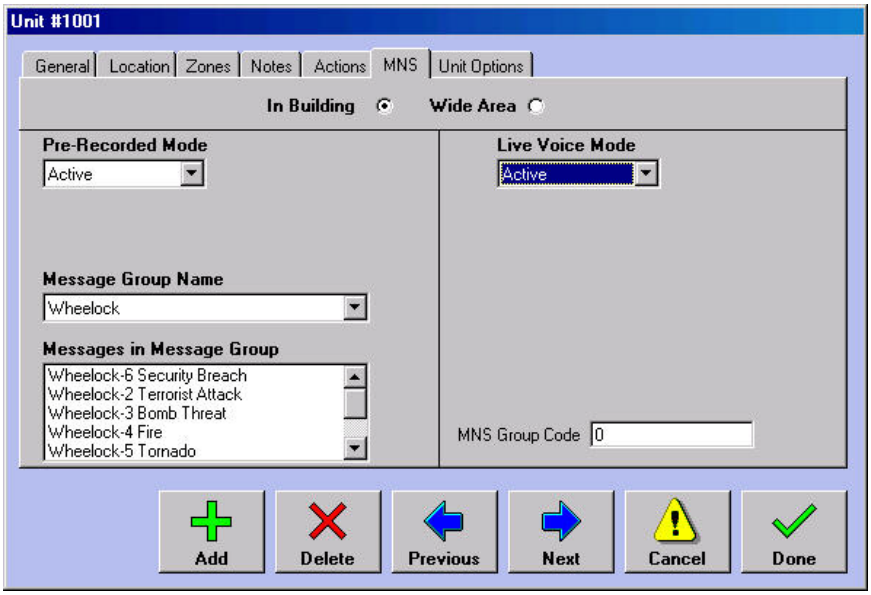


- **In Building / Wide Area** If necessary, select In Building.
- **Pre-Recorded Mode** Select Active if the remote unit will be used to play pre-recorded messages.
- **Live Voice Mode** Select Active if the remote unit will be used to play live voice messages.

- **MNS Group Code** Displays the MNS group code programmed at the remote unit. MNS remote unit groups are used with AutoMNS actions. See "To create an AutoMNS action" on page 3-28.

NOTE *You can populate the MNS Group Code field by running the Query Config command for the remote unit in the D-21 Incident Client.*

3 Configure pre-recorded messages and live-voice speaker control for the remote unit.



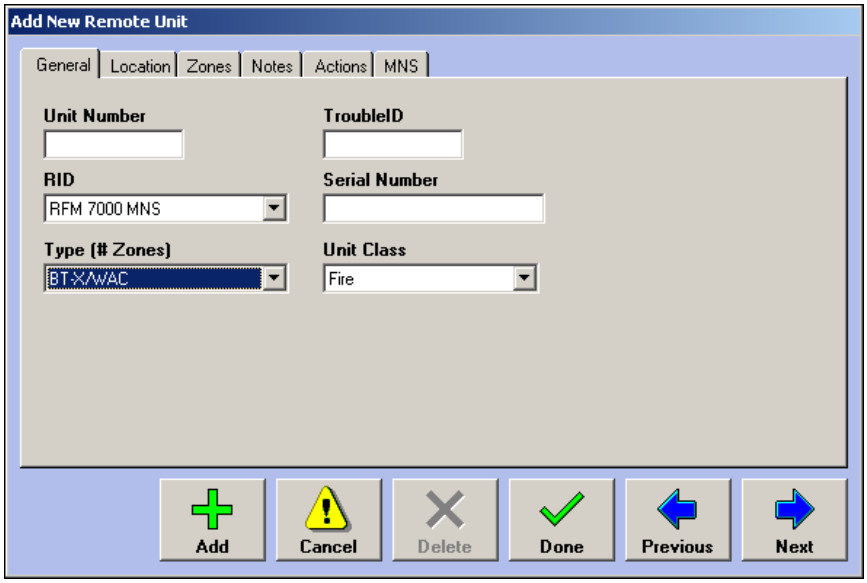
NOTE *If you are setting up pre-recorded messages for a BT-XF (16) unit type, select the unit address in the Pre-Recorded Address drop-down list. This list appears only when you are working with the BT-XF (16) unit type. If you are setting up live voice for a BT-XF (16) unit type, select the next consecutive unit address after the pre-recorded unit address in the Live Voice Address drop-down list. This list appears when you are working with the BT-XF (16) unit type.*

- **Message Group Name** Select the pre-recorded message group with the same message configuration as the MNS panel. Only pre-recorded message groups are displayed in this list. The Messages in Message Group box updates to show the messages in the selected group.

4 Click **Done**.

To add a BT-X for wide-area mass notification

1 Select **Add > Remote Unit**. The Add New Remote Unit dialog box appears.

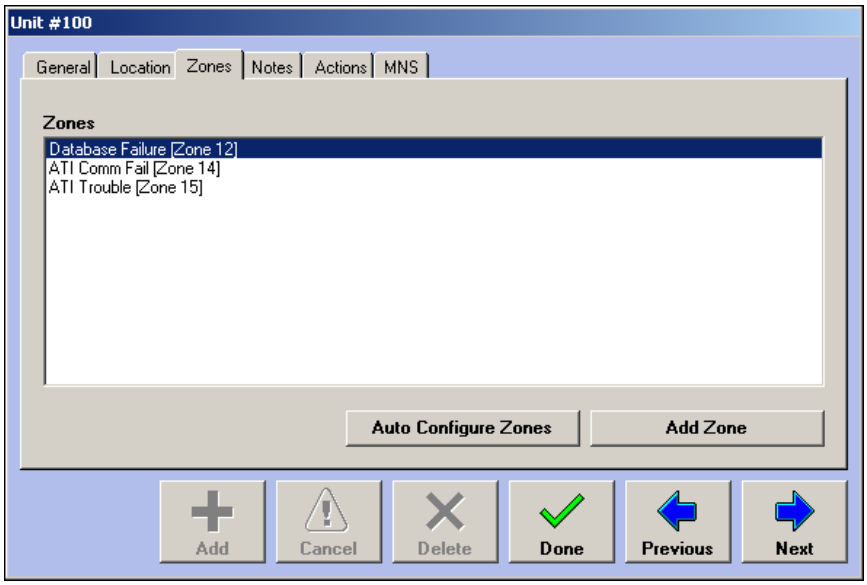


- **Unit Number** Enter a unit number between 1 and 2040 that is different from other units assigned to the same RID. Use the unit number assigned to the BT-X Wide Area Communicator when the unit was programmed locally at the BT-X.
- **RID** Select the RFM 7000 RID the BT-X will use to communicate to the D-21.
- **Type (# Zones)** Select BT-X/WAC+. The Unit Class option appears in the dialog box.
- **TroubleID** Reserved for use by Monaco Enterprises.
- **Serial Number** Enter the serial number for the remote unit hardware. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class for the remote unit type. If the unit class field is enabled, you can select either Fire, Facility Management, or Security of the unit. See "Unit Class" on page 2-52 for more information.

2 Click the Location tab.

3 Select the facility where the remote unit is located from the Facility drop-down list. If desired, enter more specific information in the Location/Directions box.

4 Click the Zones tab.



- **Auto Configure Zones** Adds three status reporting zones for the wide-area controller that is connected to the BT-X. See "Adding a BT-X with Mass Notification" on page 7-18 for more information.
- **Add Zone** The BT-X/WAC+ does not support standard fire zone inputs. Use the Add Zone button if you want to manually add status reporting zones 12, 14, or 15. See "Zones" on page 2-64.

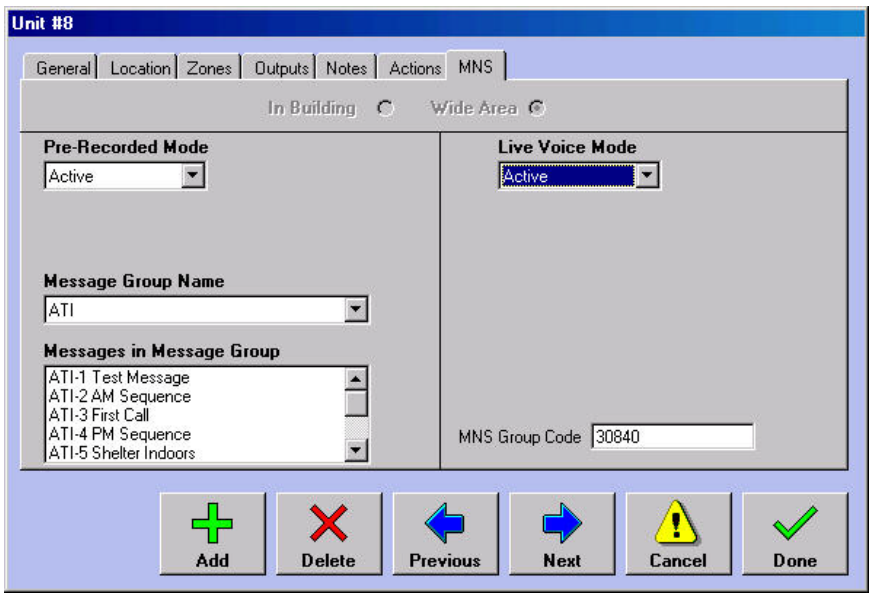
5 Click the Notes tab.

6 Enter text in the Notes box, if needed.

7 Click the Actions tab.

8 Add status change actions for the unit, if needed. See "Actions" on page 3-27.

9 Click the MNS tab.



- **Pre-Recorded Mode** Select Active if the remote unit will be used to play pre-recorded messages.
- **Message Group Name** Select the message group with the message configuration that matches the messages in the wide-area controller. Only wide-area message groups are displayed in this list. The Messages in Message Group list box displays the pre-recorded messages in the selected group.
- **Live Voice Mode** Select "Active" if the remote unit will be used to play live voice messages.
- **MNS Group Code** Displays the MNS group code programmed at the remote unit. MNS remote unit groups are used with AutoMNS actions. See "To create an AutoMNS action" on page 3-28.

NOTE *You can populate the MNS Group Code field by running the Query Config command for the remote unit in the D-21 Incident Client.*

10 Click **Done**.

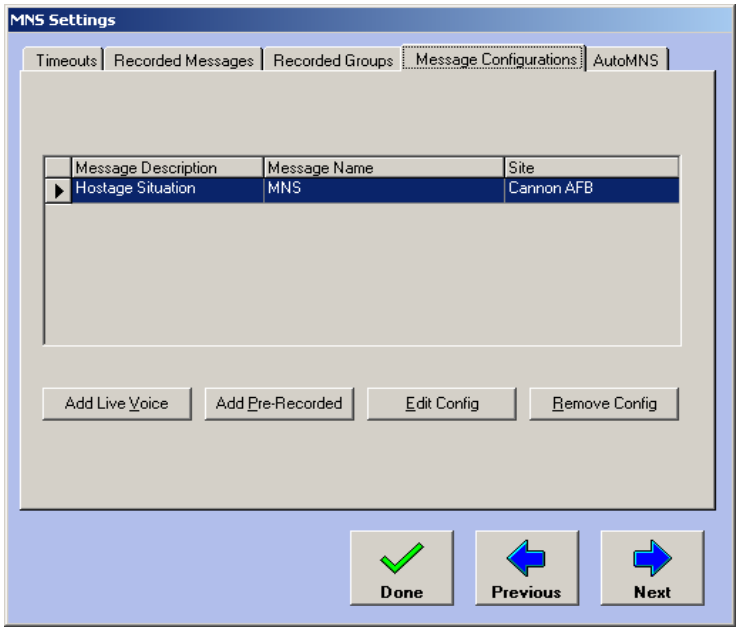
Pre-Configuring MNS Messages

The majority of pre-recorded and live-voice messages are configured and activated by operators in the D-21 Incident Client. The operator selects the type of message, the content of the message (a specific pre-recorded message or live-voice input source), and the facilities in which the message will play. Then, the operator initiates and activates the message.

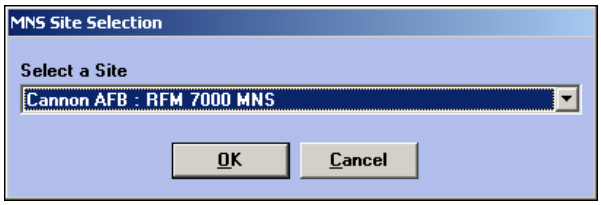
Use pre-configured messages to set up messages that have a predictable type, content, and location. Pre-configured messages are created in the D-21 Admin Client, then initiated and activated “as is” in the D-21 Incident Client. Operators can initiate the message, but cannot change it or its destination.

To pre-configure a pre-recorded message

1. Select **Options > MNS Settings**.
2. Click the Message Configurations tab.

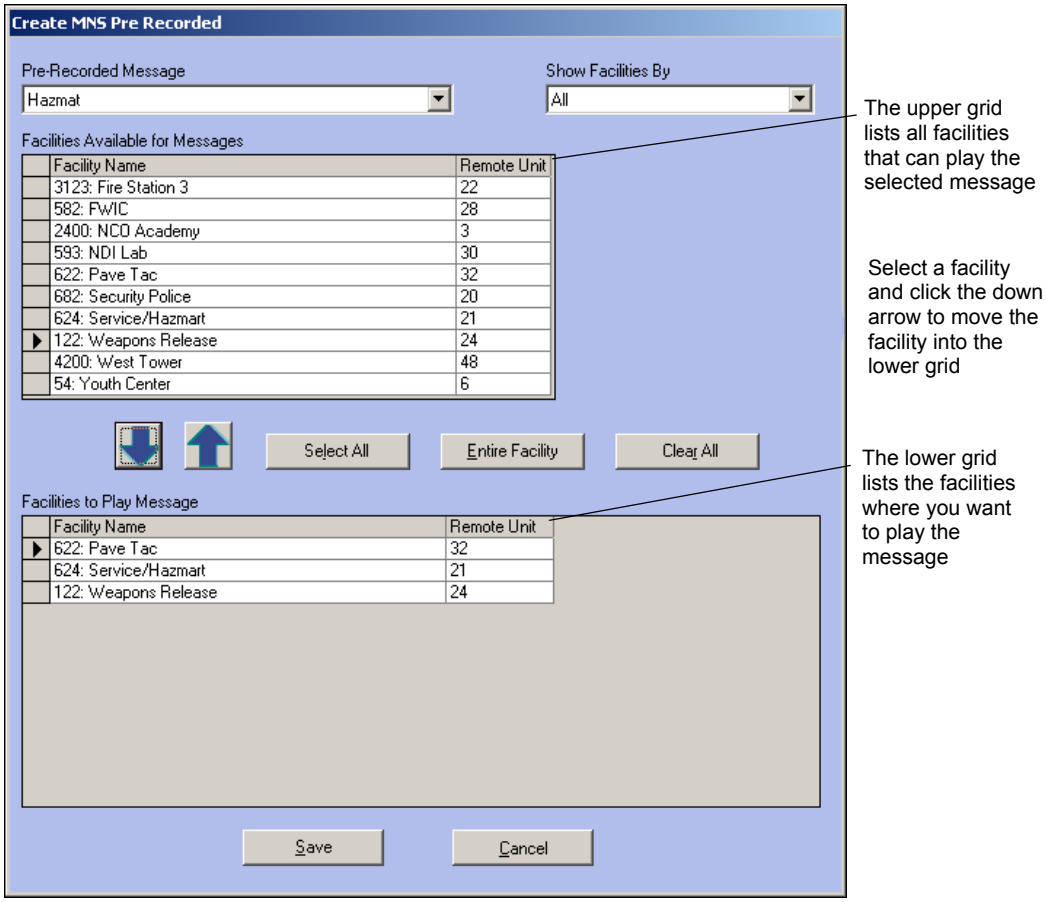


3. Click **Add Pre-Recorded**. A site selection dialog box appears.



4. Select the site where you want to broadcast the message.

5 Click **OK**. The Create MNS Pre-Recorded dialog box appears.



6 Select the message you want to broadcast in the Pre-Recorded Message drop-down list. The list of facilities in the upper grid only displays facilities where there is a BT-X remote unit that has been configured with the selected message.

7 Select the type of facility you want to display in the upper grid in the Show Facilities By drop-down list.

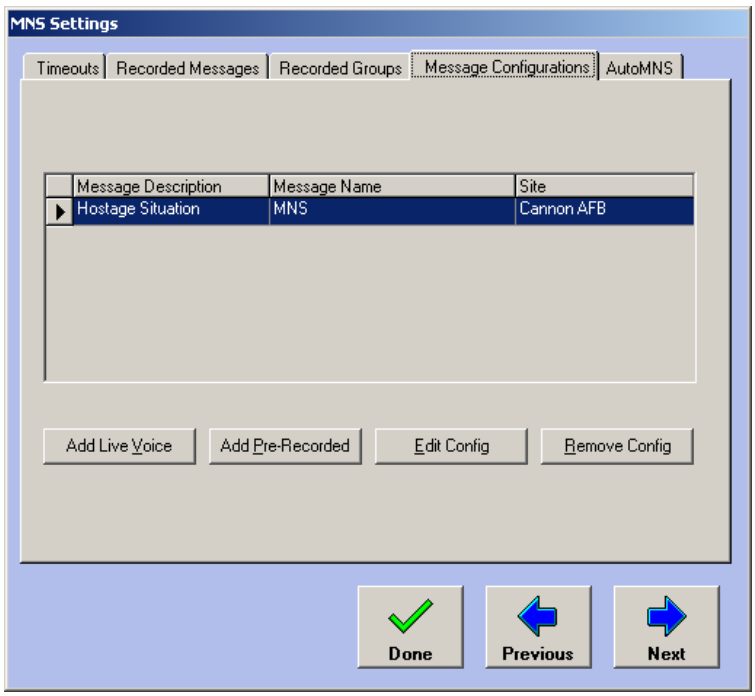
- **In-Building** All facilities associated with BT-X Communicator units configured for pre-recorded messages, with the selected message in their message group.
- **Wide-Area** All facilities associated with BT-X/WAC units configured for pre-recorded messages, with the selected message in their message group.
- **All** All units configured for pre-recorded messages, with the selected message in their message group.

8 Select the facilities in which you want to broadcast the selected message from the upper grid and click the down arrow to move them into the lower grid.

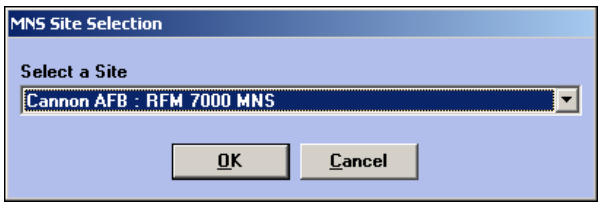
9 Click **Save**. When prompted, provide a name for the configuration. The pre-configured, pre-recorded message will now be available in the D-21 Incident Client.

To pre-configure a live-voice message

1. Select **Options > MNS Settings**.
2. Click the Message Configurations tab.

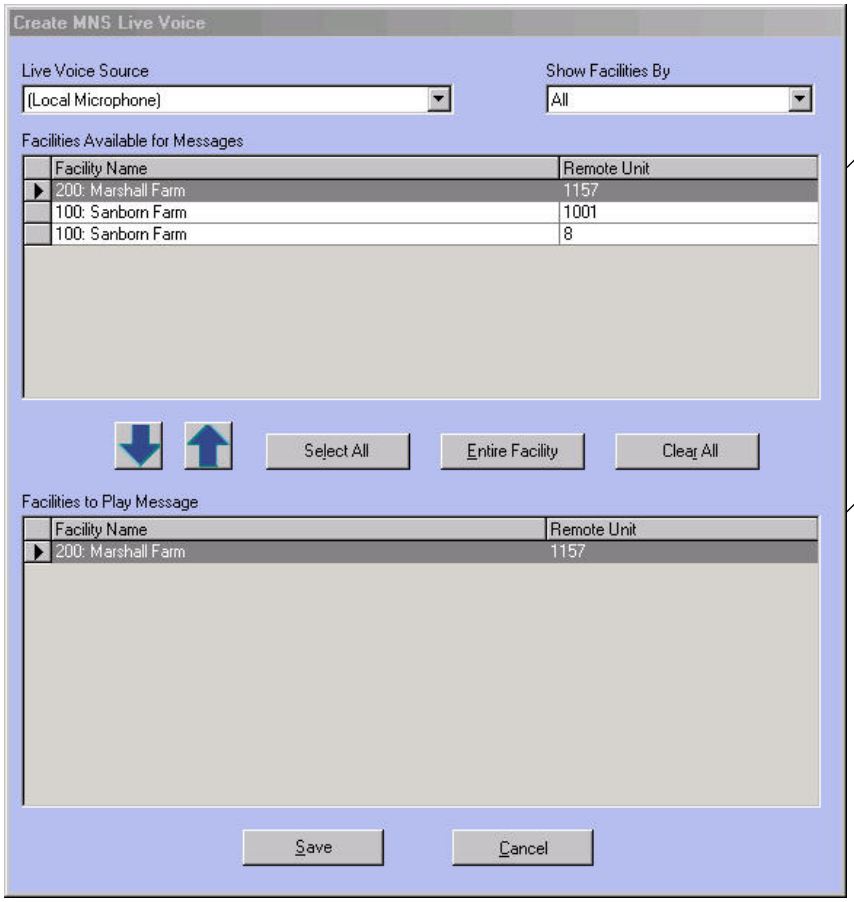


3. Click **Add Live Voice**. A site selection dialog box appears.



4. Select the site where you want to broadcast the message.

5 Click **OK**. The Create MNS Live-Voice dialog box appears.



6 Select the input source you want to broadcast in the Live Voice Source drop-down list. This list is customized for this workstation. See "Setting Workstation Options" on page 4-49.

7 Select the type of facility you want to display in the upper grid in the Show Facilities By drop-down list.

- **In-Building** All facilities associated with BT-X Communicator remote units configured for live-voice messages appear in the list.
- **Wide Area** All facilities associated with BT-X/WAC+ remote units configured for live-voice messages appear in the list.
- **All** All units configured for live-voice messages appear in the list.

8 Select the facilities in which you want to broadcast the live-voice message from the upper grid and click the down arrow to move them into the lower grid.

9 Click **Save**. Provide a name for the configuration at the prompt. The pre-configured live-voice message will now be available in the D-21 Incident Client.

Configuring AutoMNS in the D-21

AutoMNS refers to the function which allows the D-21 user to schedule an MNS message to play at a particular time over particular units on a regular basis. The automation is set up via an action which can be scheduled in the Incident Client, just as other scheduled operations are configured. AutoMNS must be configured in the D-21 Admin Client before an AutoMNS action can be scheduled.

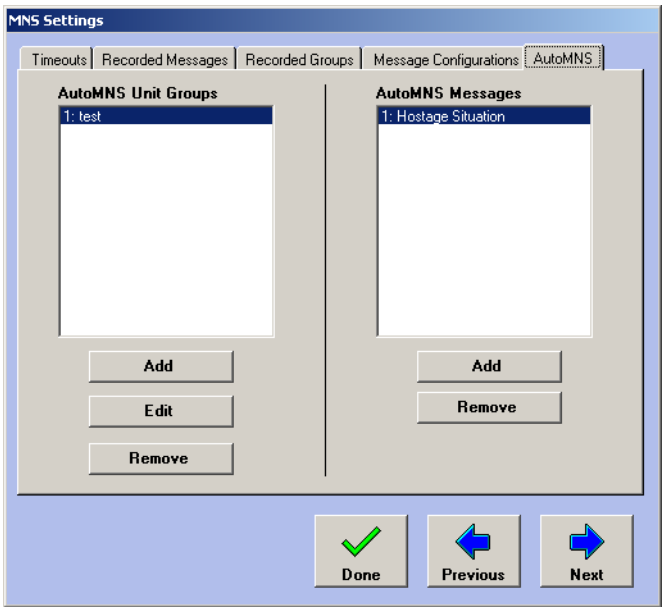
NOTE *Only BT-X/WAC+ remote units can play AutoMNS messages at this time.*

To set up AutoMNS

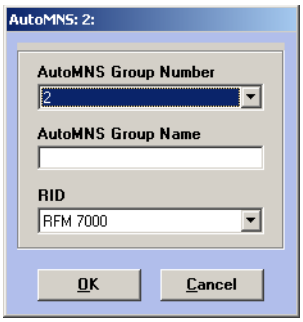
1. Add the unit group number for each group of remote units which will play AutoMNS messages. See "To add an AutoMNS unit group" on page 7-29.
2. Add the message number for each message which will be played by AutoMNS. See "To add an AutoMNS message" on page 7-31.
3. Create the AutoMNS action. See "To create an AutoMNS action" on page 3-28.
4. Schedule the AutoMNS action. See the D-21 Incident Client User Guide (P/N 001-392-00) for instructions on scheduling actions.

To add an AutoMNS unit group

1. From the Admin Client, click **Options** > **MNS Settings.** Click the AutoMNS tab.



2 Click **Add** in the Unit Groups section.



- **Group Number** Select the group number assigned to the remote units which will play the AutoMNS message.

NOTE *Group numbers are usually assigned to BT-X/WAC+ remote units when they are programmed. In addition, you can assign a BT-X/WAC+ to a group by creating a D-21 output and activating it. Please call Monaco for assistance with this procedure, if necessary.*

- **Group Name** Enter a group name into the AutoMNS Group Name field. It should be a name descriptive enough to be helpful to the user creating the action to trigger the message group.
- **RID** Select the RID device from the RID drop-down list that communicates with the remote unit group.

NOTE *Only RFM7000s and RFM-Xs show in the RID drop-down list.*

3 Click **OK.**

To add an AutoMNS message

1 Click **Add** in the AutoMNS Messages section.

2 Select the number of the message to be played by AutoMNS from the Message Number drop-down list. This should be the number of the message as assigned at the MNS panel.

IMPORTANT *The AutoMNS message number should match the number assigned to the message on the Recorded Messages tab.*

3 Select the corresponding message name from the Message drop-down list. All the messages defined on the Recorded Messages tab appear on this list.

NOTE *Only wide-area messages should be designated as AutoMNS messages at this time.*

4 Click **OK**.

Section 8
Configuring Access Control

Read this section to learn how to configure and operate an access control system in the D-21 Security Client.

Contents

Overview of Access Control 8-2
Setting Up Access Control Units and Readers 8-3
- Creating Access Control Groups 8-4
- Creating Access Schedules 8-6
- Adding a BT-X with Access Control 8-10
- Downloading Settings to Access Control Units 8-20

Operating an Access Control System 8-23
- Assigning Cards and PINs 8-23
- Changing Card Assignments 8-27
- Tracking Card Usage 8-30

Overview of Access Control

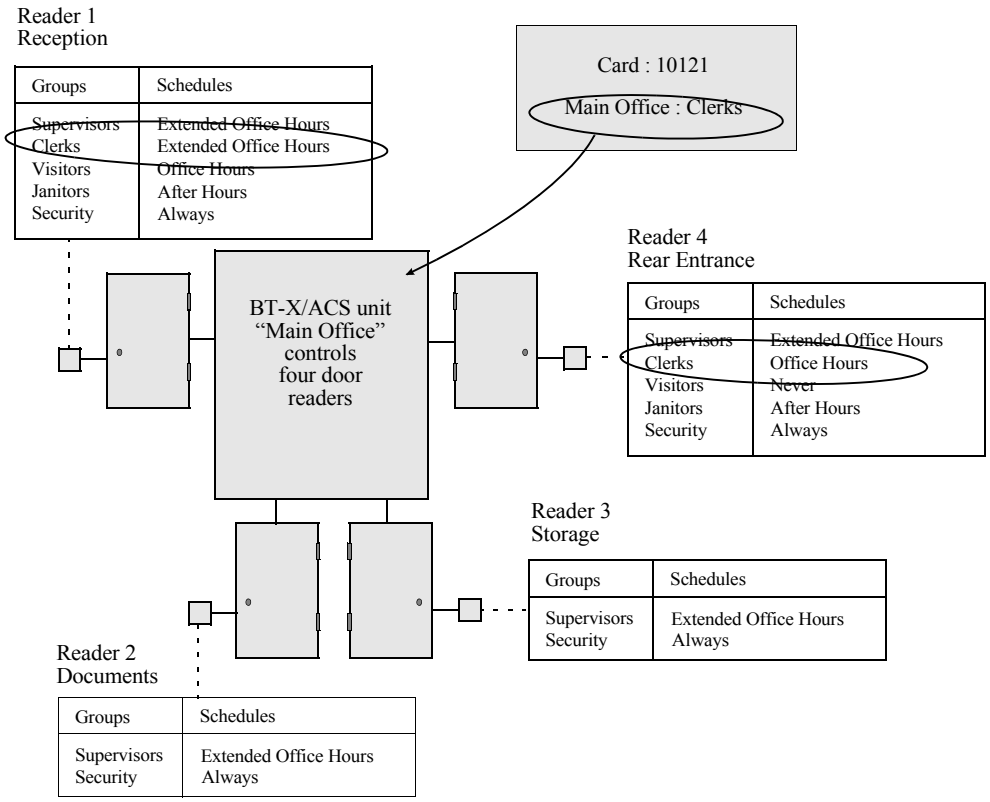
The D-21 provides access control and intrusion detection features when a D-21 Security Client is installed and running. An access control system uses card readers and keypads to grant or deny personnel access to doors at scheduled times. An intrusion detection system monitors areas for entry and exit regardless of personnel and schedule, and can use devices such as keypads for arming and disarming multiple zones. This section describes configuring and operating an access control system. For information on configuring intrusion detection, see "Configuring Intrusion Detection" on page 9-1.

Access to a reader is controlled by assigning access groups and schedules to each reader. An access group is paired with a schedule to specify when the group can use the reader to open the door. When an access card is assigned to a group, the cardholder is able to access the reader during the group's scheduled time. The card will be denied at all other times. Reader usage is logged at the D-21, and readers are monitored for forced or held open conditions, duress, invalid access requests, and tampers. Alerts are sent to the D-21 when access rules are violated.

An access card can only be assigned to one group for all the readers connected to a single BT-X remote unit. But that one group can be paired with different schedules at each reader to accommodate the access needs of different doors.

Figure 8-1 shows four readers connected to one ACS unit that is set up to control and monitor access to an office. The office has a front and rear door and two areas with higher security needs. Each reader is configured with access groups and schedules. In this example, the access groups reflect the functional groupings that use the office. Card number 10121 is assigned to the Clerks access group for the Main Office. As a member of the Clerks access group, card number 10121 only has access to Reader 1 during the Extended Office Hours schedule and Reader 4 during Office Hours.

Figure 8-1
Access control system example



Setting Up Access Control Units and Readers

To issue a card and/or PIN to personnel, ACS administrators assign the card/PIN to an access group at the BT-X/ACS unit that controls the readers the person needs to access. The cardbearer is allowed access to all readers connected to the ACS unit that have the cardbearer's access group paired with an access schedule. If the cardbearer's access group is not paired with a schedule at one of the readers attached to the unit, the card is not allowed access to that reader.

IMPORTANT *If you are assigning an access card to an ACS unit connected to a BT-X transceiver that has more than one ACS unit, and you want to assign the card to another ACS unit connected to the same BT-X, you must assign the card to the same group.*

Complete the following tasks to set up a new access control system:

- Create access groups for the entire access control system. See "Creating Access Control Groups" on page 8-4.
- Create access schedules for the entire access control system. See "Creating Access Schedules" on page 8-6.

- Add the BT-X Communicator unit. The BT-X Communicator is the unit that provides monitoring and reporting of general status conditions for the physical BT-X to which the ACS equipment is connected. See "Adding the Multi-Application BT-X" on page 6-2.
- Add a BT-X/ACS (M) unit and up to four readers to the D-21 database. The ACS unit address is used to communicate with the reader interface modules connected to the physical BT-X. See "To add a BT-X/ACS (M) application unit" on page 8-12.
- Download the database to the remote units that comprise the access control system. See "Downloading Settings to Access Control Units" on page 8-20.

Before you begin

Install and program the BT-X with ACS reader interface before configuring the access control system at the D-21. Then print the BT-X List Configuration report that shows all unit addresses required by the BT-X. See the documentation supplied with your BT-X for more information on installing, programming, and operating the unit.

Add the facilities to the database before adding the BT-X/ACS (M) remote unit. See "Facilities" on page 2-13. Before assigning cards and PINs, be sure to add the personnel to whom you want to make card assignments. See "Personnel" on page 2-85.

NOTE *If you have a large system, it may be easier to add remote units and readers first and then examine your base-wide facility usage before creating access groups and schedules. You can always add the remote units and readers, and then go back and assign groups and schedules to each reader.*

Creating Access Control Groups

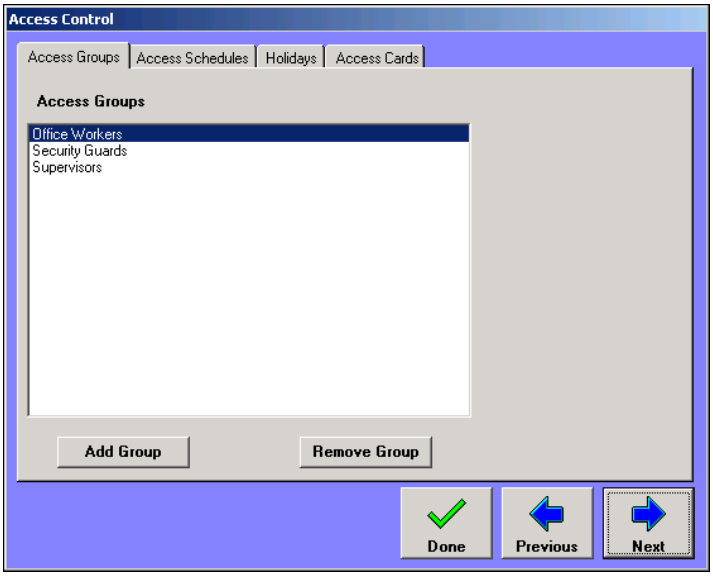
Each reader has a list of access group and schedule pairings that define when members of the group can open the reader's door using their access card. An access card is assigned to a person and then assigned to a group at an ACS unit. The card will be able to access any of the four readers on the unit where the assigned access group has been paired with a schedule.

Access groups are used system-wide. There are a total of 31 possible access groups. When you create a group, you can assign it to multiple readers throughout the access control system. Pair a group such as Clerks with different schedules to give the Clerks different access rights at different readers.

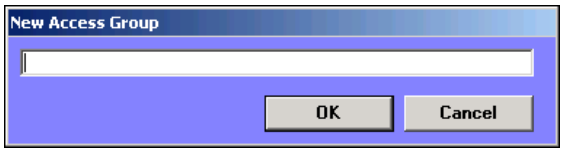
IMPORTANT *If you do not attach a schedule to a group at a particular reader, the schedule defaults to None, and cards assigned to the group are never allowed access to the reader.*

To create an access group

1 Click **Options > Access Control**. The Access Control dialog box appears.



2 Click **Add Group**. The New Access Group dialog box appears.



3 Type a name in the Access Group box.

4 Click **OK**.

5 Click **Add Group** to add another group.

6 Click **Done** when you are finished adding access groups.

To remove an access group

NOTE *You cannot delete an access group that is assigned to a reader or that has access cards assigned to it.*

1 Click **Options > Access Control**.

2 Select the Access Group you want to remove from the access group list.

3 Click **Remove Group**. A confirmation message appears.

4 Click **Yes**.

5 Click **Done**.

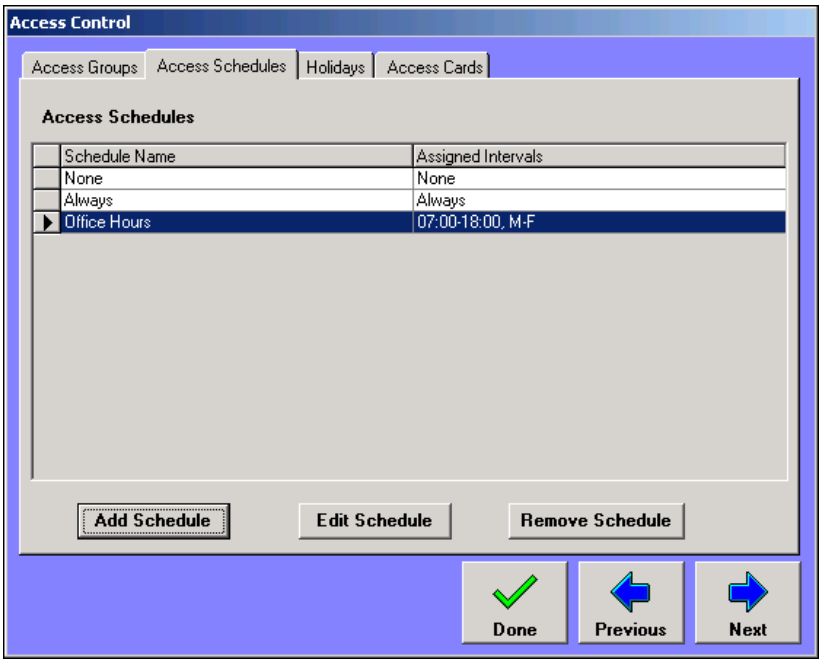
Creating Access Schedules

Access schedules, like access groups, are used globally by the entire access control system. You can define a maximum of 127 schedules, two of which are pre-defined and cannot be deleted: None and Always. The remainder are user-defined. Begin by defining the most commonly-used schedules for the most number of readers, such as office hours or visiting hours for high-traffic, common-use areas; off-hour schedules for maintenance workers, or extended office hours for supervisors. Then, use remaining schedules for special cases.

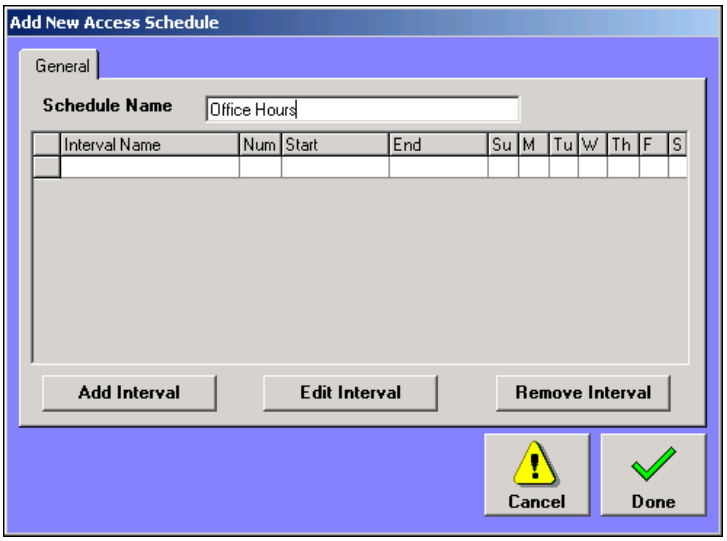
IMPORTANT *If you do not attach a schedule to a group at a particular reader, the schedule defaults to None, and cards assigned to the group are never allowed access to the reader.*

To create an access schedule

1. Click **Options > Access Control**.
2. Click the Access Schedules tab.

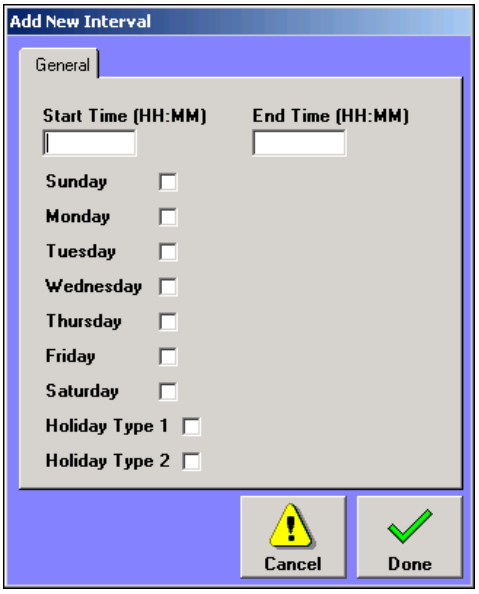


3 Click **Add Schedule**.



4 Type a name in the Schedule Name box. Use names that will help you identify the actual times.

5 Click **Add Interval**. The Add New Interval dialog box appears.



- **Start Time** The time when the interval begins. Use the 24-hour clock when entering access schedule intervals.
- **End Time** The time when the interval ends.
- **Days of the Week** The days included in the interval.

- **Holiday Types** If the interval is used to insert a holiday into the schedule, select a holiday type. For example, if you want a schedule that has shortened hours on holidays such as Thanksgiving Day and Christmas Day, add the new interval, enter the holiday-only start and end times, and click the holiday type that includes the holidays. For information on setting up holiday types, see "To create holiday types for access schedules" on page 8-8.

6 Click **Done**.

7 To enter another time interval for the schedule, click **Add Interval** again.

IMPORTANT *To create schedules that span 12 a.m., such as graveyard or night shifts, create one schedule and then add an interval for the period before midnight and an interval for the period after midnight.*

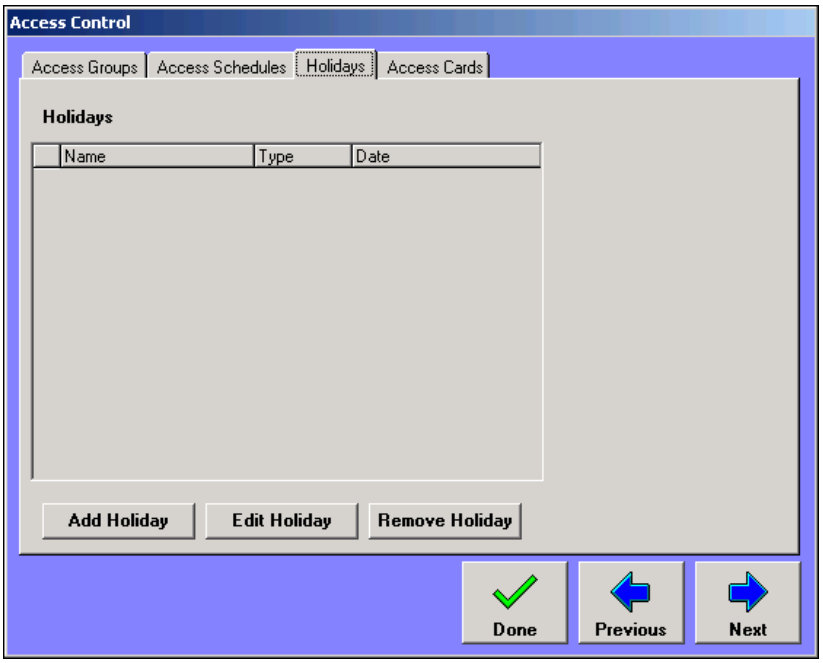
8 Click **Done** when you are finished adding intervals to the schedule.

9 Click **Done** when you are finished creating the schedule.

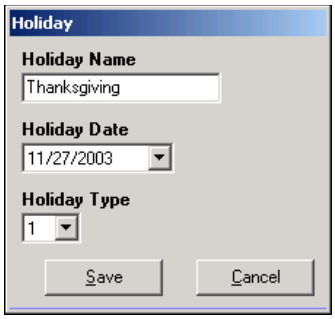
To create holiday types for access schedules

1 Click **Options > Access Control**.

2 Click the Holidays tab.



3 Click **Add Holiday**. The Holiday dialog box appears.



- **Holiday Name** Type the name of the holiday you want to include in this field.
- **Holiday Date** Select the calendar date of the holiday.
- **Holiday Type** Select which type you want to assign to this holiday. Holidays vary in the degree to which federal, state, and local authorities and businesses are open or closed. Use the two holiday types to create two different levels of holiday schedules, if necessary.

  For example, type 1 holidays could be Thanksgiving, Christmas, and New Year's Day. Type 2 holidays could be Christmas Eve, the day after Thanksgiving, Columbus Day, New Year's Eve, etc.

4 Click **Save**.

To edit an access schedule

1 Click **Options > Access Control**.
2 Click the Access Schedules tab.
3 Select the schedule you want to edit.
4 Click **Edit Schedule**. The Edit Access Schedule dialog box appears.
5 Click **Add Interval**, **Edit Interval**, or **Remove Interval**.
6 Make the changes to the schedule.
7 Click **Done**.
8 Click **Done**.

NOTE *Schedule changes will not take effect until the new schedule is downloaded to the ACS units with readers that use the edited schedule. See* *"Downloading Settings to Access Control Units" on page 8-20*.

To remove an access schedule

NOTE *You cannot delete an access schedule that is assigned to a reader. First remove the schedule from the readers where it is assigned, and then remove the schedule in the Options > Access Control dialog box. See "To edit a reader" on page 8-19.*

1. Click **Options > Access Control**.
2. Click the Access Schedules tab.
3. Select the schedule you want to remove.
4. Click **Remove Schedule**. A confirmation message appears.
5. Click **Yes**.
6. Click **Done**.

NOTE *The schedule will not be removed from the readers to which it was assigned until the edited reader schedules are downloaded to the ACS units. See "Downloading Settings to Access Control Units" on page 8-20.*

Adding a BT-X with Access Control

A BT-X connected to access control equipment, such as the AIM-4SL reader interface module, requires multiple unit addresses in the D-21 database. The first unit address is the BT-X Communicator unit. The BT-X Communicator unit provides general monitoring and reporting of the BT-X field assembly, power supply, enclosure tamper, and Central communication status. See "Adding the Multi-Application BT-X" on page 6-2 for more information.

The D-21 communicates with the access control equipment in the BT-X using the next consecutive unit address. A BT-X can be connected to up to 16 readers. A separate unit address is required for each group of four readers. Use the BT-X/ACS (M) remote unit type for each ACS unit. The D-21 receives reader status from the BT-X/ACS (M) unit and downloads access groups and schedules to the unit.

Each BT-X/ACS (M) unit supports up to four readers. If you are using the AIM-4SL, which can control up to four doors with four readers, one AIM-4SL uses one BT-X/ACS (M) unit address. If you using the AIM-1SL, which can control one reader, four AIM-1SL modules share a single BT-X/ACS (M) unit address. If the BT-X is connected to both types of reader interface modules, the unit addresses that represent AIM-4SL modules precede unit addresses for AIM-1SL modules.

The BT-X determines how many units, what type of units, and the actual unit numbers to use in the D-21 during the installation and programming of the BT-X.

IMPORTANT *Use the List Configuration report from the BT-X programming menu to configure the ACS unit addresses exactly as they were programmed at the BT-X.*

Reader Zone Status

The BT-X/ACS (M) unit type reports four status conditions for each of its four readers. The reader zones are numbered from 1 to 16. Zone numbers 1 through 4 are used to communicate status for Reader 1; zones 5 through 9 communicate status for Reader 2, and so on. The following table describes the reader status conditions and where and how they are reported to the D-21:

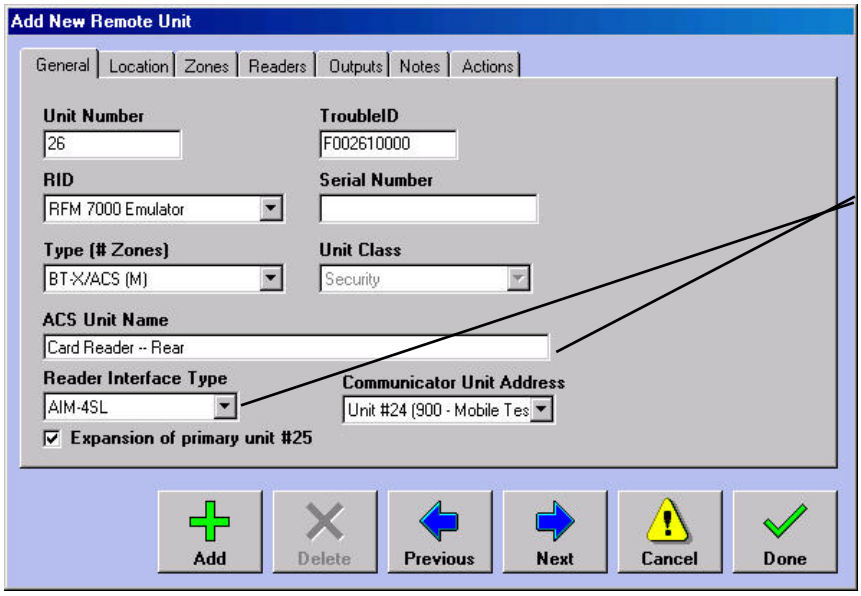
Zone conditions on a single BT-X/ACS (M) unit	Description
Held/Forced Open is reported on: Reader 1: Zone 1 Reader 2: Zone 5 Reader 3: Zone 9 Reader 4: Zone 13	Reports a Trouble (Held Open) to the D-21 when a door is held open after a valid card is presented to the reader and the door strike is activated. Held open timeouts can be set for each reader. Reports an Alarm (Forced Open) to the D-21 when a door is opened without a valid card presented to the reader.
Diddled/Duress is reported on: Reader 1: Zone 2 Reader 2: Zone 6 Reader 3: Zone 10 Reader 4: Zone 14	Reports a Trouble (Diddled) to the D-21 when an invalid card and/or PIN is presented to the reader 3 times in 5 minutes. Reports an Alarm (Duress) to the D-21 when a valid card and a duress PIN are presented to a reader. A duress PIN is created when 1 is added to the first digit of the valid PIN. For example, the normal PIN 1234 becomes duress PIN 2234. When presented with a valid card, the duress PIN opens the door and sends a duress alarm to the D-21. (If a PIN starts with 9, the duress PIN starts with 1.)
Tamper is reported on: Reader 1: Zone 3 Reader 2: Zone 7 Reader 3: Zone 11 Reader 4: Zone 15	Reports an Alarm to the D-21 when a reader interface module detects a tamper condition on itself or one of its reader devices. There is no Trouble condition for the reader Tamper input.
Auxiliary is reported on: Reader 1: Zone 4 Reader 2: Zone 8 Reader 3: Zone 12 Zone 16 (unavailable)	Reports a Trouble to the D-21 when the auxiliary input for a reader is open. Reports an Alarm to the D-21 when the auxiliary input is closed. Zone 16 on each group of 4 readers is reserved and cannot be used to report the auxiliary input on the fourth reader.

Before you begin

A multi-application BT-X with reader interface must be installed and programmed before configuring the access control system at the D-21. Print the List Configuration report, after programming the BT-X for use, when configuring the ACS unit(s) at the D-21. Then, see "To add the BT-X Communicator unit" on page 6-6 to add the BT-X Communicator unit.

To add a BT-X/ACS (M) application unit

Click **Add > Remote Unit**. The Add New Remote Unit dialog box appears.



- **Unit Number** Enter a unit number in the Unit Number box. Use the next consecutive number after the BT-X Communicator unit number. The ACS unit number you enter should match the ACS address assigned to the access control equipment when the BT-X was programmed.
- **RID** Select the same RFM 7000 RID to which you assigned the BT-X Communicator for this unit.
- **Type (# Zones)** Select BT-X/ACS (M). The ACS Unit Name and Reader Interface Type fields appear below the Type drop-down list.
- **ACS Unit Name** Enter a name for the BT-X/ACS (M) unit. This name is used to identify the unit and readers attached to this BT-X when assigning cards and PINs.
- **Reader Interface Type** Select the type of reader interface module connected to the BT-X.
- **Communicator Unit Address** Select the BT-X Communicator unit that is part of this multi-application BT-X.
- **Expansion of primary unit** This check box only appears when using the BT-X/ACS(M) and adding more than one remote unit to a site. It allows the Admin to logically group ACS units connected to the same BT-X/ACS(M) by designating the unit as an expansion of an existing unit.
- **TroubleID** For Monaco use only.
- **Serial Number** Enter the serial number for the remote unit. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class for the remote unit type. If the unit class field is enabled, you can select either Fire or Security for the unit. If the unit class field is disabled, you cannot change the unit class. See "Unit Class" on page 2-52 for more information.

1 Click the Location tab.

2 Select the facility where the ACS unit is located from the Facility drop-down list.

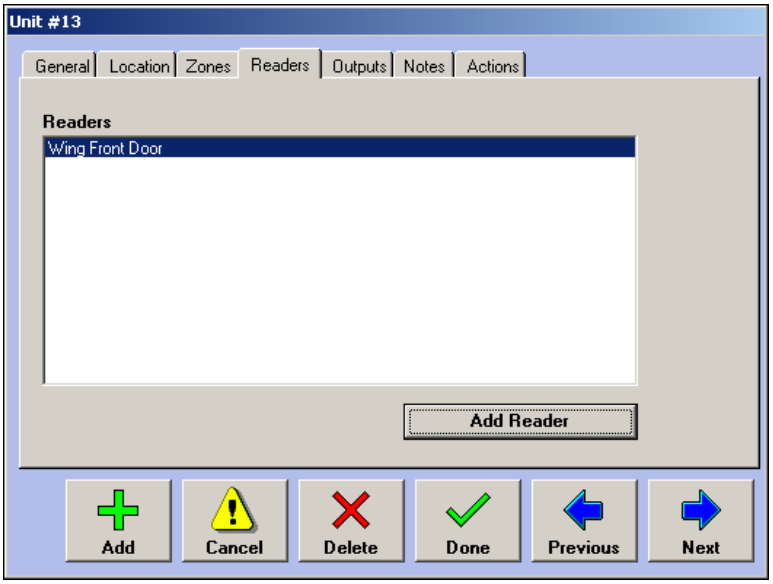
NOTE *A facility entry is required for the BT-X/ACS (M) remote unit type.*

3 Enter a description for the location of the ACS unit in the Location/Directions box.

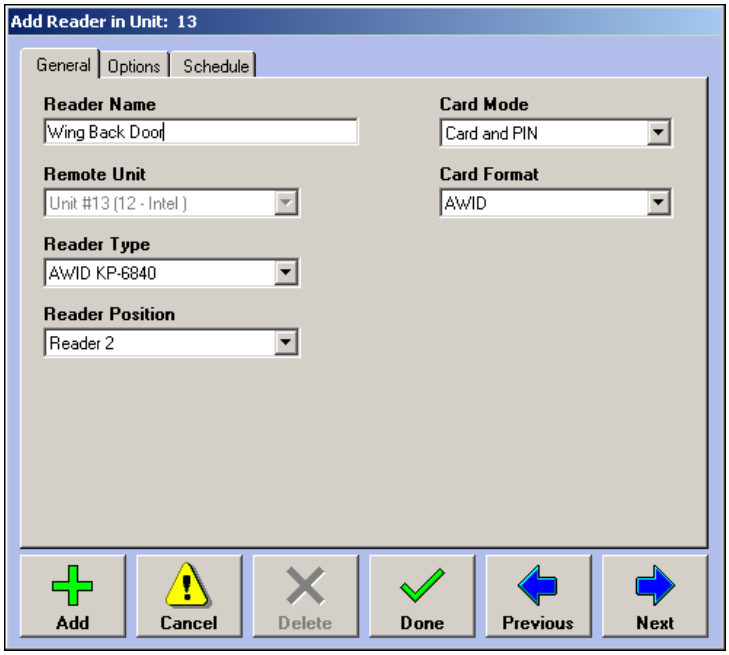
4 Click the Zones tab. The zones attached to a BT-X/ACS (M) unit are the reader zones: Held/Forced Open, Diddled/Duress, Tamper, and Auxiliary. You can automatically configure these zones when you add the readers. Use this tab for editing and viewing zone information once the zones are configured. See "Reader Zone Status" on page 8-11 for more information.

   For now, skip this tab and create the reader zones when adding the reader.

5 Click the Reader tab.



6 Click **Add Reader**. The Add Reader in Unit dialog box appears.



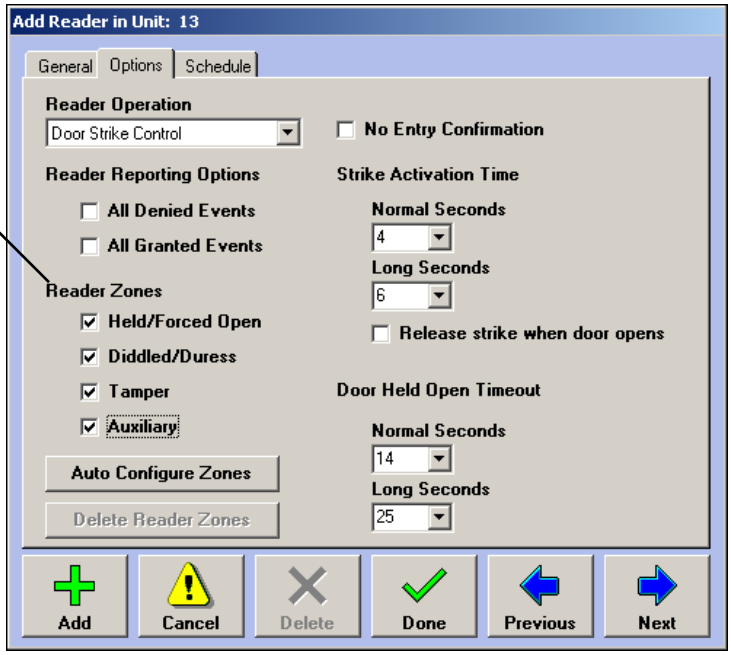
- **Reader Name** Enter a name for the reader.
- **Remote Unit** The ACS unit to which you are adding the reader.
- **Reader Type** Select the type of reader.
- **Reader Position** Select the physical position of the reader.
  - **AIM-4SL** Readers are identified by the terminal block to which it is connected on the AIM-4SL module. See the BT-X Access Control I-O-M Manual (P/N 001-398-02) for information on how the readers are numbered on the AIM-4SL.
  - **AIM-1SL** Readers are identified by the DIP switch address of the AIM-1SL. See the BT-X Access Control I-O-M Manual (P/N 001-398-02) for more information.
- **Card Mode** Select the card/PIN method used to access the reader.

Card Mode	Description
Card and PIN	Select **Card and PIN** for a door that requires both a card and PIN for access.
Card only	Select **Card only** for a door that only requires a card for access.
Card or PIN	Select **Card or PIN** for a door that requires a card or PIN but not both for access.
Inactive	Select **Inactive** to indicate a door's access control is deactivated.

- **Card Format** Select the card format associated with reader connected to the BT-X.

7 Click the Options tab.

Select the status conditions you want to report for the reader. Then click the Auto Configure Zones button to create the zones.



- **Reader Operation** Select Door Strike Control if the reader controls a door strike relay. The D-21 uses the strike activation times and door held open timeout options to determine the status of the door.
- **No Entry Confirmation** Check this box if you want to ignore the status of the door contact. Any Access Granted events will be reported as Access Granted with Entry Unconfirmed.

- **Reader Reporting Options** Select the type of information to be transmitted to the D-21. You can select one or both of the following options:
  - **All Denied Events** Any time a card or PIN is presented to a reader and denied, the event is transmitted to the D-21. Personnel and facility access activity can be viewed in the D-21 Incident Client.
  - **All Granted Events** Any time a card or PIN is presented to a reader and access is granted, the event is transmitted to the D-21. Personnel and facility access activity can be viewed in the D-21 Incident Client.

NOTE *If you only want to track events for individual cards, leave these options unchecked. Each individual card can be configured to report granted and denied events when it is assigned. See "To assign a new access card or PIN" on page 8-24.*

8 Select the zone information you want reported for the reader. Selecting a zone check box enables the reporting of the specific type of reader status to the D-21. To deactivate specific zone reporting, clear the check box. Reader zones are configured like other zones in the D-21 and can have response plans, actions, and customized alert phrases. See "Zones" on page 2-64.

NOTE *Selecting a reader zone enables* **Auto Configure Zones**. *Use this button to add the zones to the BT-X/ACS (M) zone list automatically. Unlike fire zones, reader zones are not associated with a physical terminal input in the BT-X. Reader zones are virtual zones used to report conditions based on reader device feedback and reader settings in the D-21 database.*

- **Held/Forced Open** Reports a Door Held Open trouble event to the D-21 Incident Client when a door is held open longer than the specified time. Reports a Door Forced Open alarm event to the D-21 Incident Client when a door is opened without the presentation of a valid card or PIN.
- **Diddled/Duress** Reports a Reader Diddled trouble event to the D-21 Incident Client when there are three attempts to present an invalid card or PIN to a reader. Reports a Reader Duress alarm event to the D-21 Incident Client when a special duress PIN is presented to a reader with a keypad device. Duress PINs are specified by adding one to the first digit of the PIN. For example, the duress PIN for PIN 4567 would be 5567.
- **Tamper** Reports a tamper event to the D-21 Incident Client when the reader interface module detects a tamper condition on the AIM-4SL tamper terminal or one of its reader devices. If a tamper switch is installed on the BT-X enclosure, the BT-X Communicator reports BT-X enclosure tampers.
- **Auxiliary** Reports a trouble event to the D-21 Incident Client when the auxiliary input for a reader is open. Reports an alarm event to the D-21 Incident Client when the auxiliary input is closed.

9 Click **Auto Configure Zones** to add the reader zones automatically to the database.

10 Set the door strike activation time options. The D-21 Incident Client uses the door strike settings in conjunction with reader feedback to determine the held open and forced open conditions reported on the Held/Forced Open reader zone.

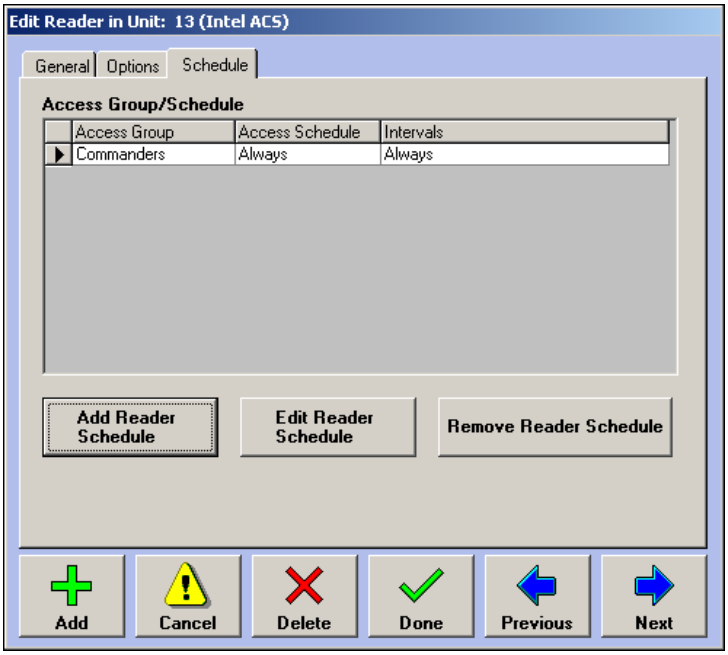
- **Normal Seconds** Select the normal strike time in seconds. This is the amount of time the door strike is not in contact before an alarm is reported to the D-21.
- **Long Seconds** Select a long strike time in seconds. Use this to specify a longer time allowed for handicap or other special needs entry.
- **Release Strike when door opens** Check this option if you want the strike to deactivate as soon as the door opens, and the door to lock as soon as the door closes. If this option is unchecked, the door strike remains active and the door remains unlocked until the strike time expires.

11 Set the door held open time options. A trouble is generated for the reader zone at the D-21 Incident Client when the held open time expires before the door closes.

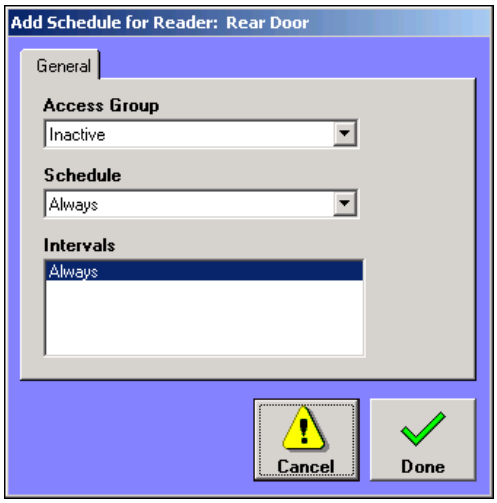
- **Normal Seconds** Select the normal held open time in seconds. This is the amount of time the door is allowed to be held open after a valid card entry.
- **Long Seconds** Select the long held open time in seconds. This is the amount of time the door is allowed to be held open for valid handicap or special needs entry.

12 Click the Schedule tab.

NOTE *You must set up access groups and schedules before you can assign them to a reader. If necessary, click* **Done**, *create access groups and schedules, and then edit the reader. See* *"Creating Access Control Groups" on page 8-4* and *"Creating Access Schedules" on page 8-6*.



13 Click **Add Reader Schedule**.



- **Access Group** Select an access group to which you want to be able to assign cards/PINs at this reader.
- **Schedule** Select a schedule for the access group. The Intervals list shows the selected schedule's time intervals. These are the times when the access group will be granted entry by the reader. Remember you can use a single schedule, such as Always, at as many readers as you want. You do not have to create a unique schedule for each reader.

14 Click **Done**. Repeat the previous three steps as many times as needed for the reader. Each time you assign an access group to a reader, it is removed from the Access Group drop-down list.

NOTE *If you do not assign an access group to a reader, the D-21 defaults the access group's schedule to None.*

---

15 When you are finished adding readers, click **Done** in the Add Reader dialog box to return to the Add Remote Unit dialog box.

16 Click the Outputs tab. If you are adding an AIM-4SL module to the database, you can add up to four outputs to this BT-X/ACS (M) unit. Outputs are not available for the AIM-1SL module. See "Outputs" on page 2-74 for how to add an output.

17 Click the Notes tab.

18 Type any notes you want saved with the remote unit.

19 Click the Actions tab.

20 Click **Add Action** to attach status change actions to the unit, if desired. For more information, see "Attaching Actions to Status Changes" on page 3-37.

21 Click **Done**.

To edit a reader

1. In the tree pane, click the plus sign (**+**) next to System. Click the plus sign next to the RFM 7000 RID associated with the BT-X/ACS (M) unit and click the plus sign next to the unit number to display the list of readers.
2. Right-click the reader you want to edit. The Edit Reader in Unit dialog box appears with the General tab showing.
   - Use the General tab to change any reader or card formats.
   - Use the Options tab to change door strike and held open timeouts, as well as which access events are reported to the D-21 Incident Client.
   - Use the Schedule tab to add or remove access groups and schedules from the reader.

NOTE *Access groups and schedules can not be removed from a reader until all related card assignments have been removed. See* *"To change an ACS unit assignment for a card or PIN" on page 8-27*.

3. Click **Done** when you are finished editing the reader.

NOTE *Reader changes will not take effect until you download them to the ACS units with the edited readers. See* *"Downloading Settings to Access Control Units" on page 8-20*.

Downloading Settings to Access Control Units

After you add BT-X/ACS (M) units, readers, and reader zones to the database and configure readers with access groups and schedules, you must download the information to the BT-X/ACS (M) unit in the field. Each unit receives the configuration for its readers from the D-21. Any changes made to the remote units or readers, and all new or changed card assignments, must be downloaded to the remote unit before the changes take effect.

See "Assigning Cards and PINs" on page 8-23 for more information on access cards.

The D-21 uses two ways to download access control settings to remote units:

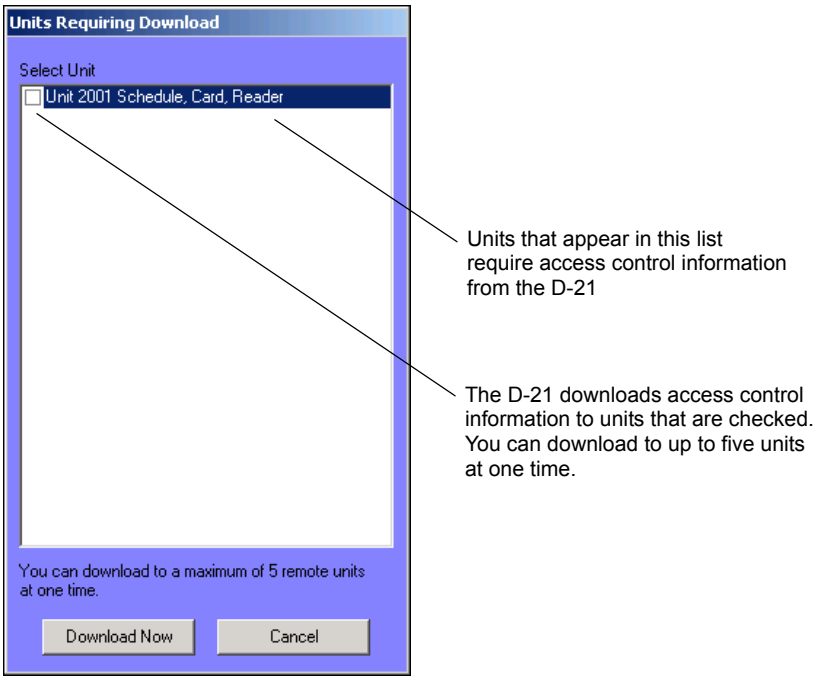
- **Partial unit configuration** The D-21 downloads all remote unit, group, schedule, card, and reader data that has changed since information was last downloaded to the ACS remote unit.
- **Entire unit configuration** The D-21 downloads all remote unit, group, schedule, card, and reader data for the ACS remote unit. Downloading entire unit configurations takes longer than downloading changes and should only be done when necessary. Use the following guidelines for downloading the entire configuration to ACS remote units:
  - If the ACS unit is new, use **Download Entire Unit Configuration** to set up the new unit.
  - If an ACS remote unit is not operating properly after attempting to update recent changes to the unit, first use **Clear Entire Unit Configuration** to erase the entire contents of the unit's configuration, then use **Download Entire Unit Configuration** to reconfigure the ACS remote unit.

NOTE *The download process can take a considerable amount of time. The reader zones report status automatically during a download. You can acknowledge the alerts during the download or after the download is complete.*

The D-21 checks the status of the RID before starting the ACS download. If the RID is disabled, in comm fail, or reporting a trouble, the D-21 generates a RID Trouble message.

To view ACS remote units that have changes to be downloaded

1. Click **Commands** and then click **Access Control**. The ACS menu commands appear.
2. Click **Show Units Requiring Download**. The Units Requiring Download dialog box appears.



NOTE *The Show Units Requiring Download command is only available if the operator who is logged in is assigned data entry level 2 in the D-21 Admin Client. For more information on setting an operator's data entry level, see* *"To add an operator" on page 2-97*.

The Units Requiring Download dialog box shows all ACS remote units that have been updated since the last time the D-21 Admin Client downloaded to them. The D-21 Admin Client compares the time stamp of the last download with the time stamps of subsequent changes to determine which ACS remote units require a download. A message indicates if there are no units requiring downloading.

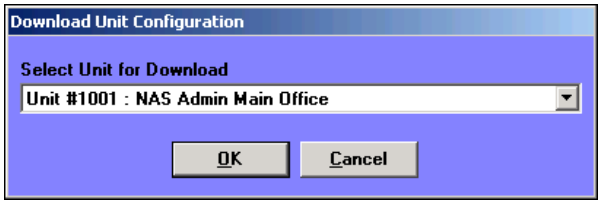
New ACS remote units that have not yet received their unit configuration from the D-21 Admin Client also appear in this list. Clicking **Download Now** downloads recent changes to existing remote units and the entire unit configuration to new units.

NOTE *This dialog box also appears when you exit the D-21 Admin Client (if there are any ACS remote units that require a download).*

To download the entire unit configuration to a new ACS remote unit

1 Click **Commands** and then click **Access Control**. The ACS menu commands appear.

2 Click **Download Entire Unit Configuration**. The Download Unit Configuration dialog box appears.



NOTE *The Download Entire Unit Configuration command is only available if the operator who is logged in is assigned data entry level 2 in the D-21 Admin Client. For more information on setting an operator's data entry level, see "To add an operator" on page 2-97.*

The Select Unit for Download drop-down list only displays ACS remote units.

3 Select the new ACS remote unit.

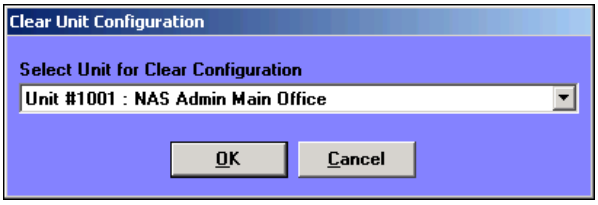
4 Click **OK**. A confirmation dialog box appears.

5 Click **OK**. A progress bar indicates the status of the downloading process.

To download the entire unit configuration to an existing ACS remote unit

1 Click **Commands** and then click **Access Control**. The ACS menu commands appear.

2 Click **Clear Entire Unit Configuration**. The Clear Unit Configuration dialog box appears.



NOTE *The Clear Entire Unit Configuration command is only available if the operator who is logged in is assigned data entry level 1 in the D-21 Admin Client. For more information on setting an operator's data entry level, see "To add an operator" on page 2-97.*

3 Select the unit to which you want to download the entire unit configuration.

NOTE *You can only clear one unit at a time.*

4 Click **Clear Unit**. A confirmation message appears.

5 Click **OK**.

6 When the remote unit configuration is cleared, click **Commands** and then click **Access Control**.

7 Click **Download Entire Unit Configuration**. The Download Unit Configuration dialog box appears.

8 Select the unit to which you want to download the entire unit configuration.

9 Click **Download Now**. A confirmation message appears.

10 Click **OK**. A progress bar indicates the status of the downloading process.

To download recent changes to one or more existing ACS remote units

1 Click **Commands** and then click **Access Control**. The ACS menu commands appear.

2 Click **Show Units Requiring Download**. The Units Requiring Download dialog box appears.

NOTE *New ACS remote units are also displayed in the Show Units Requiring Download dialog box. If a new unit is selected, the entire unit configuration is downloaded to the new unit.*

3 Select up to five remote units in the Select Units list.

4 Click **Download Now**. A confirmation message appears.

5 Click **OK**. A progress bar indicates the status of the downloading process.

Operating an Access Control System

After you add the readers to remote units and assign access group/schedule pairings to the readers, you are ready to assign cards and PINs to personnel. Card assignments must be downloaded to each remote unit before the card's assignments take effect. Use the ACS download commands to download both reader and card information to remote units. See "To download recent changes to one or more existing ACS remote units" on page 8-23.

Assigning Cards and PINs

Access cards and PINs are assigned to personnel. Administrators assign a card to a person and specify to which access group a card belongs at each ACS remote unit. The cardholder is then able to access the remote unit's readers according to the access group's schedule as it is defined at each of the readers. See Figure 8-1 on page 8-3.

IMPORTANT *If you are assigning an access card to an ACS unit connected to a BT-X transceiver that has more than one ACS unit, and you want to assign the card to another ACS unit connected to the same BT-X, you must assign the card to the same group.*

The site codes associated with pre-programmed access cards, such as HID and AWID format cards, are not used by the D-21 Security System.

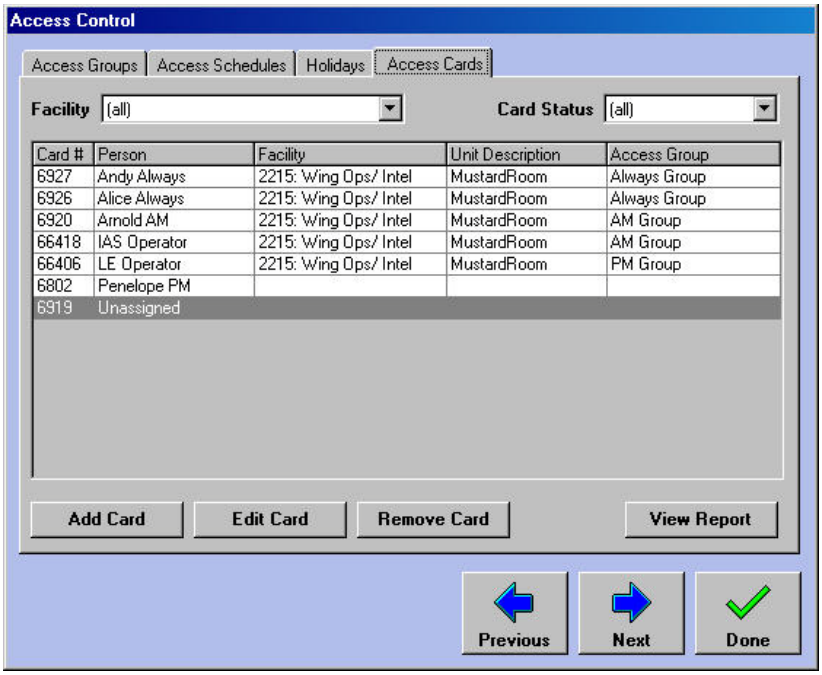
Before you begin

A person must be added to the personnel database in order to be assigned a card. For more information, see "Personnel" on page 2-85.

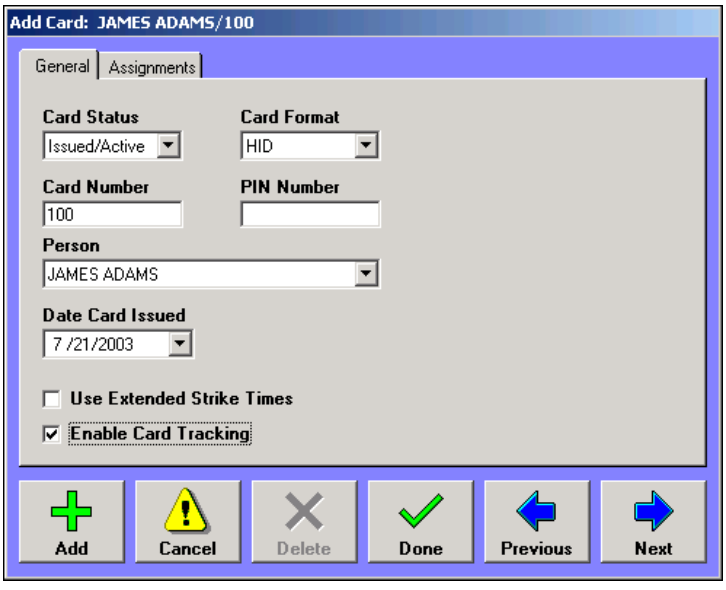
To assign a new access card or PIN

1 Click **Options > Access Control**.

2 Click the Access Cards tab.



3 Click **Add Card**.



4 Select Issued/Active in the Card Status drop-down list. The Person drop-down list is enabled.

5 Enter a card number if the card mode includes a card number.

6 Enter a PIN number if the card mode includes a PIN.

7 Select a person from the Person drop-down list. A person must be in the personnel database to appear in the list.

8 Select the card format.

9 Select an issue date for the card in the Date Card Issued drop-down calendar.

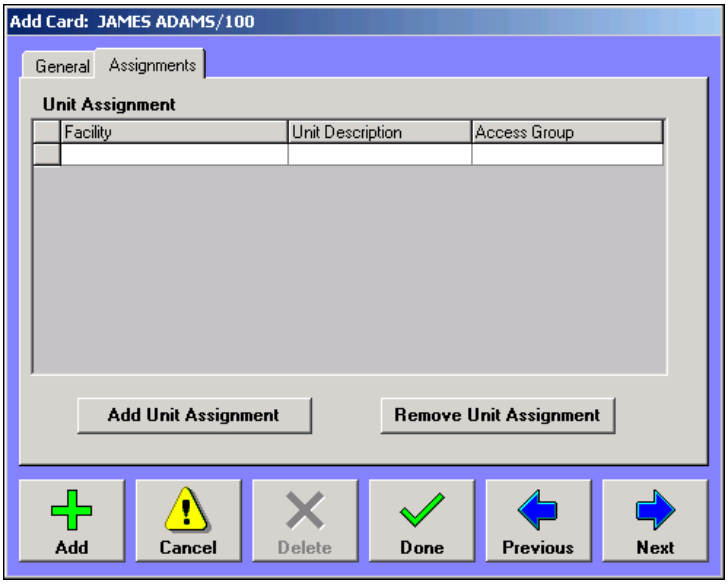
10 If the person requires longer strike times at the readers, check the Use Extended Strike Times option.

11 Select the Enable Card Tracking option if you want to track granted and denied events for this card throughout the access control system.

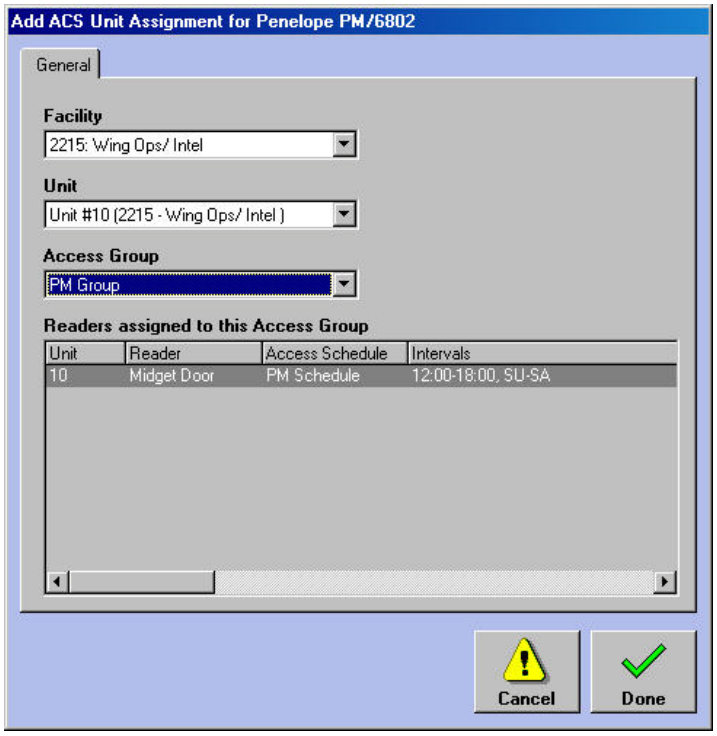
NOTE *Only check the Enable Card Tracking option if the readers do not automatically report granted and denied events to the D-21. See "To add a BT-X/ACS (M) application unit" on page 8-12 for more information on configuring readers.*

---

12 Click the Assignments tab.



13 Click **Add Unit Assignment**. The Add ACS Unit Assignment dialog box appears.



14 Select the facility to which the remote unit is associated in the Facility drop-down list.

15 Select the ACS unit in the Unit drop-down list.

NOTE *Cards are assigned to a remote unit. Cards cannot be assigned to individual readers. Cards are given the access privileges for the selected group at all readers at the selected unit.*

---

16 Select the access group for the card. The reader list updates to show the group's assignments for each reader attached to the ACS remote unit.

17 Click **Done**.

18 Download the new card assignments to the ACS remote units. See "To download recent changes to one or more existing ACS remote units" on page 8-23 for information on downloading new cards and changes to existing cards to ACS remote units.

NOTE *Cards will not be able to access the readers to which they are assigned until you download the changes to the ACS remote units.*

To remove an access card

NOTE *Only delete an access card if the card has been destroyed. Unassign a card that is no longer in use so it can be reassigned. See "To reassign an inactive card" on page 8-29.*

1 Click **Options > Access Control** and click the Access Cards tab.
2 Select the card you want to remove.
3 Click **Unassign Card**. A confirmation message appears.
4 Click **Yes**.
5 On the Access Cards tab, click the Show Unassigned option to display all unassigned and inactive cards.
6 Select the card you want to remove.
7 Click **Remove Card**. A confirmation message appears.
8 Click **Yes**.
9 Download the card change to the ACS remote units. See "To download recent changes to one or more existing ACS remote units" on page 8-23 for information on downloading new cards and changes to existing cards to ACS remote units.

NOTE *The card will continue to have access to its unit assignments until you download the changes to the ACS remote units.*

Changing Card Assignments

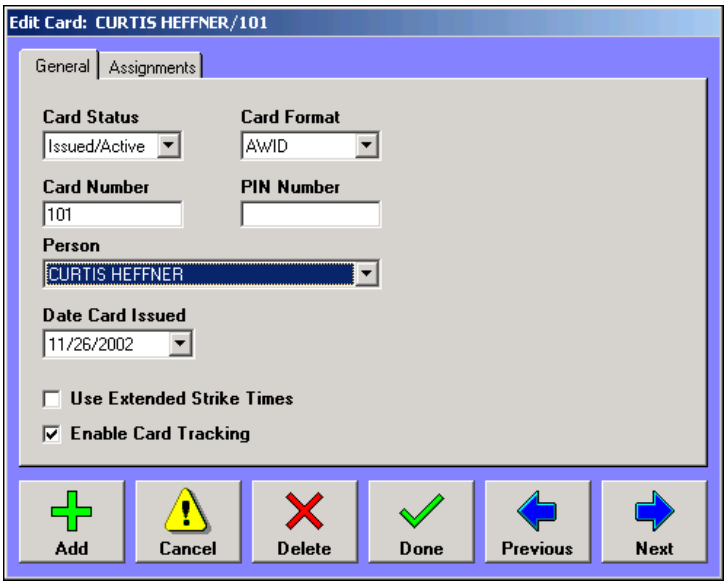
You may need to change a card's access group assignments due to promotion, demotion, changes in security clearances, etc. To change a card's access group assignments, you must edit the ACS unit assignments for each ACS unit to which the card is assigned.

You can also reassign cards to other personnel, and deactivate and reactivate cards while retaining all person and unit assignments.

To change an ACS unit assignment for a card or PIN

1 Click **Options > Access Control**.
2 Click the Access Cards tab.
3 Select a card in the list.

4 Click **Edit Card**.



5 Make changes to the card.

- Use the General tab to change the person's assignment, PIN, strike time options, or card tracking options.
- Use the Assignments tab to add or remove unit assignments for the card.
- To change the access group for an existing ACS unit assignment, you must remove the unit assignment and then add a new unit assignment with the new access group.

6 Click **Done** when you are finished editing the card.

7 Click **Done** in the Access Control dialog box when you are finished editing cards.

8 Download the card status change to the ACS remote units. See "To download recent changes to one or more existing ACS remote units" on page 8-23 for information on downloading new cards and changes to existing cards to ACS remote units.

To deactivate an access card or PIN

1 Click **Options > Access Control** and click the Access Cards tab.

2 Select a card in the list.

3 Click **Unassign Card**. A confirmation message appears.

4 Click **Yes**. The card status changes to Unissued/Inactive and the Person field displays Unassigned. To view cards that are not currently assigned to personnel, click the Show Unassigned option on the Access Cards tab.

5 Download the card status change to the ACS remote units. See "To download recent changes to one or more existing ACS remote units" on page 8-23 for information on downloading new cards and changes to existing cards to ACS remote units.

To reassign an inactive card

1. Click **Options > Access Control** and click the Access Cards tab.
2. Click the Show Unassigned option.
3. Select the inactive card you want to assign.
4. Click **Edit Card**.
5. Select Issued/Active from the Card Status list.
6. Make changes to the card.
   - Use the General tab to change the person assignment, PIN, strike time options, or card tracking options.
   - Use the Assignments tab to add or remove unit assignments for the card.
7. Click **Done** when you are finished editing the card.
8. Click **Done** in the Access Control dialog box when you are finished editing cards.
9. Download the card status change to the ACS remote units. See "To download recent changes to one or more existing ACS remote units" on page 8-23 for information on downloading new cards and changes to existing cards to ACS remote units.

Tracking Card Usage

Use the D-21 Incident Client to track the usage of active cards as well as lost/missing and stolen cards presented to readers.

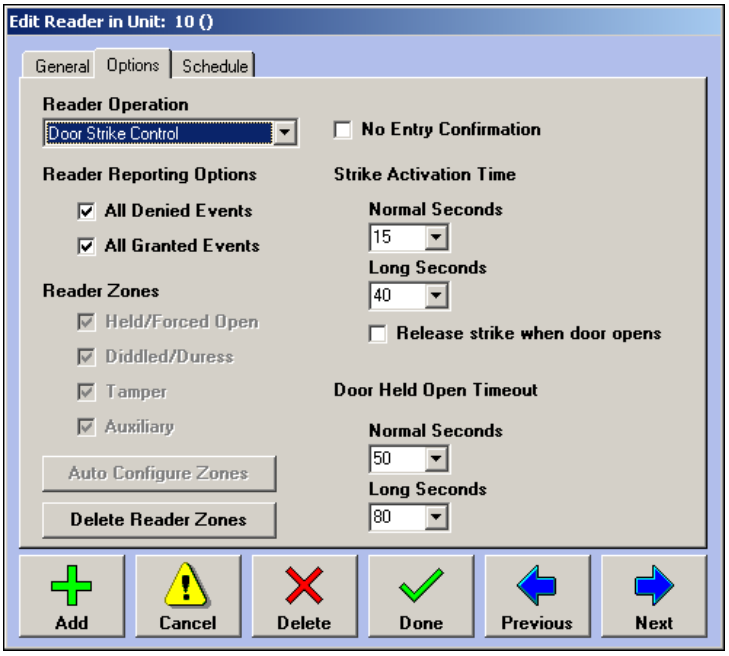
Tracking Active Cards

Tracking active cards can be configured per reader or per card. A reader can be configured to send all Denied events, all Granted events, or all events to the D-21 Incident Client. Denied events are sent to the D-21 as alarms. Granted events are sent to the D-21 as non-alarms with a lower priority than troubles. If you want to track cards on a card-by-card basis, select the Enable Card Tracking option when assigning the card. Each time the card is presented at a reader, the time, unit, and status (Denied or Granted) are recorded in the D-21 log and in the Facility Access and Personnel Access Views in the D-21 Incident Client.

To track all cards presented at an existing reader

NOTE *See "To add a BT-X/ACS (M) application unit" on page 8-12 for information on setting up ACS units and readers.*

1. Click the plus sign (**+**) next to the unit number of the BT-X/ACS (M) unit to which the reader is attached.
2. Right-click the reader. The Edit Reader dialog box appears.
3. Click the Options tab.



4 Select the reader reporting options you want.

- **All Denied Events** Every time a card is denied access, the event is transmitted to the D-21 Incident Client as an alarm condition.
- **All Granted Events** Every time a card is granted access, the event is transmitted to the D-21 Incident Client as a non-alarm condition with a priority lower than a unit trouble.

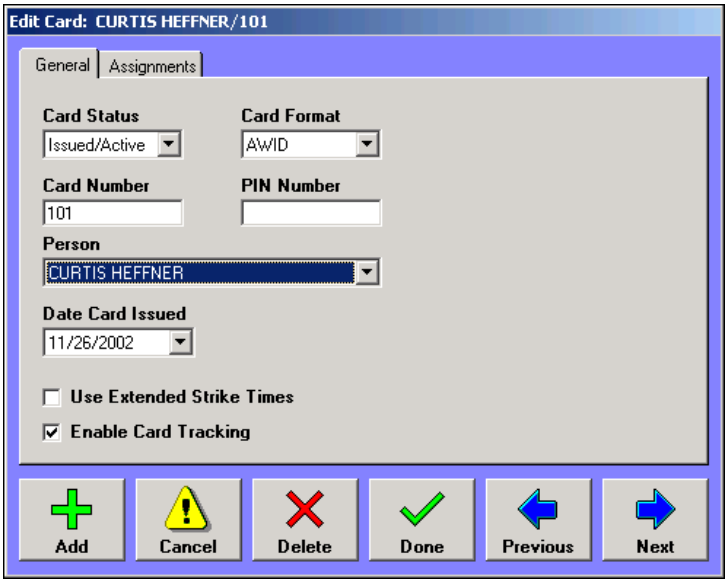
NOTE *All tracked card activity can be viewed in the Facility Access and Personnel Access Views in the D-21 Incident Client.*

To track one card at all readers

NOTE *If all readers are configured to report denied and granted events, selecting the Enable Card Tracking option for an individual card will not change how the D-21 tracks the card. All card events are logged in the D-21 log and reported to the D-21 Incident Client.*

1 Click **Options > Access Control** and click the Access Cards tab.

2 Click **Edit Card**. The Edit Card dialog box appears.



3 Select the Enable Card Tracking option.

4 Click **Done**.

Tracking Lost or Stolen Cards

When an active card is reported lost, missing, or stolen, you can either deactivate the card and no longer track its use, or you can keep the card active and track where it is presented in an attempt to recover the card.

To record a card lost or stolen and deactivate it

1. Click **Options > Access Control** and click the Access Cards tab.
2. Select the card you want to record as lost or stolen.
3. Click **Edit Card**.
4. Select Lost/Missing or Stolen in the Card Status drop-down list.
5. Click the Assignments tab.
6. Select all the card's unit assignments.
7. Click **Remove Unit Assignment**. The unit assignments are changed to Inactive until the next time the units involved receive a download. After the next successful download, the inactive unit assignments will be removed.

To record a card lost or stolen and track it

NOTE *If you change a card's status to lost or stolen and do not change the unit assignments, the card can still be granted access to its assigned unit readers. To prevent access and track the attempted usage of a lost or stolen card, create an access group (such as No Access) and assign the access group to "None" at all readers. See "To create an access group" on page 8-5. Then assign the lost or stolen card to the "no access" group and to the "None schedule" at all readers.*

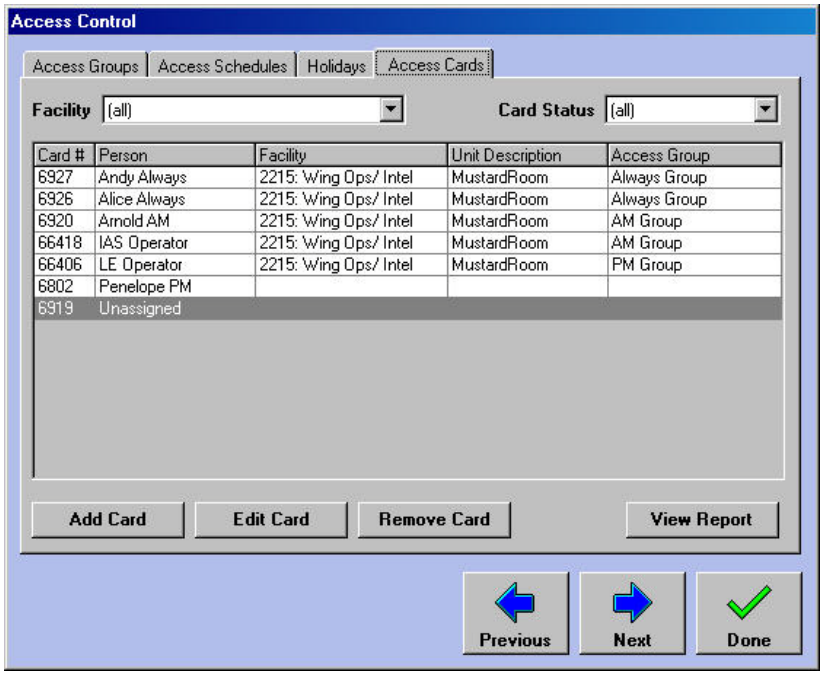
1. Click **Options > Access Control** and click the Access Cards tab.
2. Select the card you want to record as lost or stolen.
3. Click **Edit Card**.
4. Select Lost/Missing or Stolen in the Card Status drop-down list.

5 Assign the card to an active access group using the None access schedule for each unit assignment.

NOTE *If the card is presented to any of the readers where the card is assigned to the "no access" group, the D-21 operator will receive a card denied alert that also indicates the card is lost or stolen.*

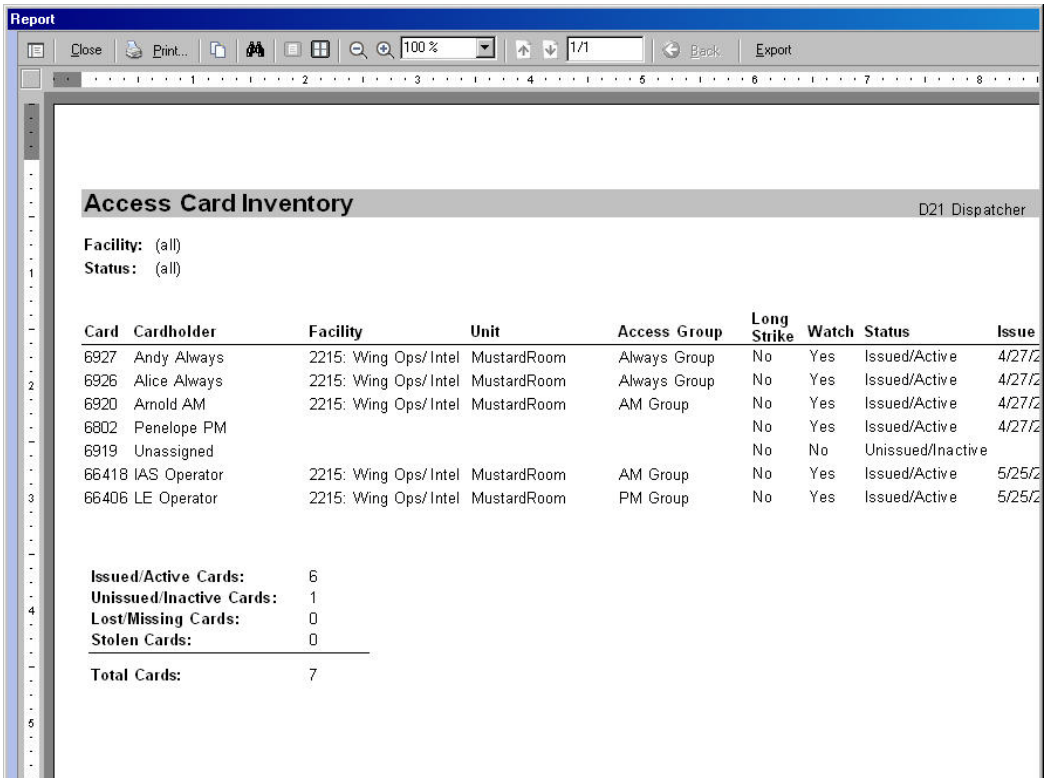
To print a card inventory report

1 Click **Options** > **Access Control** and click the Access Card tab.



2 Use the **Facility** and **Card Status** drop-down lists to define the cards included in the card inventory report.

3 Click **View Report**. A preview of the report is displayed in a separate window.



4 Click **Print** to print the report.

5 Click **Close** to close the print preview window.

6 Click **Done** to close the Access Control dialog box.

Section 9
Configuring Intrusion Detection

Read this section to learn how to configure remote units for intrusion detection using the D-21 Security Client.

Contents

Overview of Intrusion Detection 9-2
Setting Up the BT2-8S Security Unit 9-2
- BT2-8S Zone Types 9-3
- Master Control Zones on the BT2-8S 9-4

Setting Up the BT-X Security Unit 9-11
- BT-XS Zone Types 9-11
- Master Zones on the BT-XS 9-12
- Adding a BT-X with Intrusion Detection 9-14

IDS iButton and PIN Assignments 9-24
- Enrolling Administrators 9-25
- Enrolling Users 9-29
- Managing iButtons 9-37
- Downloading iButton Authentications 9-43

Overview of Intrusion Detection

The D-21 provides intrusion detection features when a D-21 Security Client is installed and running. Intrusion detection monitors areas for entry and exit regardless of personnel privileges and building schedules, and can use devices such as keypads to arm and disarm one or more zone.

Remote units, such as the BT2-8S and the BT-X, can be connected to intrusion detection devices, such as motion sensors, and configured to monitor security zones within a facility. Other devices, such as push-to-exit buttons and keypads, can be used in addition to sensor devices to provide controlled access to secured areas. Each zone is configured with a zone type that specifies the rules the remote unit and the D-21 use to determine the status of the zone.

In addition to monitoring single zones for status changes, the BT2-8S and the BT-X provide Master zones that can be associated with one or more Automatic zone. When a Master zone changes state, all Automatic zones associated with it change to that state. For example, if a Master zone changes to Access, all Automatic zones associated with it change to Access. When the Master zone returns to Secure, the Automatic zones return to Secure.

This section covers the configuration of the following remote unit types:

- **BT2-8S** Configures a BT2-8S 16-zone security remote unit or a 32-zone BT2-8S (a master and slave unit in one enclosure).
- **BT2-8S-MC** Configures a BT2-8S with the ability to use master control and automatic zones.
- **BT-XS** Configures the legacy BT-XS.
- **BT-XS (M)** Configures a multi-application BT-X with intrusion detection.

For more information on D-21 remote unit types, see “Remote Units” on page 2-51.

Setting Up the BT2-8S Security Unit

The BT2-8S is a 16-zone security transceiver that communicates with the D-21 using an RFM 7000 RID. Use the BT2-8S remote unit type to configure this unit. If the BT2-8S is capable of providing master control and automatic zones, use the BT2-8S-MC remote unit to configure the unit. For more information on the installation and programming of the BT2-8S, see the BT2-8S I-O-M Manual (P/N 001-256-00).

IMPORTANT *Older BT2-8S transceivers require the BT2-8S Master Control Upgrade Kit (P/N 227-273-00) to provide master control and automatic zones. Newer BT2-8S units provide this functionality. See the documentation provided with your BT2-8S unit to determine if it supports master control and automatic zones.*

The procedure for adding the BT2-8S and the BT2-8S-MC remote unit types are the same except where noted.

BT2-8S Zone Types

This table lists the zone types available with the BT2-8S. Refer to the BT2-8S I-O-M Manual (P/N 001-256-00) for information on how to wire the following zone types:

BT2-8S Zone Types	Description
Central Initiate	Operators at the D-21 Central control whether the zone is in an Access or Secure condition; there is no access/secure switch at the protected area. If the zone is set to Access, security alarms are not reported to the Central. Security alarms are only reported when the zone is set to Secure.
Central Initiate NT*	Operates like Central Initiate, except conditions that normally cause a Tamper Alarm cause a Security Alarm.
Two Man Access/Secure	When a zone operates in this mode, the zone has an access/secure device located outside the protected area, such as a card reader or iButton, that can be used for local zone access. Status changes are reported to the Central where an operator can accept or deny the change. If the operator denies the change, a security alarm is generated.
Two Man Access/Secure NT*	Operates like Two Man Access/Secure, except conditions that normally cause a Tamper Alarm cause a Security Alarm.
Entry/Exit Delay	The zone is paired with an access/secure switch located inside the protected area. A delay time of 10 to 80 seconds is specified (in 10-second increments) during which a person must physically set the switch to avoid triggering an alarm. On entry, the switch must be set to Access by the end of the delay time or an alarm is reported to the Central. On exit, the switch is set to Secure and the area must be properly cleared by the end of the delay time or an alarm is reported to Central. If you select Entry/Exit Delay, enter a delay time.
Entry/Exit Delay NT*	Operates like Entry/Exit Delay, except that conditions that normally cause a Tamper Alarm cause a Security Alarm.
Constant Secure	When a zone operates in this mode, it cannot be placed in Access. After an alarm has been acknowledged by Central, the zone automatically returns to Secure.
Constant Secure NT*	Operates like Constant Secure, except that conditions that normally cause a Tamper Alarm cause a Security Alarm.
Automatic*	Zones defined as Automatic change to Access or Secure when their master control zone changes to Access or Secure. Zone 1 controls Automatic zones between zone 2 and 8; if zone 9 is defined as anything other than Automatic, Constant Secure, or (none), it controls the Automatic zones between 10 and 16.
Automatic NT*	Operates like Automatic, except conditions that normally cause a Tamper Alarm cause a Security Alarm.
*Only available with the BT2-8S-MC zone type	

Master Control Zones on the BT2-8S

The BT2-8S supports the use of two master control zones. Use the BT2-8S-MC remote unit type when configuring a BT2-8S with master control zones.

- **One master control zone** Use zone 1 to control all zones between 2 and 16 that are defined as Automatic or Automatic [NT]. Zone 1 can be configured as any zone type except Constant Secure or Automatic when used as a master control zone. If zone 1 controls any Automatic zones above zone 9, zone 9 must be configured as Not in Use, Automatic, Automatic [NT], or Constant Secure.
- **Two master control zones** Zone 1 controls all zones between 2 and 8 defined as Automatic or Automatic [NT]. Zone 9 controls all Automatic zones between 10 and 16. When used as master control zones, zones 1 and 9 can be defined as any zone type except Constant Secure or Automatic.

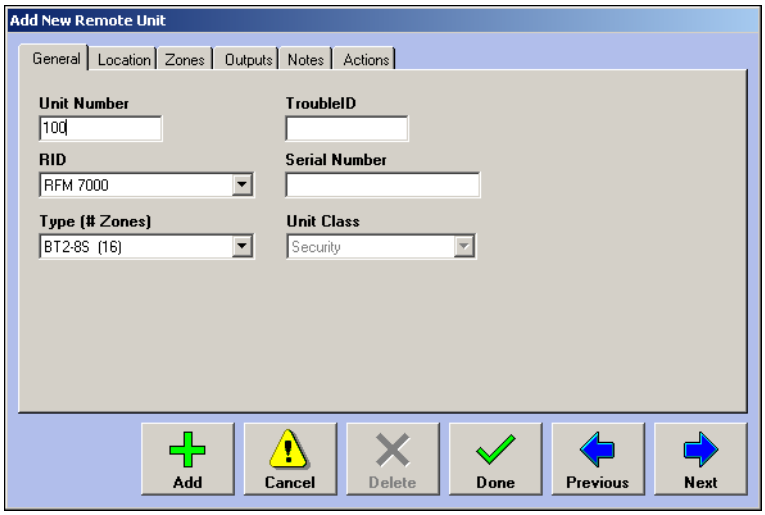
IMPORTANT *If you want to use zone 1 or zone 9 as master control zones, they cannot be defined as Constant Secure or Automatic.*

Before you begin

Be sure you already added the remote interface driver (RID) that will act as the communications link between the D-21 and the BT2-8S. See "Remote Interface Drivers (RIDs)" on page 2-30 for more information on adding RIDs.

To add a BT2-8S security remote unit

1 Click **Add > Remote Unit**. The Add New Remote Unit dialog box appears.



- **Unit Number** Enter a number between 1 and 2046. All unit numbers attached to a specific RID must be unique.
- **RID** Select the RFM 7000 RID handling the communication between the D-21 and the remote unit.
- **Type** Select the BT2-8S(16) or BT2-8S-MC depending on how the remote unit is wired. For more information, see the BT2-8S I-O-M Manual (P/N 001-256-00) provided with your BT2-8S transceiver.
- **Trouble ID** For Monaco use only.

- **Serial Number** Enter the serial number for the remote unit hardware. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class (Security) for these remote unit types. It is not possible to change the unit class for these remote unit types. See "Unit Class" on page 2-52 for more information.

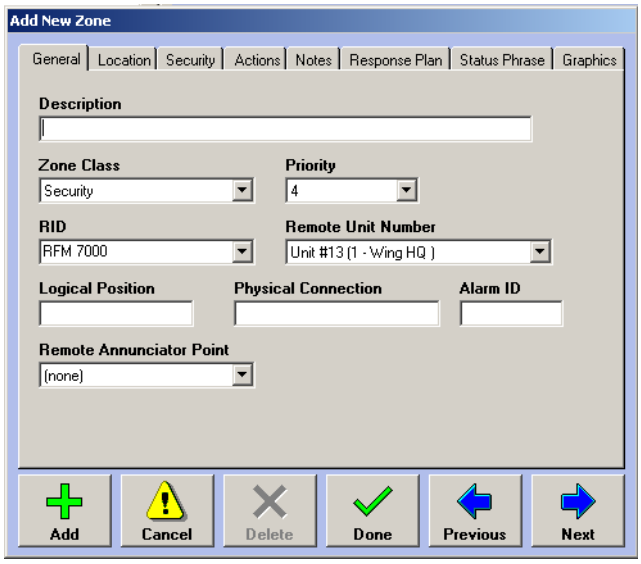
2 Click **Next** to advance to the Location tab.

3 Enter a facility and any directions to describe the position of the unit.

4 Click **Next** to advance to the Zones tab.

5 Click **Add Zone** to add the security zones to the D-21 database.

NOTE *The configuration process must be performed for each zone on the security remote unit.*



- **Description** Identifies the zone throughout the D-21 system.
- **Zone Class** The default zone class for a BT2-8S is Security, but BT2-8S zones can also be configured as Fire. Security zones report Security Alarms, Tamper Alarms, Access, and Secure conditions and can be viewed in the D-21 Incident Client Security Status View. BT2-8S fire zones report Alarms, Troubles, and Normal conditions, and can be viewed in the Fire Status View. For more information, see "Zone Class" on page 2-64.

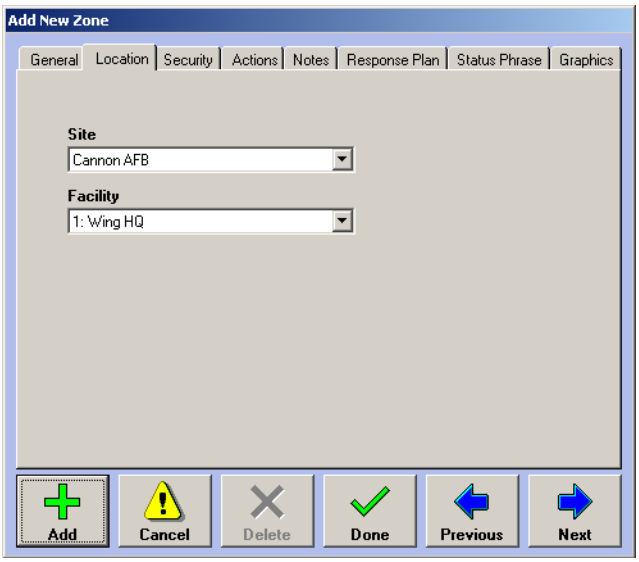
  If the zone class is defined as Fire, Fire Auxiliary, or Security Auxiliary, the security zone type is set automatically to Constant Secure and the Security tab is not available.
- **Priority** Determines the order in which a buffered alert is presented by the D-21 Incident Client. For more information, see "Zone Priority" on page 2-65.
- **RID** The RID the zone and remote unit use to communicate with the D-21.
- **Remote Unit Number** The unit number for the remote unit to which the zone is attached. Only remote units associated with the selected RID appear in the drop-down list.

- **Logical Position** Identifies the number of the remote unit terminal to which the zone is connected. The system uses the logical position to identify the source of an alert associated with a zone. See "Master Control Zones on the BT2-8S" on page 9-4 for information on configuring zone 1 and zone 9.
- **Physical Connection** Describes the physical location of the zone in the facility.

NOTE *The Alarm ID option is currently not in use.*

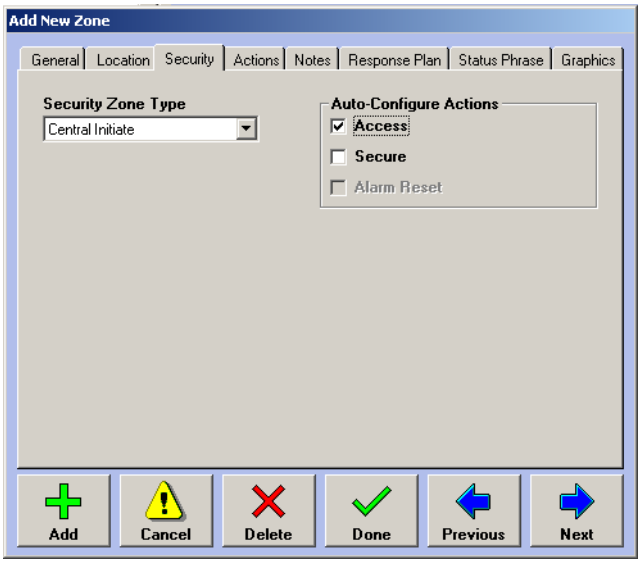
- **Remote Annunciator Point** Identifies a position on a remote annunciator panel where the zone status will be displayed. For more information on setting up remote annunciators, see the D-21 Remote Interface Driver Guide (P/N 001-399-01).

6 Click **Next** to advance to the Location tab.



- **Site** If necessary, select the Site from the drop-down list.
- **Facility** If necessary, select the Facility from the drop-down list. This value identifies the facility in which the zone is located, which may or may not be the same as the unit's facility. If the desired facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See "To add a facility" on page 2-13.

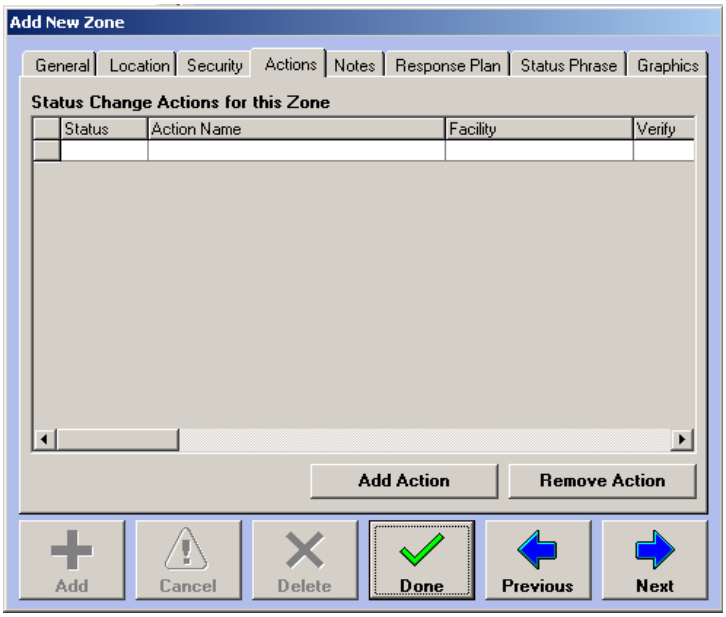
7 Click **Next** to advance to the Security tab.



- **Security Zone Type** Select the security zone type for the zone. See "BT2-8S Zone Types" on page 9-3 for more information.
- **Auto Configure Actions** Generates actions that can be used for this zone in D-21 response plans, scheduled actions, and status changes. The D-21 automatically creates the following actions for security zones:

Action	Description
Access	Created for Central Initiate zones. Access action can be used to manually change the zone status to Access.
Secure	Created for Central Initiate zones. Secure action is used to manually change the zone status to Secure.
Alarm Reset	Created for Constant Secure, Automatic, Pre-Authorized, Two Man Access/Secure, and Entry/Exit Delay zones. Alarm Reset action can be used to manually normalize the zone status.

8 Click **Next** to advance to the Actions tab.



- **Status Change Actions for this Zone** Lists the actions that are run when this zone changes to the indicated state.
- **Add Action** Adds another status change action to the list of actions assigned to this zone.
- **Remove Action** Deletes the status change action from the list of actions assigned to this zone.

NOTE *For more information on working with actions, see "Actions" on page 3-27.*

9 Click **Next** to advance to the Notes tab.

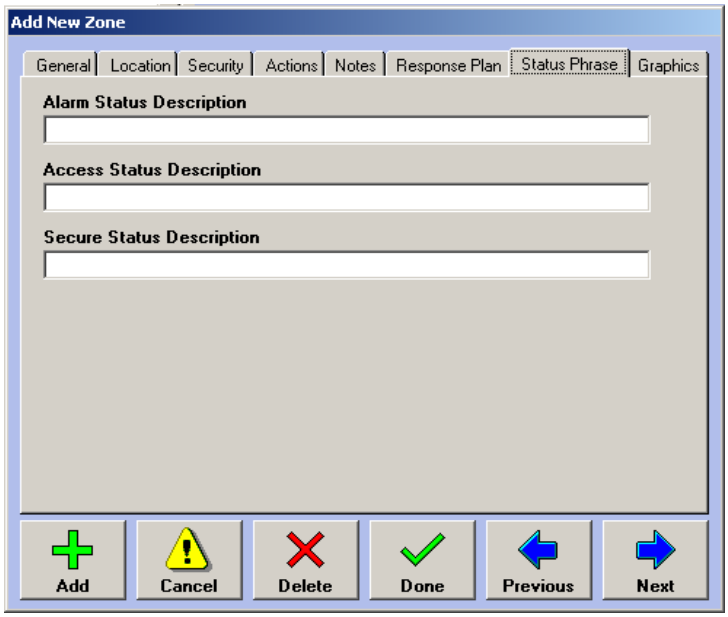
10 Enter the desired text in the Notes and Alert Notes textboxes.

11 Click **Next** to advance to the Response Plan tab.

12 Click **Add Response Plan** to display the Response dialog box. For information on using the Response dialog box, see "Response Plans" on page 3-2.

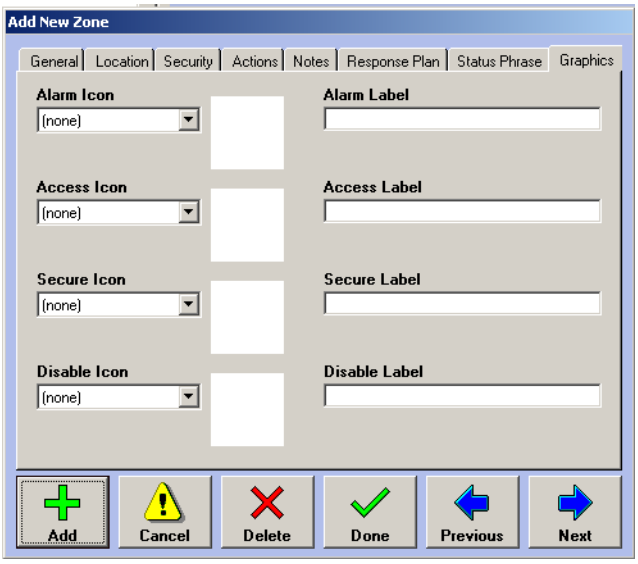
NOTE *Once the zone has a response plan, the Add Response Plan button is dimmed, and the Remove Response Plan and Edit Response Plan buttons are active.*

13 Click **Next** to advance to the Status Phrase tab.



- **Alarm Status Description** Enter the text you want to appear in alerts and in status fields in the D-21 Incident Client when the zone reports an alarm.
- **Access Status Description** Enter the text you want to appear in alerts and in status fields in the D-21 Incident Client when the zone reports an Access or access request.
- **Secure Status Description** Enter the text you want to appear in alerts and in status fields in the D-21 Incident Client when the zone reports a Secure or secure request.

14 Click **Next** to advance to the Graphics tab.



- **Alarm Status Icon** The graphic and label displayed on a graphic or floor plan when the zone is in alarm. See "Icons" on page 5-12.
- **Access Icon\Label** The graphic and label displayed on a graphic or floor plan when the zone is in Access. See "Icons" on page 5-12.
- **Secure Status Icon** The graphic and label displayed on a graphic or floor plan when the zone is in Secure. See "Icons" on page 5-12.
- **Disable Status Icon** The graphic and label displayed on a graphic or floor plan when the zone is disabled. See "Icons" on page 5-12.
- **Preview** Displays the graphic selected in the Status Icon drop-down lists.

15 Click **Done** to add the zone to the D-21 database.

IMPORTANT *You must download information to the BT2-8S in order to enable correct operation of the zones. Download to the BT2-8S unit from the D-21 Incident Client Security Commands pane. For more information, see the D-21 Incident Client User Guide (P/N 001-392-00).*

16 Once zones have been added, add Outputs, Notes, and Actions as desired.

Setting Up the BT-X Security Unit

Use the BT-XS (M) remote unit type to configure IDS application units in a multi-application BT-X with program chip P/N 325-304-00 revision B.8 or higher. For more information on the multi-application BT-X, see "Adding the Multi-Application BT-X" on page 6-2. If you are configuring an older, legacy BT-XS transceiver with a program chip lower than B.8, use the BT-XS remote unit type.

The configuration of the Master zones and onboard zones varies depending on which program chip is installed in your BT-X:

- **Revision B.8 or higher** The BT-XS (M) remote unit type supports up to twelve Master zones associated with keypads or access/secure keyswitches. The four BT-X onboard zones are added to the BT-X Communicator unit.
- **Revisions before B.8** The BT-XS remote unit type supports the four BT-X onboard zones for use with access/secure keyswitches and eight Master zones. The legacy BT-XS does not require a BT-X Communicator remote unit.

Both unit types must be flagged as an IDS Master unit, or left unflagged to be configured as IDS application units. Both unit types reserve zone positions 13 through 16 for communication status with the D-21 when the IDS Master unit option is flagged.

BT-XS Zone Types

The following table lists the zone types available with the legacy BT-XS and BT-XS (M) remote unit types:

BT-XS Zone Types	Description
Automatic*	When a Master zone changes state (from Secure to Access or from Access to Secure), the Automatic zones associated with the Master zone also change to that state. Automatic zones can be flagged as Entry/Exit Delay so the sensors wired to the Automatic zone can be shunted for the Entry/Exit delay time set for the Master zone. Automatic zones can also be flagged as Trigger zones for a Master zone via the BT-X programming menus. For more information on working with Master and Automatic zones, see the BT-X Intrusion Detection Installation Manual (P/N 001-398-01) and the BT-X Intrusion Detection Programming Guide (P/N 001-398-05).
Central Initiate	Operators at the D-21 Central control whether the zone is in Access or Secure; there is no access/secure switch at the protected area. If the zone is set to Access, security alarms are not reported to the Central. Security alarms are only reported when the zone is Secure.
Constant Secure*	Zone can only be Secure or Alarm. Depending on the latching configuration of the zone, the zone status may or may not automatically return to Secure when the zone normalizes.
Entry/Exit Delay	The zone is paired with an arm/disarm device, such as a keypad or access/secure keyswitch, located inside the protected area. A delay time of 10 to 80 seconds is specified (in 10-second increments) during which a person must disarm the zones in the area to avoid triggering an alarm. On entry, the user must disarm the zones by the end of the delay time or an alarm is reported to the Central. On exit, the user must arm the zones and the area must be properly cleared by the end of the delay time or an alarm is reported to Central. If you select Entry/Exit Delay, enter a delay time.
Keyswitch*	This zone type is only available on the BT-XS (M) unit type. Use it for a physical zone input wired to an access/secure key switch that is associated with a Master zone on the IDS Master unit. Key switch zones behave the same way as Constant Secure zones: they are always Secure or Alarm.

BT-XS Zone Types	Description
Pre-Authorized	Zone status changes are logged and used to update zone status on graphics, floor plans, and status views, but the D-21 does not display any access or secure requests for processing by an operator.
Pre-Authorized EE	This zone type is the same as Pre-Authorized except the zone can be configured with an Entry/Exit Delay timer.
Two Man Access/Secure	Designed for zones that have an arm/disarm device located outside the protected area, such as a keypad or iButton, that can be used for local zone access. Status changes are reported to the D-21 where an operator can accept or deny the change. If the operator denies the change, a security alarm is generated.

Master Zones on the BT-XS

Master zones are used to control the status of Automatic zones. When a Master zone changes state, the Automatic zones associated with it also change state. Master zones can be configured as Central Initiate, Two-Man Access/Secure, Entry/Exit, Pre-Authorized, and Pre-Authorized EE. If an entry or exit delay timer is used in conjunction with the Master zone, the delay timer is configured and downloaded to the IDS Master unit from the D-21. All Master zones are added to the IDS Master unit.

A single Master zone can be associated with multiple Automatic zones regardless of their location on the physical zone cards in the BT-X. If there are multiple Automatic zones on a single security zone card, all the Automatic zones must be associated with the same Master zone on the IDS Master unit.

IMPORTANT *Print the List Configuration report after programming the Master and Automatic zones at the BT-X to aid in adding these zones to the D-21 database.*

IDS Master Units

The IDS Master unit is not a physical unit or set of security zone cards. It is a “virtual” unit created via programming at the BT-X and at the D-21. When you program a security zone card at the BT-X, the BT-X automatically adds one extra unit address for the IDS Master unit. Add IDS Master units and Master zones to the D-21 database the same way you add “real” security units and zones to the database. See “To add an IDS application unit” on page 9-21.

IMPORTANT *The IDS Master unit on the BT-XS remote unit type (legacy) supports four onboard access/secure keyswitch zones (positions 1 through 4) and eight Master zones (zones 5 through 12). Zones 13 through 16 are reserved for communication status.*

Zones 13-16 on the IDS Master Unit are reserved for communicating the status of the BT-XS unit to the D-21. Add the following zones to the D-21 database when you add the IDS Master unit:

Zone	Use zone type	Description
13	Constant Secure	Used for primary communication fallback to secondary communication. Do not add this zone if the BT-XS you are configuring only uses one communication method. See "Configuring Dual Communication Channels" on page 6-4 for more information.
14	Constant Secure	Used to report a zone card communication failure between the BT-X and a security card.
15	Constant Secure	Used to report a communication failure between the keypads connected to the BT-X and the BT-X.
16	Constant Secure	Used to report a bad database at the BT-XS.

Setting Up BT-X Keypads

BT-X Keypads and BT-X iButton Keypads are associated with Master zones at the BT-X. One or more keypads can be used to control the status of associated Automatic zones connected to physical zone inputs on the security zone cards.

When you add a Master zone to the IDS Master unit, use the Keypad Master Zone check box on the Security tab in the Zones dialog box to specify the Master zone is controlled by a keypad. When this option is checked, the following rules apply to the Master zone and its associated Automatic zones:

- Security alarms for the Master zone are reported as Keypad Duress at the D-21. Associated Automatic zones remain in their current state and do not change to Secure.
- Tamper alarms for the Master zone are reported as Keypad Tamper at the D-21. Associated Automatic zones remain in their current state and do not change to Secure.

NOTE *If the Keypad Master Zone check box is not selected, Security and Tamper alarms on the Master zones force the Automatic zones to change status along with their associated Master zones.*

For more information on working with the BT-X iButton Keypad, see the BT-X iButton Keypad I-O-M Manual (P/N 001-428-00). For more information on the BT-X Keypad, see the BT-X Keypad I-O-M Manual (P/N 001-434-00).

Adding a BT-X with Intrusion Detection

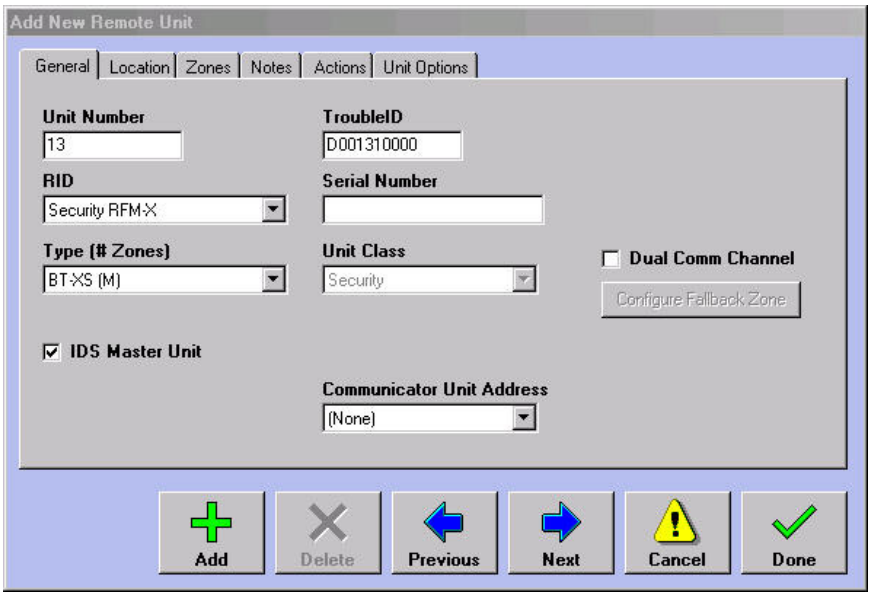
Complete the following tasks to configure a multi-application BT-X for intrusion detection. If you are working with a legacy BT-XS model, you do not need to configure the BT-X Communicator unit.

IMPORTANT *Use the List Configuration report from the BT-X programming to configure the remote units exactly as they were programmed at the BT-X.*

- Add the BT-X Communicator unit. See "Adding the Multi-Application BT-X" on page 6-2.
- Add the IDS Master unit and Master zones. See "To add an IDS Master unit" on page 9-14 or "To add an IDS Master unit with iButton keypad control" on page 9-18.
- Add a BT-XS (M) remote unit for each group of up to four security zone cards. Use "To add an IDS application unit" on page 9-21.

To add an IDS Master unit

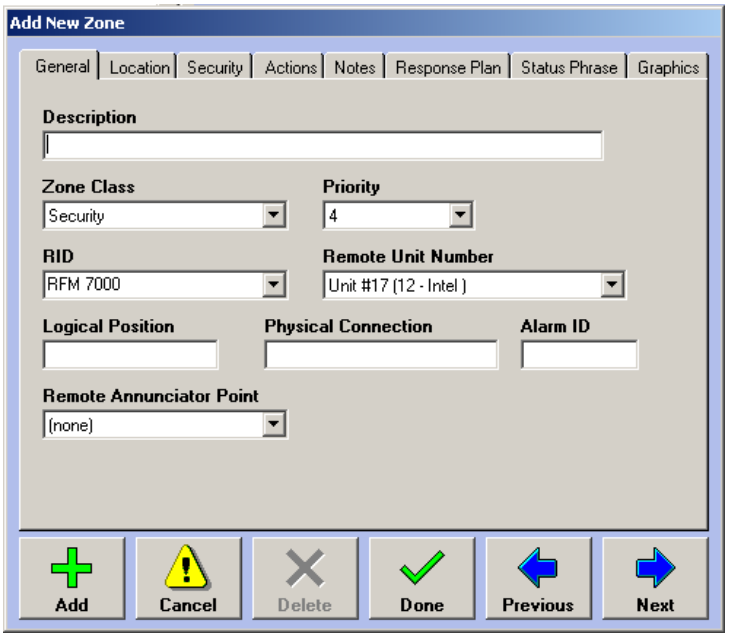
1 Select **Add > Remote Unit**. The Add New Remote Unit dialog box appears.



- **Unit Number** Enter the number assigned to the IDS Master unit at the BT-X. The unit numbers entered in the D-21 must match the unit addresses programmed into the BT-X.
- **RID** Select the RFM 7000 RID handling communication between the D-21 and the BT-X.
- **Type** Select the BT-XS (M) remote unit type if you are working with a multi-application BT-X (program chip revision B.8 or higher). Select the BT-XS remote unit type if the program chip is revision B.8 or lower.
- **IDS Master Unit** Check this box to flag the unit as an IDS Master unit. Add all Master zones to this unit number.
- **Communicator Unit Address** Select the BT-X Communicator unit that is part of this multi-application BT-X.

- **TroubleID** For Monaco use only.
- **Serial Number** Enter the serial number of the remote unit. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class (Security) for these remote unit types. It is not possible to change the unit class for these remote unit types. See "Unit Class" on page 2-52 for more information.
- **Dual Comm Channel** Check this box if this unit is configured to report dual communication channel status in the BT-X programming menus. For more information, see "Configuring Dual Communication Channels" on page 6-4.

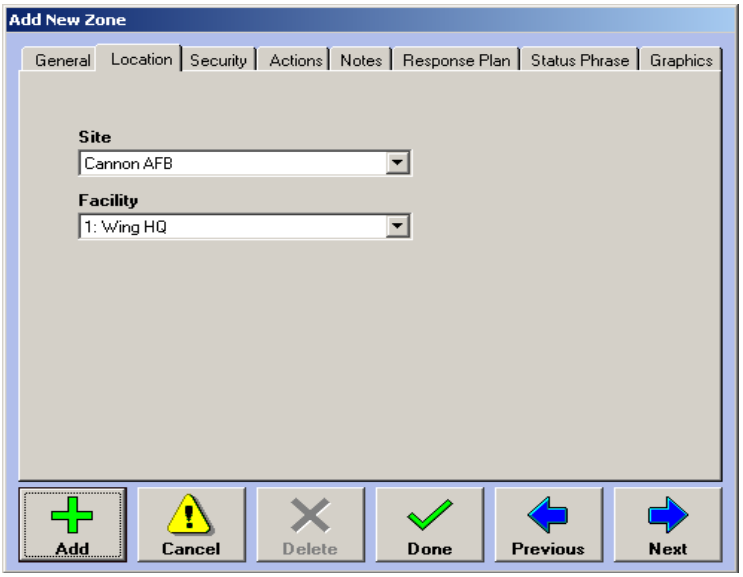
2. Click **Next** to advance to the Location tab.
3. Enter a facility and any directions to describe the position of the remote unit.
4. Click **Next** to advance to the Zones tab.
5. Click **Add Zone** to add each Master zone to the D-21 database. The Add New Zone dialog box appears.



- **Description** Enter a name identifying the Master zone throughout the D-21 system.
- **Logical Position** Enter the zone number assigned to the Master zone at the BT-X.

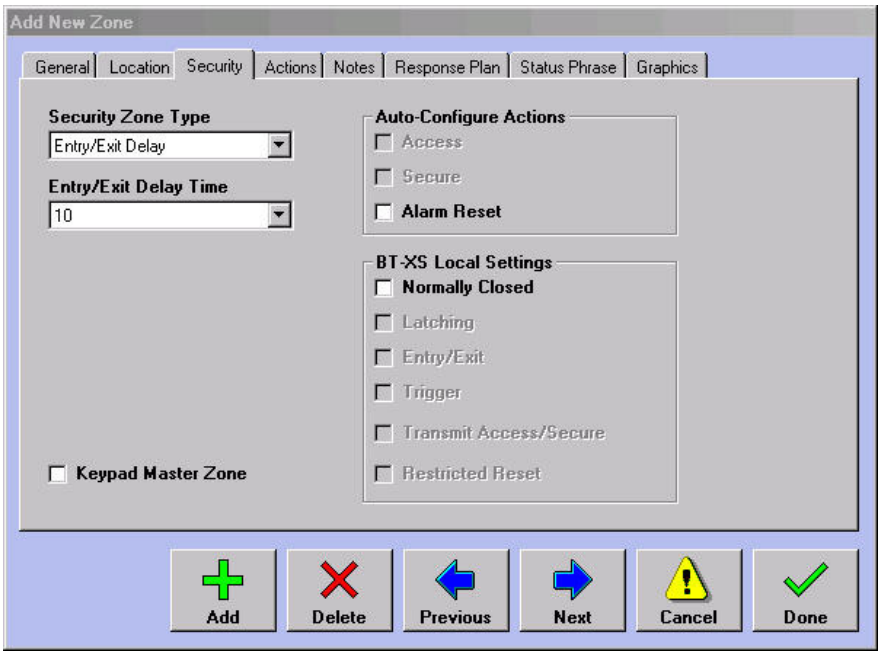
For information on other fields on this tab, see "Zones" on page 2-64.

6 Click **Next** to advance to the Location tab.



- **Site** Select the Site from the drop-down list.
- **Facility** Select the Facility from the drop-down list. Identifies the facility in which the zone is located. If the desired facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See "To add a facility" on page 2-13.

7 Click **Next** to advance to the Security tab.



- **Security Zone Type** Select the zone type you want to assign to this Master zone.
- **Keypad Master Zone** Select this option if there is one or more keypads associated with the Master zone. See "Setting Up BT-X Keypads" on page 9-13.

- **Auto Configure Actions** Select the commands for which you would like to create an action. These actions can be assigned to status changes for RIDs, remote units, and zones throughout the D-21. For more information on using actions, see "Actions" on page 3-27. The D-21 can automatically create the following actions for security zones:

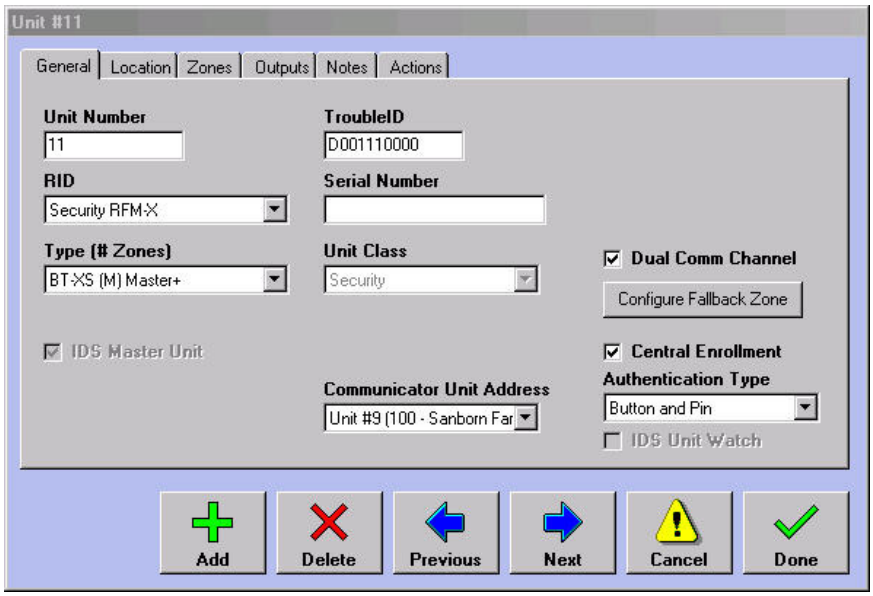
Action	Description
Access	Created for Central Initiate zones. Access action can be used to manually change the zone status to Access.
Secure	Created for Central Initiate zones. Secure action is used to manually change the zone status to Secure.
Alarm Reset	Created for Constant Secure, Automatic, Pre-Authorized, Two Man Access/Secure, and Entry/Exit Delay zones. Alarm Reset action can be used to manually normalize the zone status.

- **BT-XS Local Settings** Use the check boxes in this area to record the zone options programmed at the BT-X. Only settings that apply to the selected zone type are enabled. These options are only for record-keeping purposes and do not control any behavior at the BT-X.

8 See "Zones" on page 2-64 for more information on adding actions, notes, response plans, and status phrases to this zone.

To add an IDS Master unit with iButton keypad control

1 Select **Add > Remote Unit**. The Add New Remote Unit dialog box appears.



- **Unit Number** Enter the number assigned to the IDS Master unit at the BT-X. The unit numbers entered in the D-21 must match the unit addresses programmed into the BT-X.
- **RID** Select the RFM 7000 RID handling communication between the D-21 and BT-X.
- **Type** Select the BT-XS (M) Master+ remote unit type.

NOTE *An IDS Master unit of this type requires BT-X chipset C.2 or higher.*

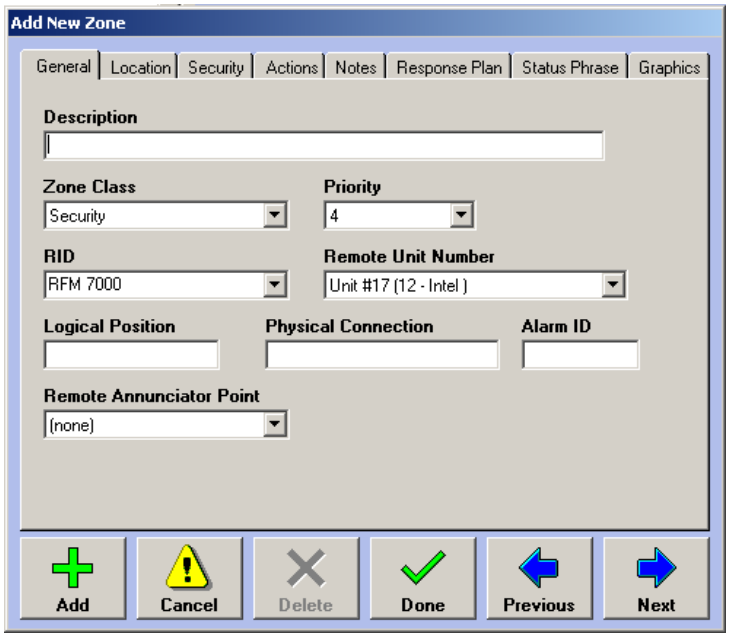
- **IDS Master Unit** Check this box to flag the unit as an IDS Master unit. Add all Master zones to this unit number.
- **Communicator Unit Address** Select the BT-X Communicator unit that is part of this multi-application BT-X.
- **TroubleID** For Monaco use only.
- **Serial Number** Enter the serial number of the remote unit. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class (security) for these remote unit types. It is not possible to change the unit class for this remote unit type. See "Unit Class" on page 2-52 for more information.
- **Dual Comm Channel** Check this box if this unit is configured to report dual communication channel status in the BT-X programming menus. For more information, see "Configuring Dual Communication Channels" on page 6-4.
- **Central Enrollment** Check this box if this unit will use Central Enrollment to manage iButton users. See "IDS iButton and PIN Assignments" on page 9-24.
- **Authentication Type** Select Button and PIN if users will present an iButton at the keypad and enter a PIN to gain entry. Select PIN Only if users will not present an iButton.

2 Click **Next** to advance to the Location tab.

3 Enter a facility and any directions to describe the position of the remote unit.

4 Click **Next** to advance to the Zones tab.

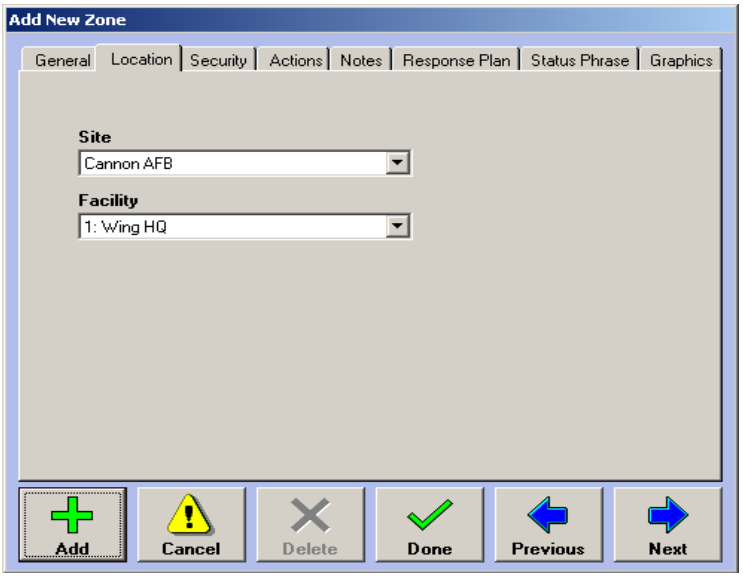
5 Click **Add Zone** to add each Master zone to the D-21 database. The Add New Zone dialog box appears.



- **Description** Enter a name identifying the Master zone throughout the D-21 system.
- **Logical Position** Enter the zone number assigned to the Master zone at the BT-X.

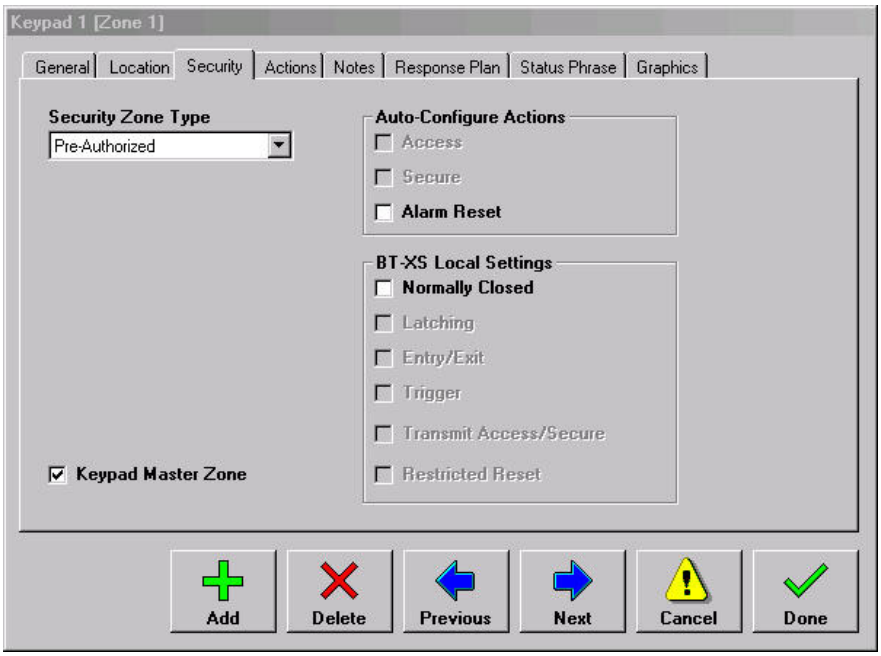
For information on other fields on this tab, see "Zones" on page 2-64.

6 Click **Next** to advance to the Location tab.



- **Site** Select the Site from the drop-down list.
- **Facility** Select the Facility, where the zone is located, from the drop-down list. If the desired facility does not appear in the drop-down list, make a note to return to this dialog box after the facility has been added to the database. See "To add a facility" on page 2-13.

7 Click **Next** to advance to the Security tab.



- **Security Zone Type** Select the zone type you want to assign to the Master zone.

- **Keypad Master Zone** Select this option if there is one or more keypad associated with the Master zone. See "Setting Up BT-X Keypads" on page 9-13.
- **Auto Configure Actions** Select the commands for which you would like to create an action. These actions can be assigned to status changes for RIDs, remote units, and zones throughout the D-21. For more information on using actions, see "Actions" on page 3-27. The D-21 can automatically create the following actions for security zones:

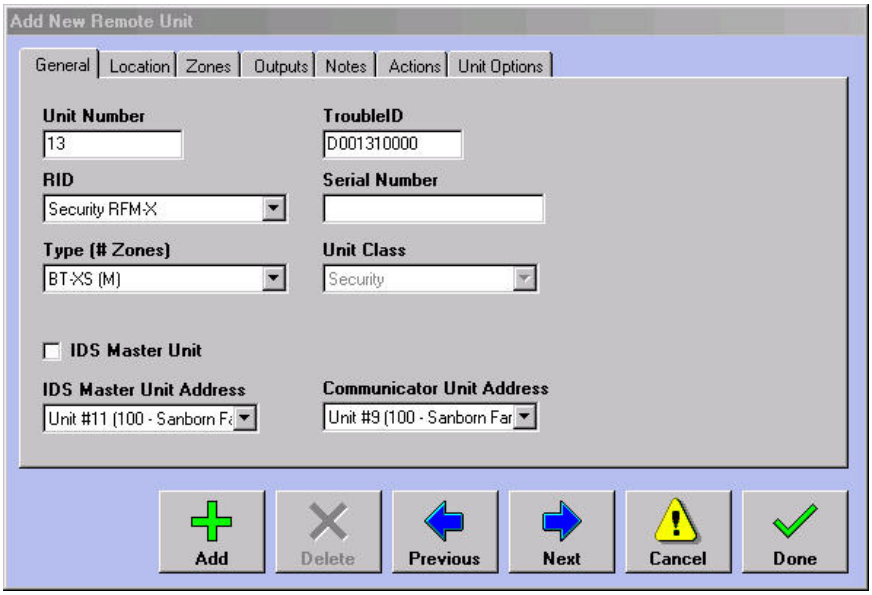
Action	Description
Access	Created for Central Initiate zones. Access action can be used to manually change the zone status to Access.
Secure	Created for Central Initiate zones. Secure action is used to manually change the zone status to Secure.
Alarm Reset	Created for Constant Secure, Automatic, Pre-Authorized, Two Man Access/Secure, and Entry/Exit Delay zones. Alarm Reset action can be used to manually normalize the zone status.

- **BT-XS Local Settings** Use the check boxes in this area to record the zone options programmed at the BT-X. Only settings that apply to the selected zone type are enabled. These options are only for record-keeping purposes and do not control any behavior at the BT-X.

8 See "Zones" on page 2-64 for more information on adding actions, notes, response plans, and status phrases to this zone.

To add an IDS application unit

1 Select **Add > Remote Unit**. The Add New Remote Unit dialog box appears.



- **Unit Number** Enter the number assigned to the unit at the BT-X. The unit numbers you enter in the D-21 must match the unit addresses programmed into the BT-X.
- **RID** Select the RFM 7000 RID that handles the communication between the D-21 and the BT-X.

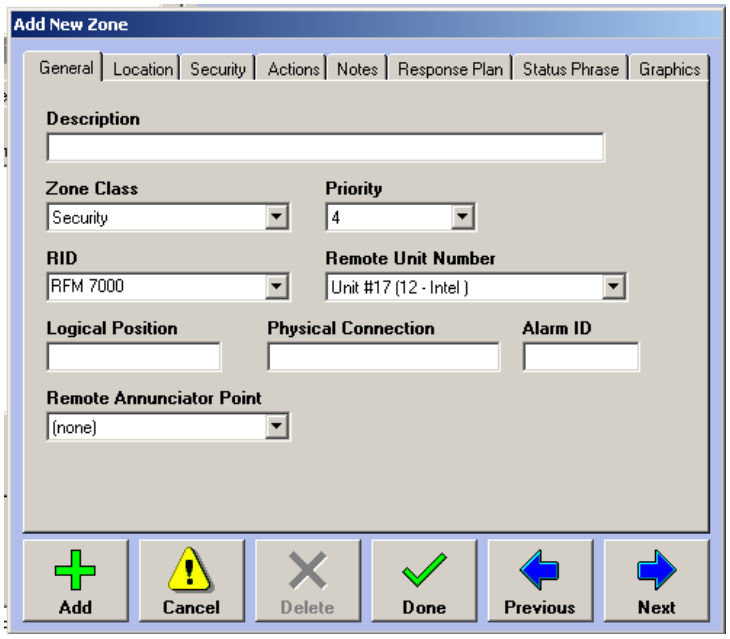
- **Type (# Zones)** Select the BT-XS (M) remote unit type if you are working with a multi-application BT-X (program chip revision B.8 or higher). Select the BT-XS remote unit type if the program chip is revision B.8 or lower.
- **IDS Master Unit** Clear this check box to configure the unit as an IDS application unit.
- **IDS Master Unit Address** Select the IDS Master unit to which you want to associate the Automatic zones on this unit. Be sure to select the IDS Master unit that is in the same BT-X as this application unit. This drop-down list is only available when the IDS Master Unit check box is not checked.
- **Communicator Unit Address** Select the BT-X Communicator unit that is part of this multi-application BT-X.
- **TroubleID** For Monaco use only.
- **Serial Number** Enter the serial number of the remote unit. This field is for informational purposes only and is not required.
- **Unit Class** Displays the default class (security) for these remote unit types. See "Unit Class" on page 2-52 for more information.

2 Click **Next** to advance to the Location tab.

3 Enter a facility and any directions to describe the position of the remote unit.

4 Click **Next** to advance to the Zones tab.

5 Click **Add Zone** to add the security zones to the D-21 database. The Add New Zone dialog box appears.



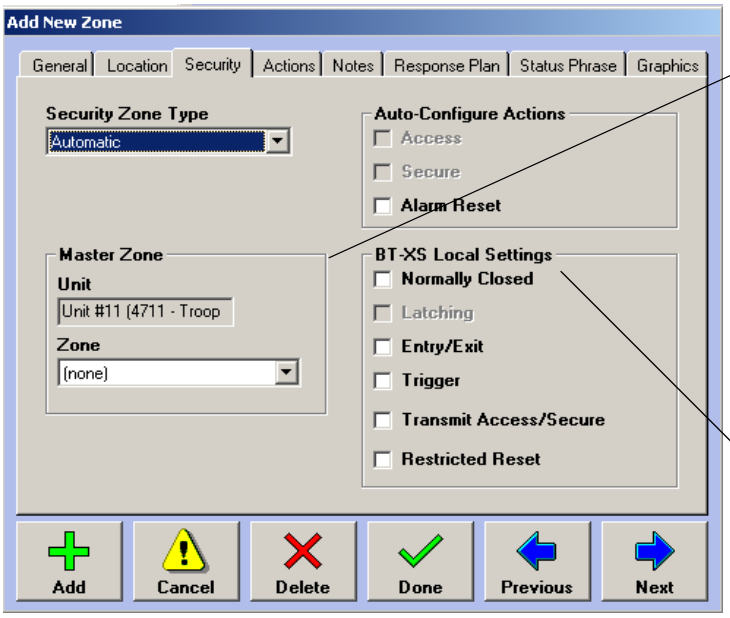
- **Description** Enter a name that identifies the zone throughout the D-21 system.
- **Logical Position** Identifies the number of the remote unit terminal to which the zone is connected. The system uses the logical position to identify the source of an alert associated with a zone.

  For information on other fields on this tab, see "Zones" on page 2-64.

6 Click **Next** to advance to the Location tab.

7 Enter a facility and any directions to describe the position of the remote unit.

8 Click **Next** to advance to the Security tab.



- **Security Zone Type** Select the security zone type for the zone. See "BT-XS Zone Types" on page 9-11.
- **Master Zone** If you select the Automatic zone type, select the Master zone to which you want to associate the Automatic zone. This box only appears when you select the Automatic zone type. All Automatic zones on a single security zone card must be associated with the same Master zone. For more information, see "Master Zones on the BT-XS" on page 9-12.
  - **Unit** Displays the IDS Master unit for the BT-X. Automatic zones can be associated with only one Master zone on the IDS Master unit.
  - **Zone** Select the Master zone to which you want to associate this Automatic zone.
- **Auto Configure Actions** Select the commands for which you would like to create an action. These actions can be assigned to status changes for RIDs, remote units, and zones throughout the D-21. For more information on using actions, see "Actions" on page 3-27. The D-21 can automatically create the following actions for security zones:

Action	Description
Access	Created for Central Initiate zones. Access action can be used to manually change the zone status to Access.
Secure	Created for Central Initiate zones. Secure action is used to manually change the zone status to Secure.
Alarm Reset	Created for Constant Secure, Automatic, Pre-Authorized, Two Man Access/Secure, and Entry/Exit Delay zones. Alarm Reset action can be used to manually normalize the zone status.

- **BT-XS Local Settings** Use the check boxes in this area to record the zone options programmed at the BT-X.

9 See "Zones" on page 2-64 for more information on adding actions, notes, response plans, and status phrases to this zone.

IMPORTANT *You must download information to the BT-X in order to enable correct operation of the zones. Download to each BT-XS (M) unit you configured in the D-21 Admin Client from the D-21 Incident Client Security Commands pane. For more information, see the D-21 Incident Client User Guide (P/N 001-392-00).*

10 Click Done to return to the unit dialog box.

11 Click the Outputs tab in the remote unit dialog box to add outputs to the IDS application unit. You can add up to eight output relays to this unit. For more information on adding outputs, see "Outputs" on page 2-74.

12 Click the Notes tab.

13 Enter descriptive information about the IDS application unit.

14 Click the Actions tab. Use the Actions tab to add status change actions to this unit. See "Actions" on page 3-27 for more information.

15 Click **Done** to add the unit to the database.

IDS iButton and PIN Assignments

When a Master zone is associated with a BT-X iButton Keypad, users arm and disarm the Master zone with an iButton presented to the keypad.

In the past, each BT-X which controlled an iButton reader/keypad implemented Local Enrollment, whereby an authentication database was created and maintained at each local BT-X. The Monaco IDS now implements Central Enrollment, whereby authentication credentials for the entire IDS are created and maintained in a central database and distributed to the local BT-X remote units. Central Enrollment supports authentication through a keypad using either iButton and Personal Identification Number (PIN) or PIN only.

An IDS iButton authentication matches a person from the D-21 database with a specific iButton, PIN, or iButton/PIN combination. Then access is granted for the iButton/PIN to specific master zones that are controlled by BT-X iButton keypads. IDS administrators create and manage IDS authentications at the D-21.

When authentications have been added or changed, an IDS administrator downloads the authentication credentials from the D-21 to the appropriate BT-X units. The BT-X units will then use the authentication information to allow or deny access and report IDS activity back to the D-21. Central Enrollment allows the D-21 to synchronize multiple BT-X units with updated authentication information at all sites from a centralized location.

iButton/PIN assignments can only be done at D-21 workstations configured with an iButton socket hub. All iButton assignment tasks require the insertion of the primary or backup administrator's iButton/PIN in the workstation's iButton hub. Operators who will act as IDS administrators must have the iButton Enrollment option enabled on their Operator dialog box.

Additionally, operators who are authorized to enroll IDS primary and backup administrators must have administrator privileges for the Admin Client. See "To add an operator" on page 2-97.

Before You Begin

You must add the iButton Hub RID to the database and configure the workstation for the iButton hub you want to use for enrolling iButtons. For information on setting up the iButton Hub RID, see the D-21 Remote Interface Driver Guide (P/N 001-399-01). For more information on associating an iButton hub with a workstation, see "Setting Workstation Options" on page 4-49.

Enrolling Administrators

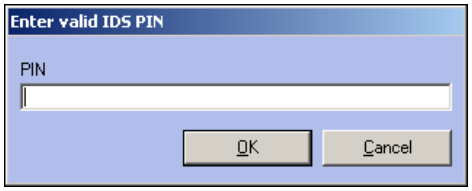
Primary and backup iButton administrators create and manage user authentications and perform authentication downloads to the BT-X remote units. The operators enrolled as the primary and backup administrators must have administrator privileges for the Admin Client and must be assigned their own iButtons. See "To add an operator" on page 2-97 for more information on operator privileges. The primary or backup administrator iButton must always be inserted in one of the iButton sockets connected to the D-21 workstation's iButton hub before any additions or changes to iButton enrollments can be made.

To enroll the primary administrator

1. Log into the D-21 Admin Client as an operator with administrator privileges for the Admin Client.
2. Confirm the iButton reader is attached to the system and enabled. Place the button to be assigned to the Central Enrollment administrator in the reader.

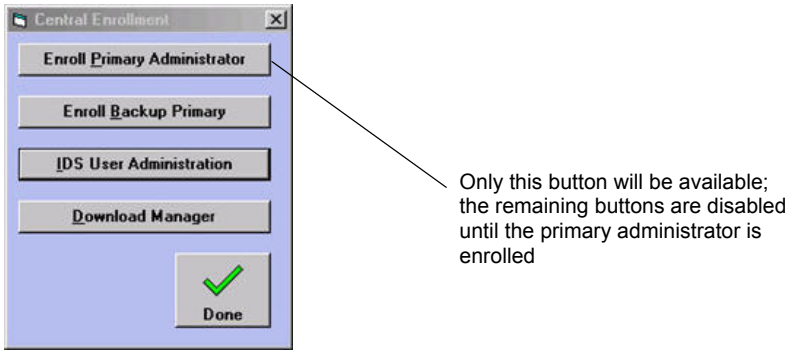
NOTE *The button used for administering Central Enrollment cannot be used for keypad access to controlled areas.*

3. Select **Options > IDS Central Enrollment**.



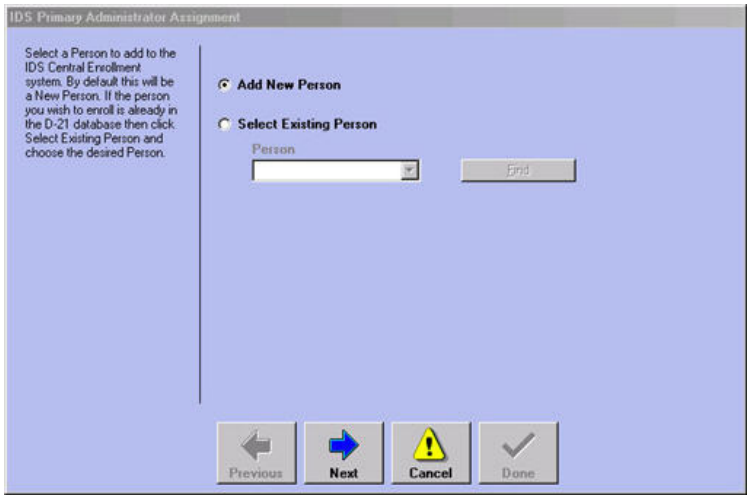
4. Enter the Central Enrollment initialization PIN in the dialog box that appears. (Monaco support personnel will assist you with this step. See "Contact Information" on page ii.)

5 Click **OK**. The Central Enrollment switchboard dialog box appears.

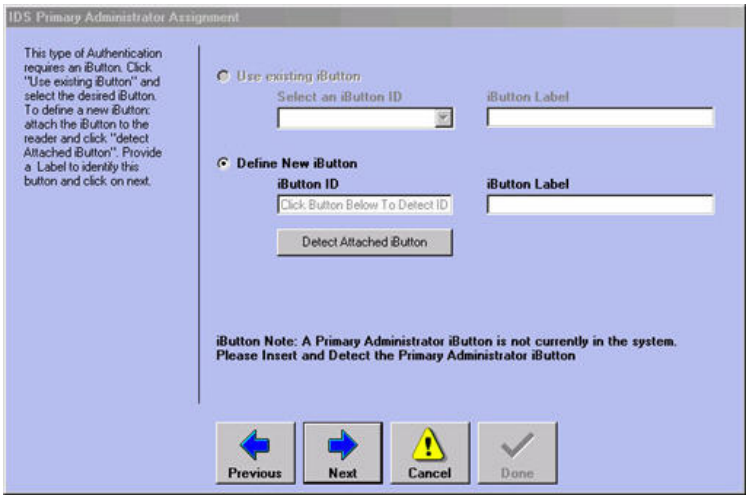


6 Click **Enroll Primary Administrator**. The IDS Primary Administrator Assignment wizard launches.

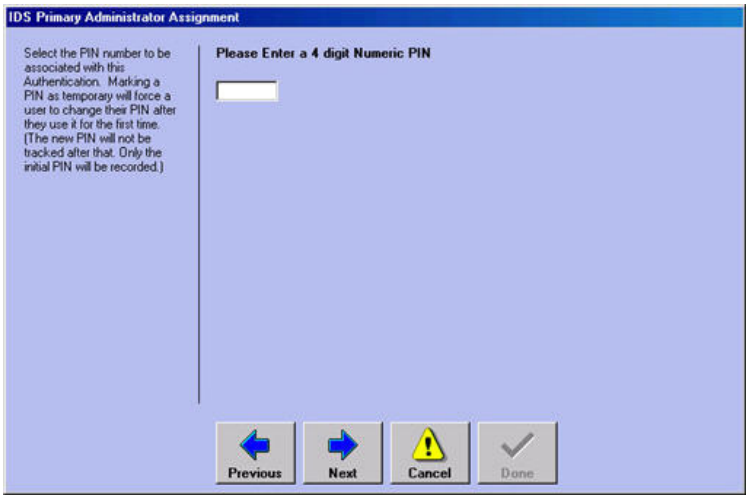
7 In the first screen, click **Select Existing Person**. Select the administrator's name from the Person drop-down list. Click **Next** to proceed to the next screen.



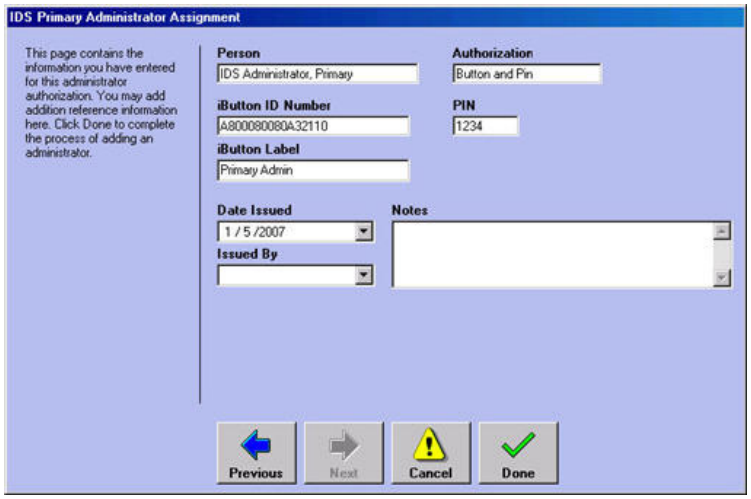
8 Click **Detect Attached iButton**. The unique ID of the button in the reader will appear in the iButton ID text box and in the iButton Label text box. If you would like to give the button a meaningful name, replace the string in the iButton Label text box with the desired text. Click **Next** to proceed to the next screen.



9 Enter a 4-digit numeric PIN. Click **Next** to proceed to the next screen.



10 Add Issued information and Notes as desired. Click **Done**.



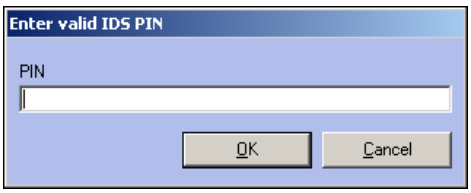
Once the primary administrator account has been created, all IDS iButton management tasks, including creating the Backup Primary account, can be performed from the Central Enrollment switchboard.

IMPORTANT *If you can no longer use either the primary or backup administrator accounts because of lost iButtons or forgotten PINs, contact Monaco for assistance.*

To access the Central Enrollment switchboard

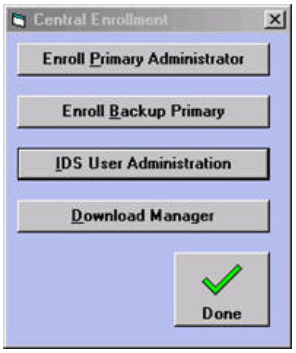
1 Confirm the iButton reader is attached to the system and enabled, with the administrator's button in place.

2 Select **Options > IDS iButton Assignments**.



3 Enter the PIN for the administrator iButton.

4 Click **OK**. The Central Enrollment switchboard dialog box appears.



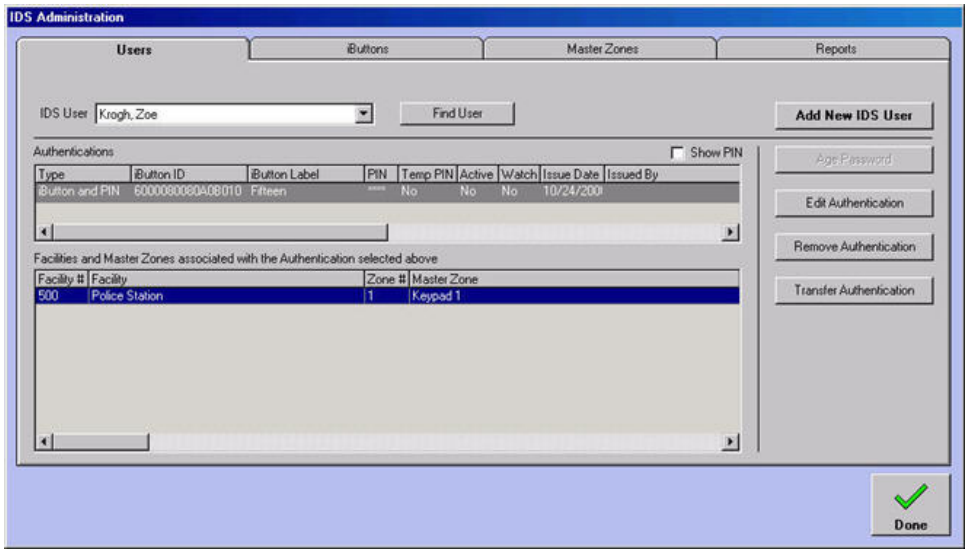
Enrolling Users

Users are enrolled at the D-21 by the primary or backup IDS administrator. The administrator creates an authentication for the user by assigning an iButton and defining which iButton keypads the user can access. Then the administrator must download the authentication to the BT-X remote units which manage the iButton keypads.

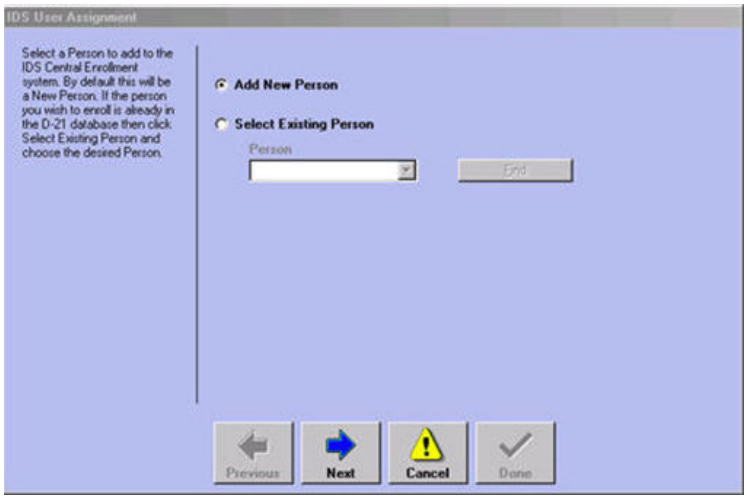
To add a user authentication

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

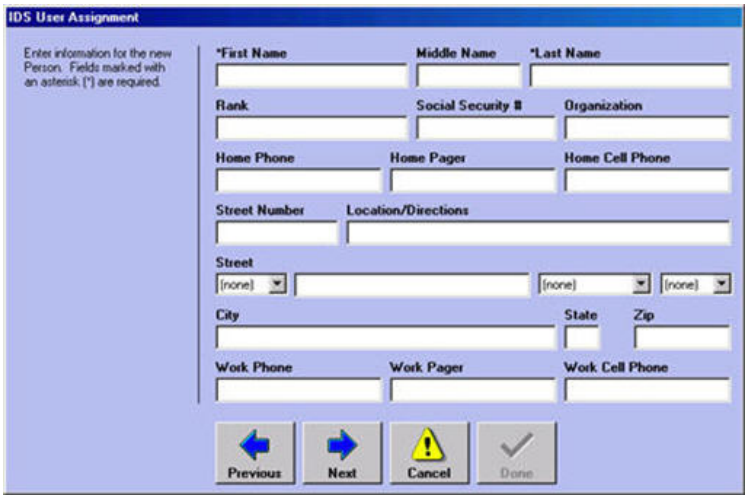
2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.



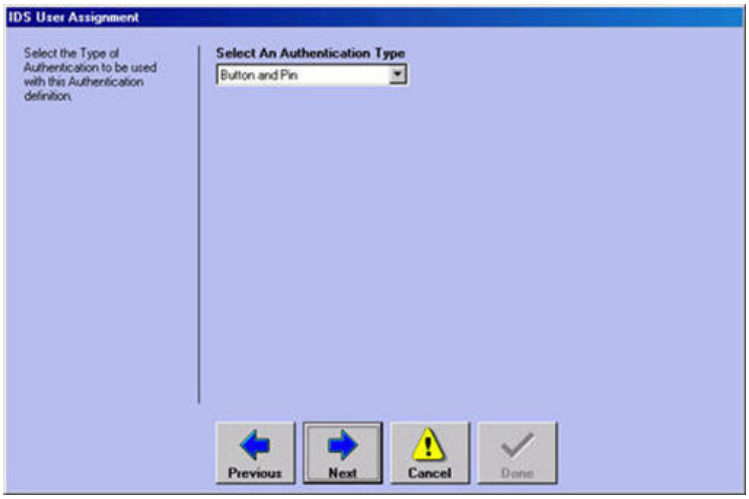
3 Click **Add New IDS User**. The IDS User Assignment wizard launches.



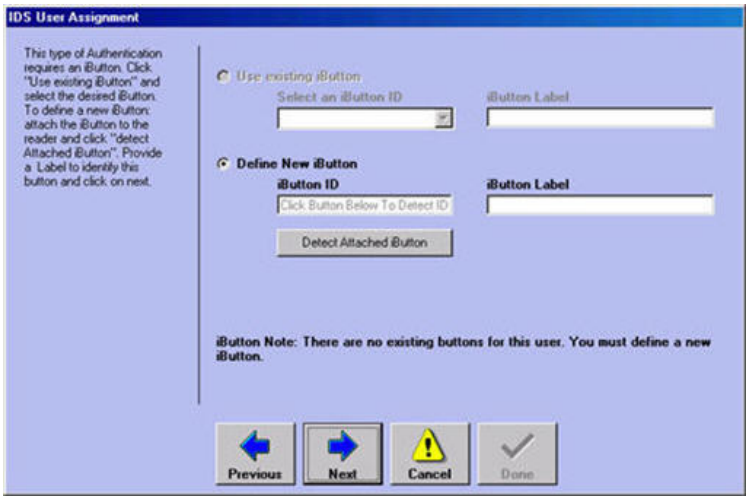
4 If the new user is already entered in the D-21 database, click **Select Existing Person**, select the appropriate name from the Person drop-down list, and click **Next**. If the new user is not already entered in the D-21 database, click **Next** to access a screen which will allow you to create a new Person record.



5 When you are finished entering personnel information, click **Next** to proceed to the next screen.

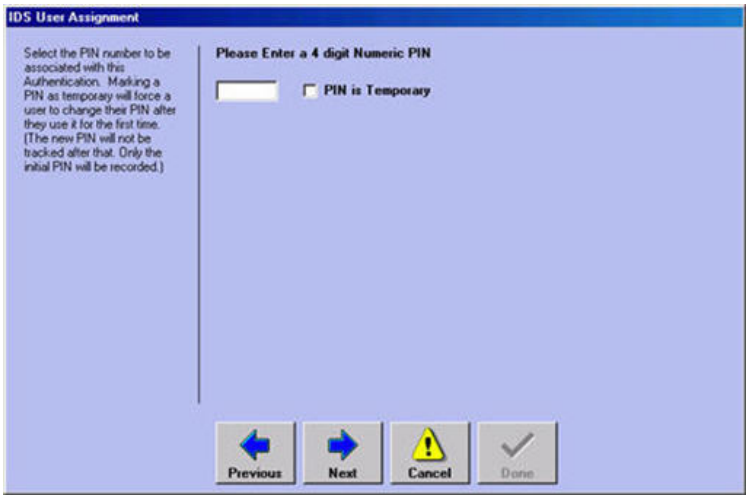


6 Select the Button and PIN authentication type. (This process can also be used to add a new user to a PIN-only system. Select PIN Only and skip the next step.) Click **Next** to proceed to the next screen.



7 Place the button to be assigned to the new user in the iButton reader, then click **Detect Attached iButton**. The unique ID of the button in the reader will appear in the iButton ID text box and in the iButton Label text box. If you would like to give the button a meaningful name, replace the string in the iButton Label text box with the desired text.

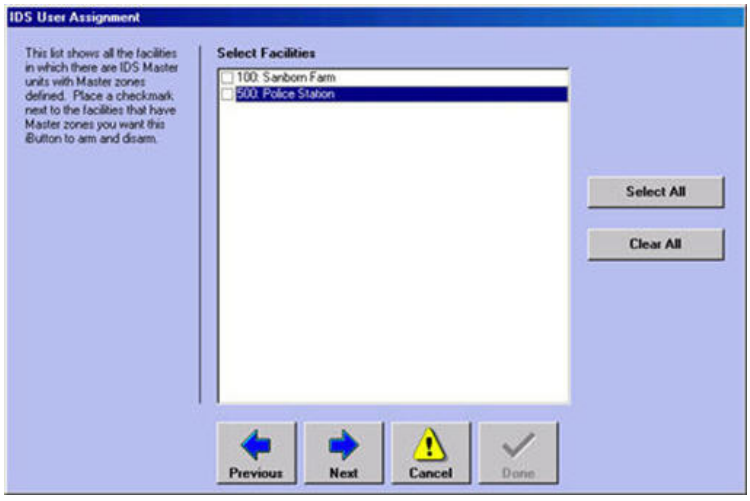
8 Click **Next** to proceed to the next screen.



9 Enter a 4-digit numeric PIN. If the user will be able to set their own PIN, check the box labeled PIN is Temporary.

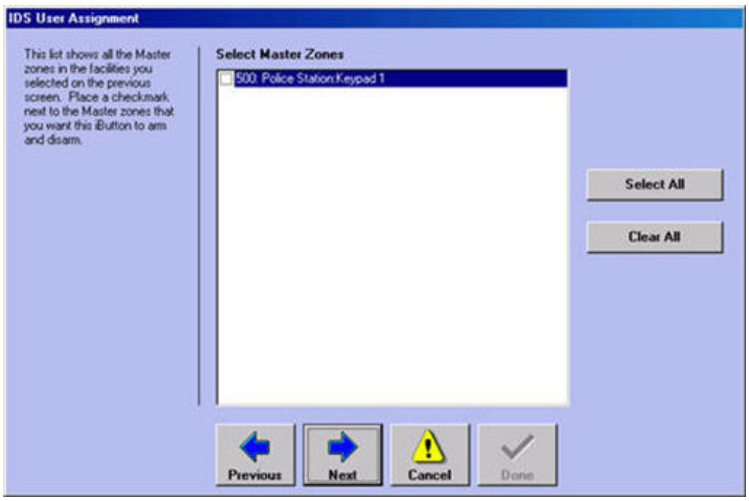
NOTE *The first time a user presents a button assigned a temporary PIN at a keypad, he/she must enter the temporary PIN. Then he/she will be prompted to create a permanent PIN at the keypad. The permanent PIN will not be recorded in the D-21 database.*

10 Click **Next** to proceed to the next screen.

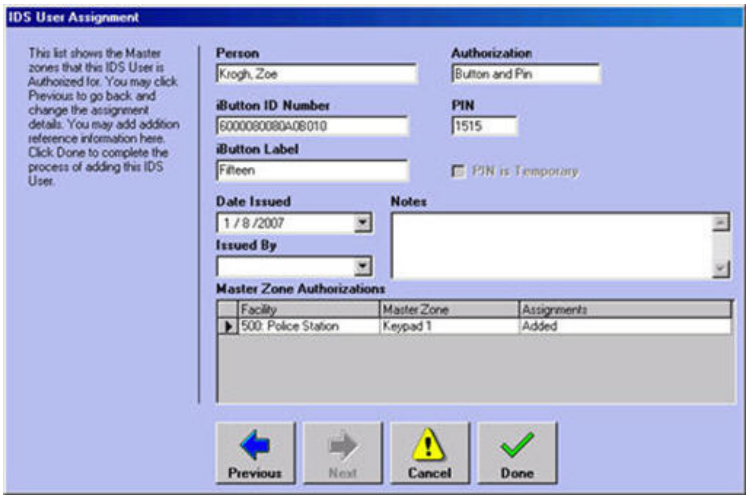


11 Check the appropriate boxes to select the facilities at which the user will be allowed access.

12 Click **Next** to proceed to the next screen.



13 Check the appropriate boxes to select the keypads where the user will be allowed access. Click **Next** to proceed to the last screen.



14 Add Issued information and Notes as desired, and then click **Done**.

IMPORTANT *Add User transactions must be downloaded to the appropriate BT-X units before they will take effect. See* *"To download all pending authentication records" on page 9-43*.

To edit a user authentication

You may need to modify existing user authentications periodically. The following section discusses the modifications, and the steps required to make the changes:

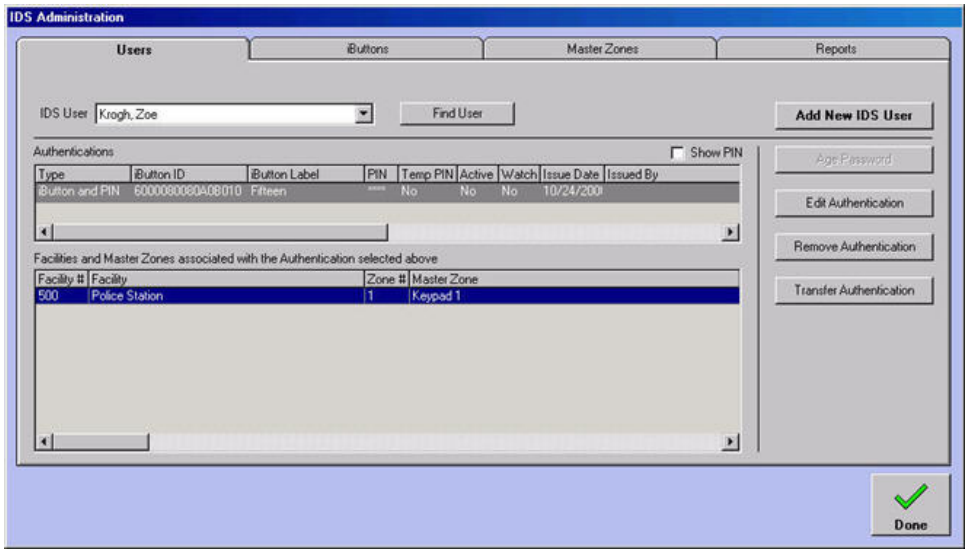
- Resetting the PIN.
- Marking a new PIN as temporary.

NOTE *The first time a user presents a button assigned a temporary PIN at a keypad, he/she must enter the temporary PIN. Then he/she will be prompted to create a permanent PIN at the keypad. The permanent PIN will not be recorded in the D-21 database.*

- Deactivating or re-activating the authentication.
- Adding or removing facilities/keypads assigned to the authentication.
- Placing or removing a Watch on the authentication. When an authentication is set for Watch, each time it is used the activity will be logged in the Incident Client.

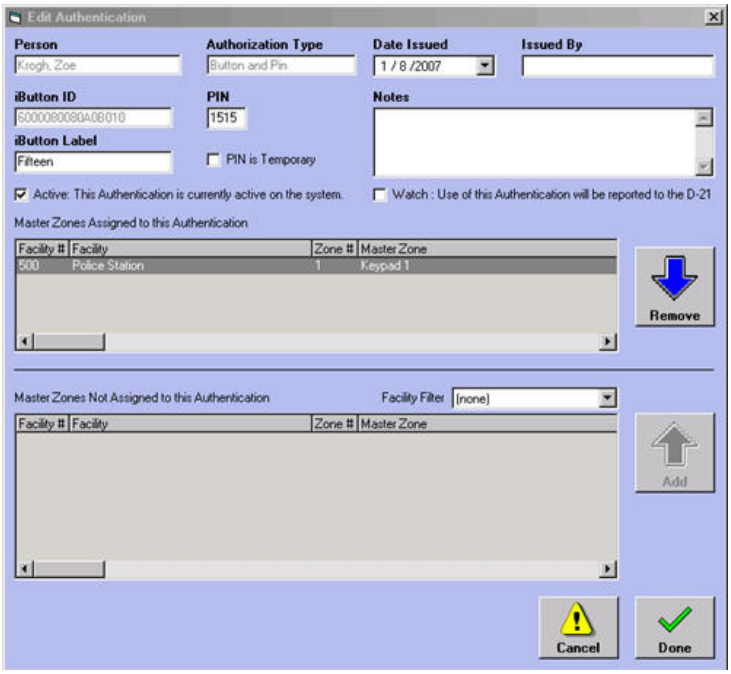
1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.



3 Select the name of the user to edit from the IDS User drop-down list.

4 Click the **Edit Authentication** button. The Edit Authentication dialog box appears.



- **Person** Displays the name of the person selected. To change the person to whom an iButton is assigned, see "To transfer an iButton assignment from one user to another" on page 9-39.
- **Authentication Type** Displays either iButton and PIN or PIN only.
- **Date Issued** Displays the date recorded in this field when the authentication was created. This value can be edited if desired.
- **Issued By** Displays what was recorded in this field when the authentication was created. This value can be edited if desired.
- **iButton ID** Displays the ID number of the iButton assigned to the selected person.
- **iButton Label** Displays the meaningful name given to the iButton when the authentication was created. This value can be edited if desired.
- **PIN** Displays the PIN assigned when the authentication was created. To reset the PIN, delete the text in the PIN text box and enter the new 4-digit numeric PIN.
- **PIN is Temporary** If unchecked, indicates the PIN is permanent, that is, the user will not be required to change it the next time the iButton is used. To mark a new PIN as temporary, check this box.

NOTE *The D-21 does not record whether a user has created a permanent PIN to replace a temporary one. Permanent PINs created by users at the keypad are not recorded in the D-21 database.*

- **Notes** Displays notes entered when the authentication was created. This value can be edited if desired.

- **Active** If checked, indicates that the authentication is currently active. To deactivate or re-activate the authentication, uncheck or check this box.
- **Master Zones Assigned** Displays the master zones which control the keypads where this authentication provides entry. To remove a master zone from the authentication, select the appropriate row in this grid, then click **Remove**. The row is removed and can be found again in the Master Zones Not Assigned grid.
- **Master Zones Not Assigned** Displays the master zones which control the keypads where this authentication does not provide entry. To add a master zone to the authentication, select the appropriate row in this grid (use the **Facility Filter** drop-down list to help you find it) then click **Add**. The row is added to the Master Zones Assigned grid.
- **Watch** If checked, a log entry will be created in the D-21 whenever the authentication is used. See the D-21 Incident Client User Guide (P/N 001-392-00) for more information on viewing log entries. To place or remove a Watch on the authentication, check or uncheck this box.

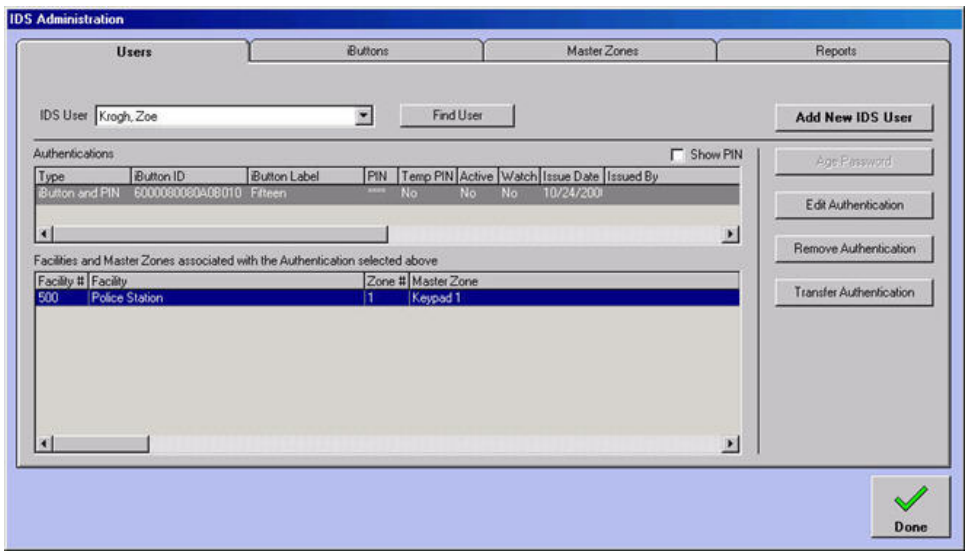
5 When you are finished editing the authentication, click **Done**.

IMPORTANT *All Edit Authentication transactions must be downloaded to the appropriate BT-X units before they will take effect. See "To download all pending authentication records" on page 9-43.*

To remove a user authentication

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.



3 Select the name of the user to be removed from the IDS User drop-down list. The Authentications and Master Zones grids will refresh to display the current authentication information for the user.

4 Click **Remove Authentication**. Click **Yes,** in the message box that appears, to confirm the removal.

The button will now be available to assign to a different user. This operation does not remove the user from the D-21 database. To remove a user, see "To delete a person record" on page 2-92.

IMPORTANT *Remove Authentication transactions must be downloaded to the appropriate BT-X units before they will take effect. See "To download all pending authentication records" on page 9-43.*

Managing iButtons

Use the IDS User Administration dialog box to perform the following iButton management tasks:

- Deactivate an assigned iButton (temporary). See "To deactivate an assigned iButton (temporary)" on page 9-37.
- Re-activate an assigned iButton. See "To re-activate an assigned iButton" on page 9-38.
- Transfer an iButton assignment from one user to another. See "To transfer an iButton assignment from one user to another" on page 9-39.
- Age a PIN. See "To age a PIN" on page 9-40.
- Determine if an iButton has been assigned to a user. See "To determine if an iButton has been assigned to a user" on page 9-40.
- View the users with access to a Master Zone. See "To view the users with access to a Master Zone" on page 9-41.
- Create a Facility Access Report. See "To create a Facility Access Report" on page 9-42.

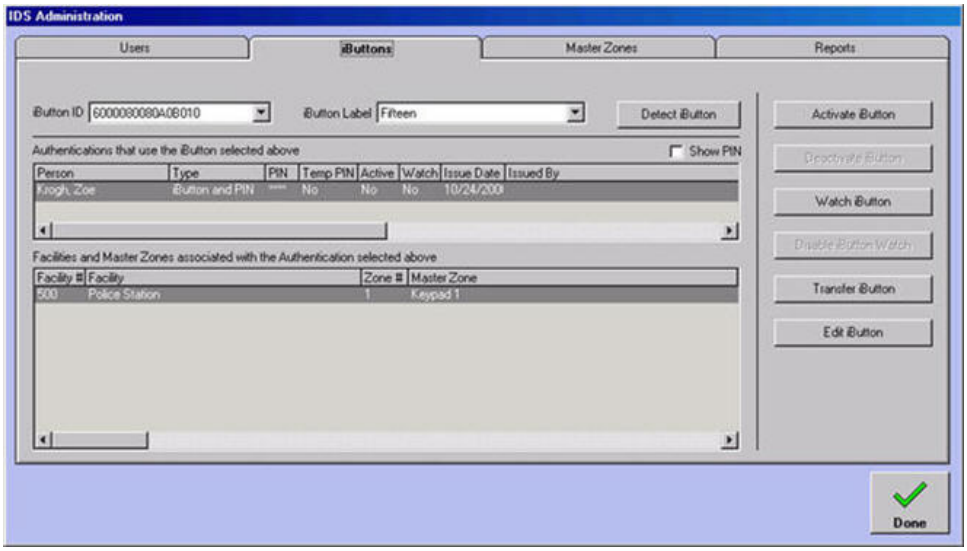
To deactivate an assigned iButton (temporary)

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 If you know the name of the user to whom the button is assigned, but do not know the button's ID or label, select the name of the user to be deactivated from the IDS User drop-down list. Make a note of the iButton ID or iButton Label assigned to the user.

4 Click the iButtons tab.



5 Select the button from either the iButton ID or the iButton Label drop-down lists.

6 Click **Deactivate iButton**. You will see the Active value for the button change from Yes to No.

The button cannot be assigned to another user, and will not allow access to secured areas until it has been re-activated.

IMPORTANT *Deactivate transactions must be downloaded to the appropriate BT-X remote units before they will take effect. See "To download all pending authentication records" on page 9-43.*

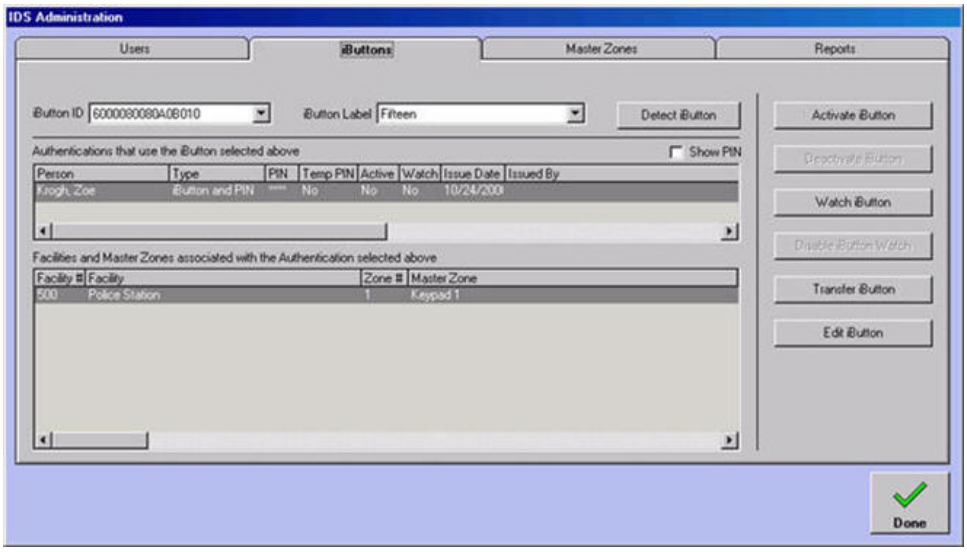
To re-activate an assigned iButton

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 If you know the name of the user to whom the button is assigned, but do not know the button's ID or label, select the name of the user to be activated from the IDS User drop-down list. Make a note of the iButton ID or iButton Label assigned to the user.

4 Click the iButtons tab.



5 Select the button from either the iButton ID or the iButton Label drop-down lists.

6 Click **Activate iButton**. You will see the Active value for the button change from No to Yes.

IMPORTANT *Activate transactions must be downloaded to the appropriate BT-X remote units before they will take effect. See "To download all pending authentication records" on page 9-43.*

To transfer an iButton assignment from one user to another

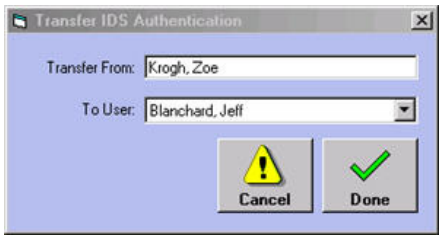
Before you begin: If the user to whom you are going to assign the button has not already been added to the D-21 database, stop and do so now. See "To add a person" on page 2-86.

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 Select the name of the user to whom the button is currently assigned from the IDS User drop-down list.

4 Click **Transfer Authentication**. The Transfer IDS Authentication dialog box appears.



5 Select the name of the user to whom the button is being assigned from the To User drop-down list.

6 Click **Done**.

NOTE *This operation does not remove the original user from the D-21 database.*

To age a PIN

At some point you may wish to have a user with a private permanent PIN (i.e. a user to whom you issued a temporary PIN) choose a new PIN. This is called "ageing" a PIN.

NOTE *You do not have to age a PIN for a user to whom you originally assigned a permanent PIN. Instead, you can simply change the PIN and inform the user.*

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 Select the name of the user whose PIN you wish to age from the IDS User drop-down list.

4 Click **Age Password**. The next time the user requests access at a keypad, he/she will be required to create a new private permanent password.

NOTE *The Age Password transaction is immediately and automatically downloaded to the appropriate BT-X remote units, and does not require a user to manually initiate a download.*

To determine if an iButton has been assigned to a user

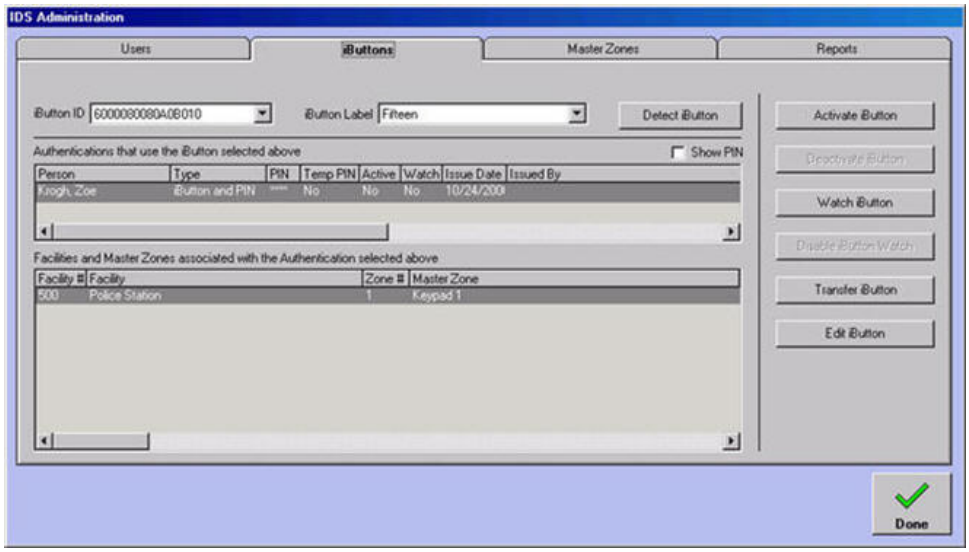
To determine whether a button in your possession has already been assigned to a user, follow this procedure.

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 Place the button in question in the iButton reader.

4 Click the iButtons tab.



5 Click **Detect iButton**.

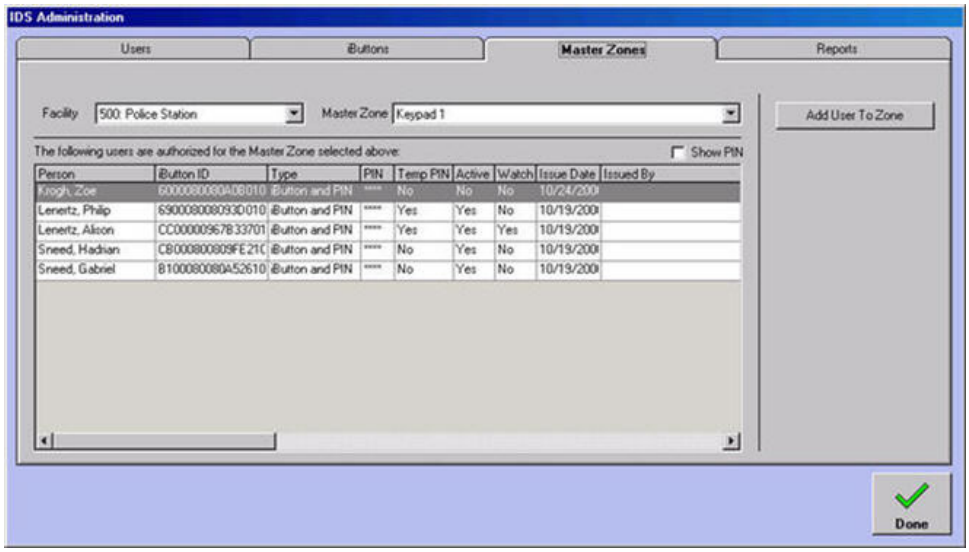
The dialog box that appears will tell you the ID number for the button in question, and the iButton ID drop-down list on the iButtons tab will switch to that particular ID number if the button has already been assigned.

To view the users with access to a Master Zone

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 Click the Master Zones tab.



4 Select the appropriate Facility and Master Zone from the drop-down lists. The grid will display all the users whose authentication includes access to the selected Master Zone.

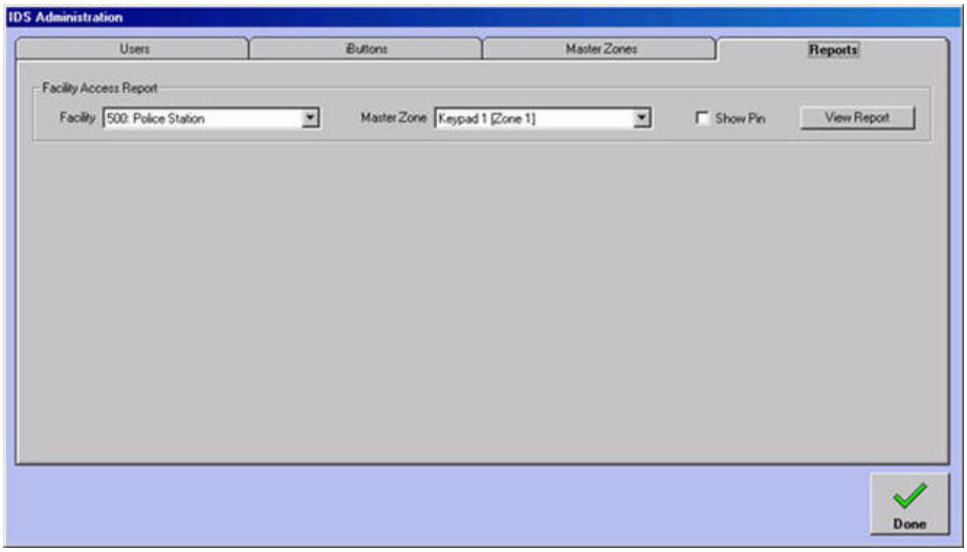
NOTE *You can add a user to the Master Zone from this tab by clicking* ***Add User To Zone****. This has the same effect as editing the user's authentication on the Users tab. See "To edit a user authentication" on page 9-34.*

To create a Facility Access Report

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **IDS User Administration**. The IDS Administration dialog box appears, with the Users tab displayed.

3 Click the Reports tab.



4 Select the facility in question from the Facility drop-down list.

5 Make the appropriate selection from the Master Zone drop-down list, either All or a particular Master Zone.

6 If you wish the Facility Access Report to include PINs, check the Show PIN box.

7 Click **View Report**. A Print Preview window opens, displaying the Facility Access Report as it will display when printed.

From the Print Preview window you can choose to print the report immediately or export it to one of several common file formats. See the D-21 Incident Client User Guide (P/N 001-392-00) for more information about printing in the D-21 system.

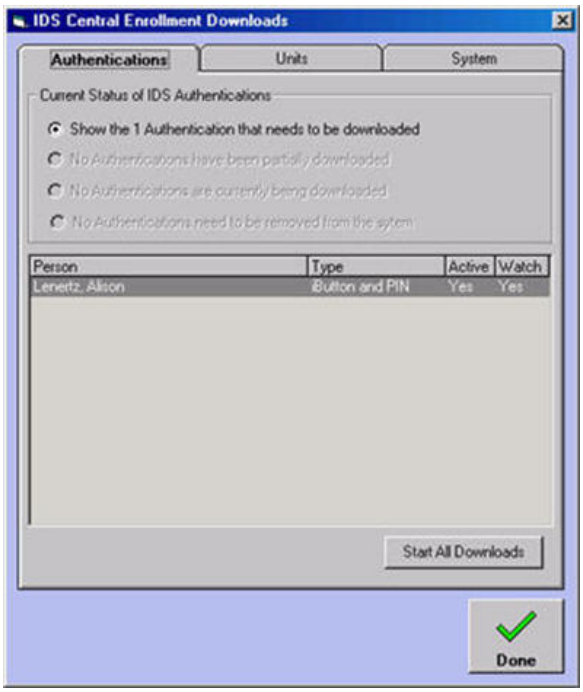
Downloading iButton Authentications

After you have added, edited, or removed authentications, you must download the records to the appropriate BT-X remote units. When you click **Done** to close the IDS Administration dialog box, a message will inform you if you have any records awaiting download.

It is important to perform the download as soon as possible, since the authentication changes will not take effect until you do so.

To download all pending authentication records

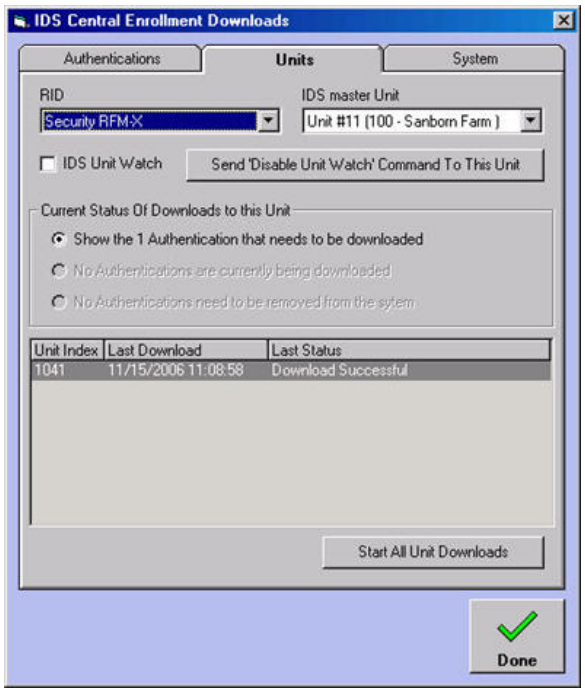
1. Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.
2. Click **Download Manager**. The IDS Central Enrollment Downloads dialog box opens.



3. Click **Start All Downloads**.

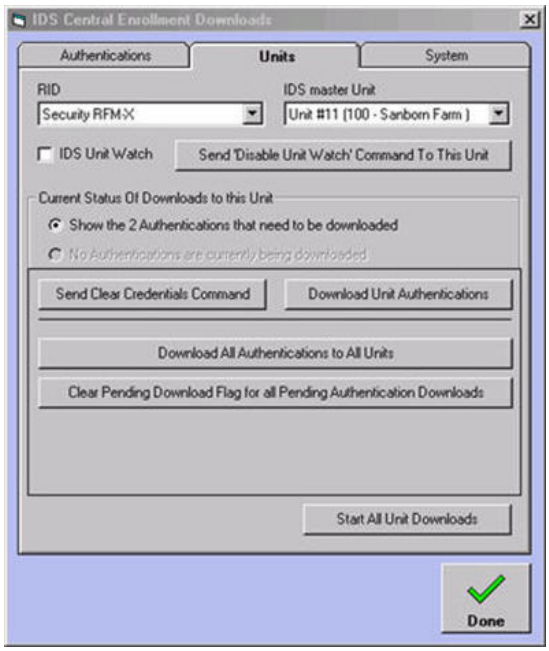
To download authentication records for a specific BT-X

1. Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.
2. Click **Download Manager**. The IDS Central Enrollment Downloads dialog box opens with the Authentications tab selected.
3. Click the Units tab.



NOTE *Clicking* **Start All Unit Downloads** *initiates a standard authentication download, equivalent to clicking* **Start All Downloads** *on the Authentications tab.*

4 Press Alt+H. Additional command buttons are displayed.



- **Send Clear Credentials Command** Removes all authentication records from the selected BT-X remote unit. Use to reset the local database of the selected BT-X.

IMPORTANT *The Master Zones controlled by the selected BT-X will not allow any access until the next time authentications are downloaded to the remote unit. Do not issue this command unless instructed to do so by Monaco support personnel.*

- **Download Unit Authentications** Re-sends all authentications associated with the selected BT-X regardless of whether they are pending or not. These authentications are used to repopulate the local database of a remote unit which has been reset with the Clear Credentials command.
- **Download All Authentications for All Units** Re-sends all authentications to all BT-X remote units regardless of whether they are pending or not. These authentications are used to populate the local databases of all remote units in a new IDS iButton installation.
- **Clear Pending Download Flag for all Pending Authentication Downloads** Removes all authentications from the pending download list. These authentications are used to reset the pending download list.

IMPORTANT *Use of the Clear Pending Download Flag for all Pending Authentication Downloads command can cause the central D-21 database to become out of sync with the local BT-X databases. Do not issue this command unless instructed to do so by Monaco support personnel.*

5 Select the appropriate RID and IDS Master Unit from the drop-down lists.

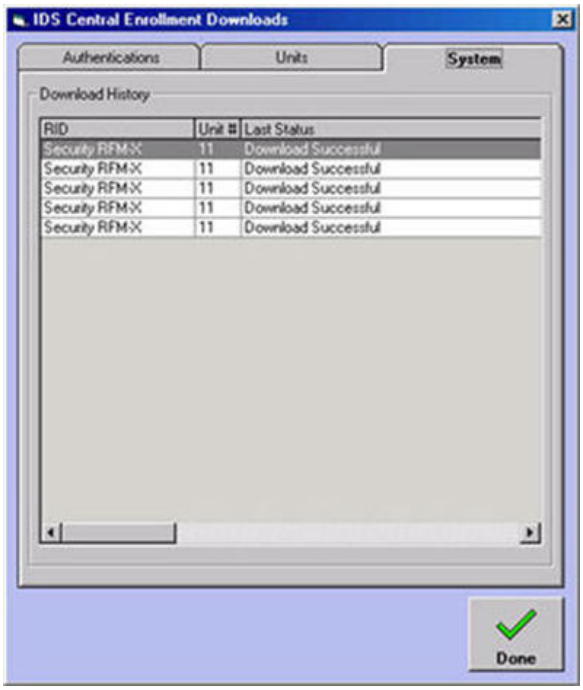
6 Click **Download Unit Authentications**.

To view download results and retry an unsuccessful download

Authentication downloads can take up to a minute per record, so the entire operation can be lengthy especially if you have many changes to download. Therefore, you may not want to monitor the download as it is occurring. You can view the results of the most recent download and retry an unsuccessful download in the Download Manager.

1. Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.
2. Click **Download Manager**. The IDS Central Enrollment Downloads dialog box opens with the Authentications tab selected.
3. If a download is still under way, you can view the records queued to be downloaded on either the Authentications tab (organized by person) or the Units tab (organized by BT-X unit).
4. If you wish to re-start the download, click **Retry All Downloads** on the Authentications tab, or **Retry All Unit Downloads** on the Units tab.

5 Click the System tab to see the results of the most recently completed record downloads. Any record downloads that are unsuccessful will be marked again for download.



IMPORTANT *Contact Monaco support personnel if a record download consistently fails after several attempts.*

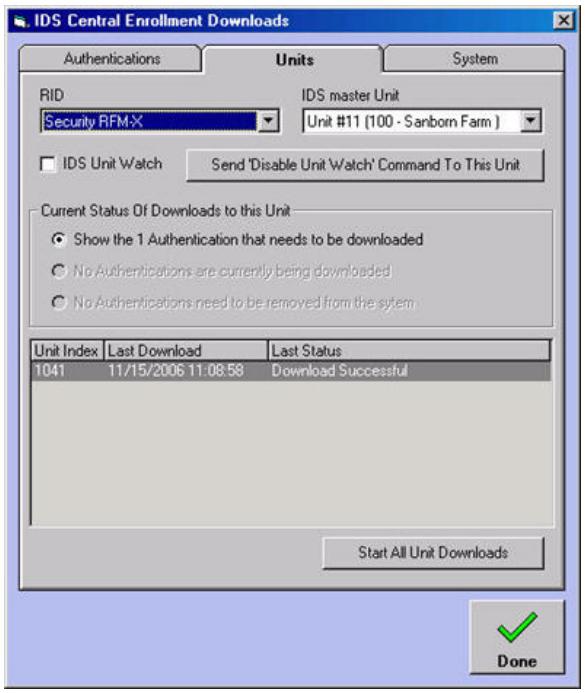
To enable or disable a unit watch

A unit watch sends a log record to the D-21 Incident Client each time an authentication is used at the BT-X remote unit.

1 Go to the Central Enrollment switchboard. See "To access the Central Enrollment switchboard" on page 9-28.

2 Click **Download Manager**. The IDS Central Enrollment Downloads dialog box opens with the Authentications tab selected.

3 Click the Units tab.



4 Select the appropriate RID and IDS Master Unit from the drop-down lists.

5 The IDS Unit Watch check box displays whether a unit watch is currently in place for the unit selected.

NOTE *The IDS Unit Watch check box can also be found on the General tab of the IDS Master Unit's properties dialog box, accessed from the System tree pane in the Admin Client. However, the Enable Unit Watch and Disable Unit Watch commands can only be sent from the Download Manager.*

6 The button next to the IDS Unit Watch check box provides access to the Disable Unit Watch or Enable Unit Watch command, depending on the current unit watch setting.

- **Send Enable Unit Watch Command To This Unit** Sets a unit watch for a BT-X which is not currently being watched.
- **Send Disable Unit Watch Command To This Unit** Removes a unit watch for a BT-X which is currently being watched.

NOTE *Any watches set up for specific authentications remain in effect after a Disable Unit Watch command is executed.*

Section 10
Configuring an E-911 System

Read this section to learn how to configure an E-911 remote interface driver and phone number database for your site.

Contents

Configuring an E-911 System 10-2
Creating an E-911 Phone Number Database 10-8

Configuring an E-911 System

The D-21 provides a remote interface driver (RID) to communicate with the E-911 system that services your organization. When your E-911 system receives a 911 call, the information available in the E-911 provider's database is passed to the D-21. The D-21 displays an alert on the D-21 workstation with information from the E-911 feed and editable fields allowing operators to record more information from the phone call.

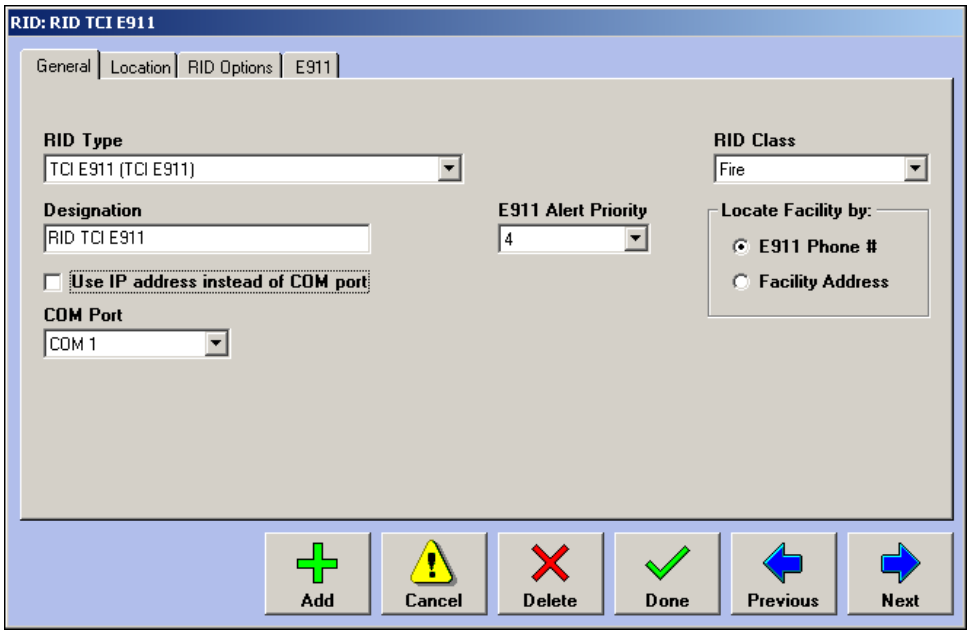
The D-21 can also provide additional facility information from its own database for use with the incoming call. There are two ways you can link the incoming call with additional information from the D-21 database, and you must specify one of the following when configuring the RID:

- **Facility Address** The D-21 matches the address on the incoming E-911 feed with facility addresses in the D-21 database. If there is a match, the D-21 displays additional facility information in the fields of the E-911 alert displayed to the D-21 operator. This option requires street address information be entered when facilities are added to the database.
- **E911 Phone Numbers** The E-911 Phone List database is a listing of phone numbers linked to a facility in the D-21 database. When a phone number on an incoming E-911 feed matches one of the numbers in the E-911 phone database, the D-21 displays the information from the E-911 phone list. This option requires that an E-911 phone number database be added to the D-21 database. For more information, see "Creating an E-911 Phone Number Database" on page 10-8.

NOTE *The D-21 can be configured to import E-911 phone number information from an external source. Contact Monaco D-21 support if you wish to use the E-911 import feature.*

To add an E-911 RID

1 Select **Add > RID**. The Add New RID dialog box appears.



- **RID Type** Select the RID for your E-911 service provider.
- **Designation** Type a name for the RID.
- **E911 Alert Priority** Priority determines the order in which a buffered alarm alert is displayed by the D-21 Incident Client. For example, if there are five alarm alerts in the buffer, alerts with a priority of 1 are presented before alerts with a priority of 2, even if the priority 2 alerts occurred before the priority 1 alerts. For more information on how the D-21 processes alerts, see "Setting Up Alert Processing" on page 3-45.
- **RID Class** Select either Fire or Security to specify which workstations will display status for this RID. If you select Fire, the RID will only be displayed on workstations with the Fire Client enabled. If you select Security, the RID is only available on workstations with the Security Client enabled.
- **Locate Facility by** Select the method to use for locating additional information about the incoming E-911 call:

– **E911 Phone #** The D-21 attempts to match the incoming E-911 phone number with one of the numbers in the D-21 E-911 phone database. When you select this option, the E911 tab becomes available for adding E-911 phone numbers. See "To add a phone number to the E-911 database" on page 10-9.

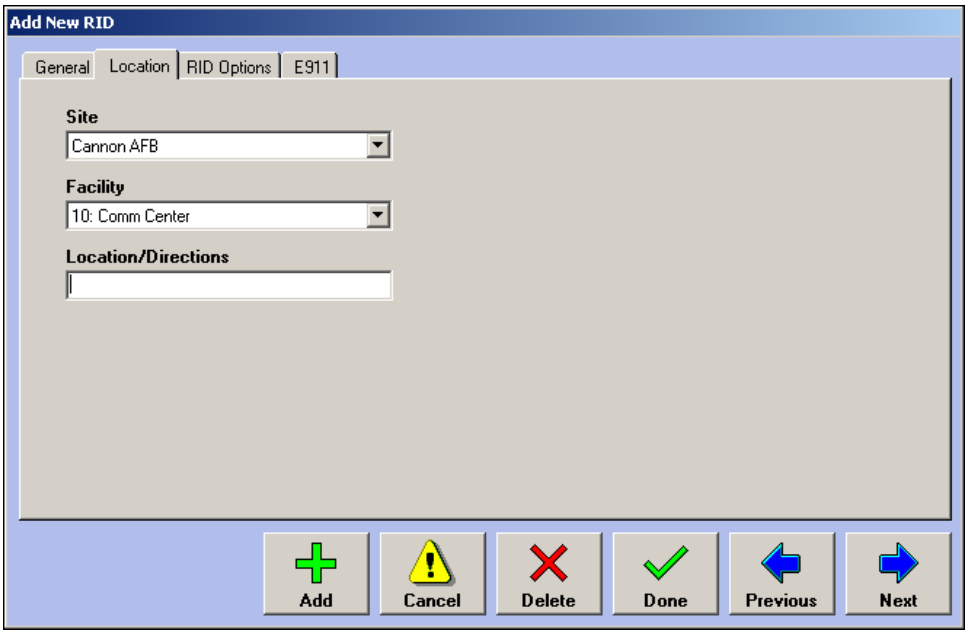
– **Facility Address** The D-21 attempts to match the incoming address on the E-911 feed to the address information saved with each facility. This option requires street address information be entered when facilities are added to the D-21 database.

- **COM Port** Select this option if the E-911 equipment is connected directly to one of the available COM ports on the back of the D-21 computer.

NOTE *Each COM port can only be assigned to one RID.*

- **Use IP address instead of COM port** Select this option if the E-911 system will communicate with the D-21 over a network. Enter an Internet Protocol (IP) address, Port and Port Time-out for the E-911 system. Alternate IP addresses and ports can be configured to provide redundancy for your E-911 system. See "To configure alternate E-911 systems over IP" on page 10-6.

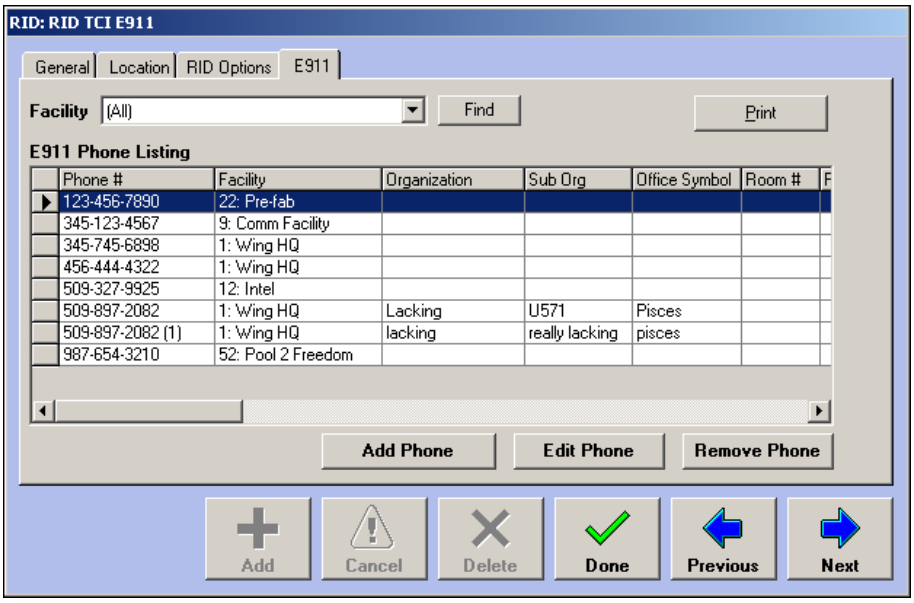
2 Click **Next** to advance to the Location tab.



- **Site** Select the site you want to associate with the E-911 system.
- **Facility** Select the facility where the E-911 system is located. If the appropriate facility does not appear in the drop-down list, make a note to return to this dialog box to specify the facility after it has been added to the database. See "To add a facility" on page 2-13.
- **Location/Directions** Enter information describing the physical location of the E-911 equipment in the facility.

3 Click **Next** to advance to the RID Options tab. Enable options on this tab only when instructed to do so by Monaco personnel.

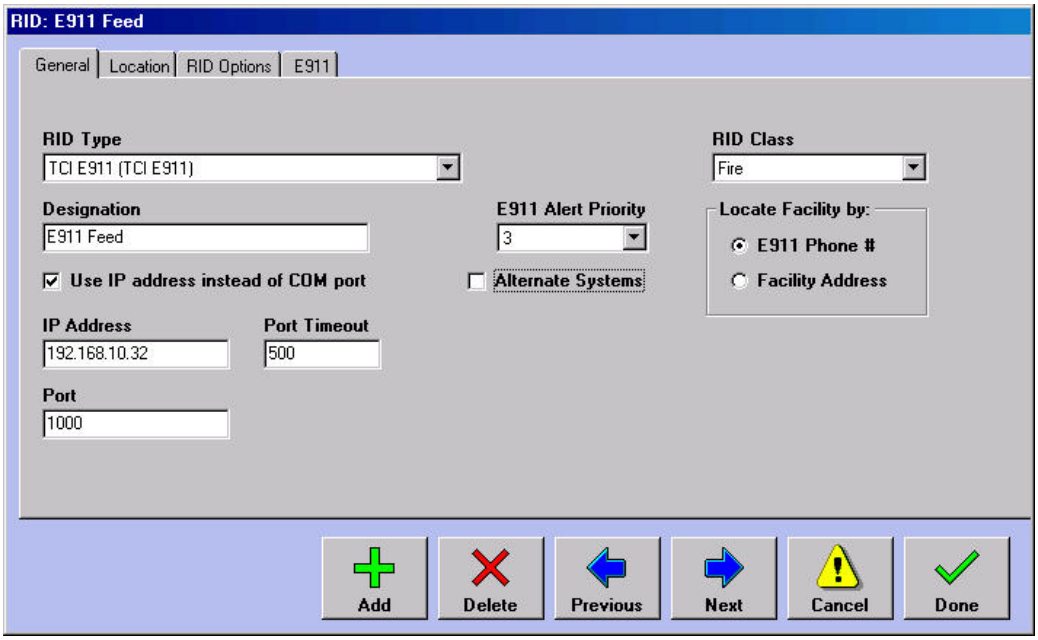
4 Click **Next** to advance to the E911 tab. This tab is only available when the Locate Facility by E911 Phone # option on the General tab is selected.



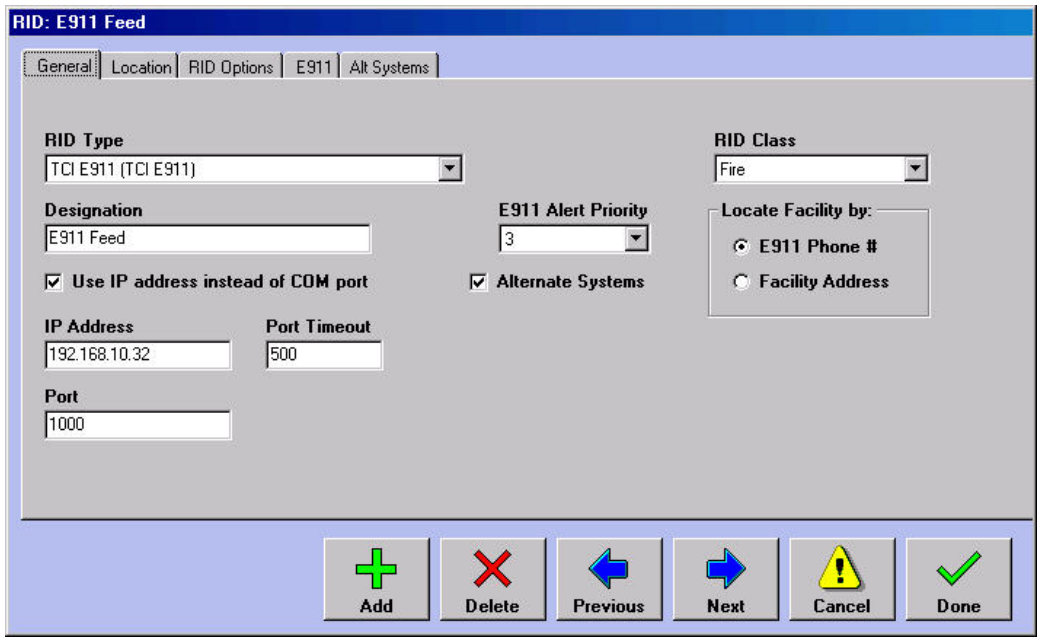
NOTE *The E911 tab lists all the phone numbers that have been entered in the D-21 E-911 database. For more information on adding and editing the E-911 database, see* *"Creating an E-911 Phone Number Database" on page 10-8*.

To configure alternate E-911 systems over IP

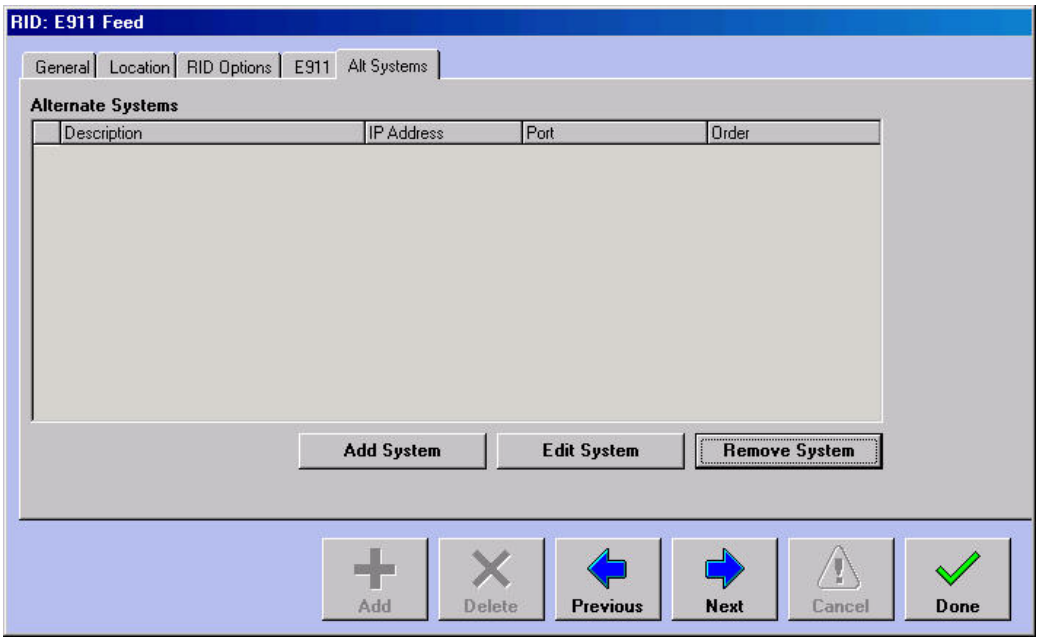
1 If necessary, access the E-911 RID dialog box by right-clicking it in the System tree pane.



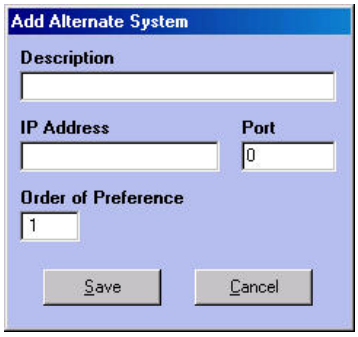
2 Enable Alternate Systems by clicking the checkbox. The Alt Systems tab appears to the right of the E911 tab.



3 Click the Alt Systems tab.

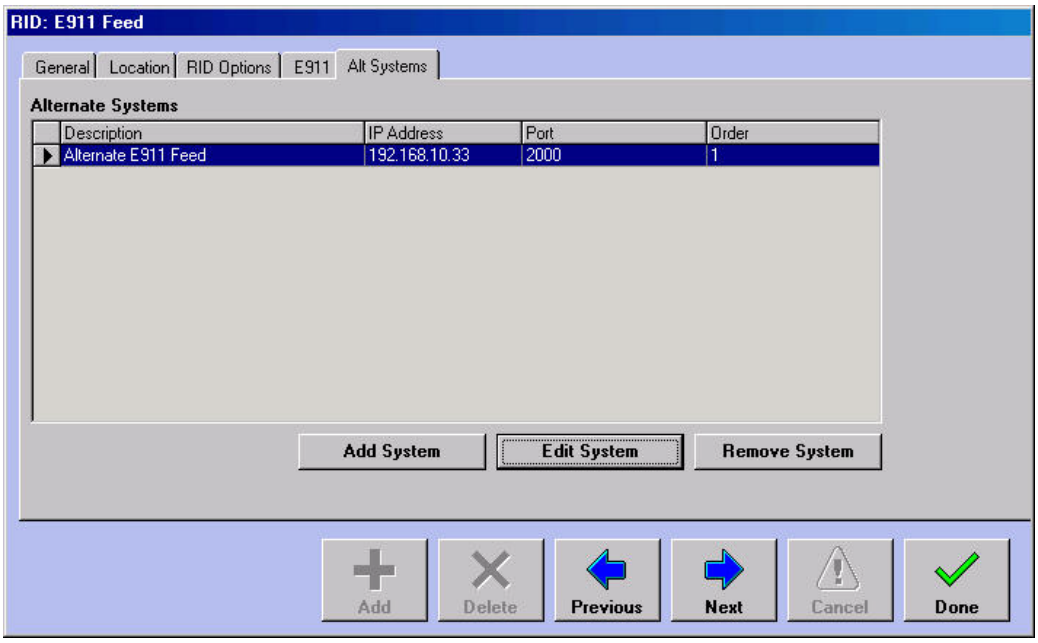


4 Click **Add System**. The Add Alternate System dialog box appears.



- **Description** Provide a recognizable name for the alternate system.
- **IP Address** Provide the IP address to be used by the alternate system.
- **Port** Provide the port to be used by the alternate system.
- **Order of Preference** Defaults to 1, which means this IP address will be used when the E-911 RID's primary IP address is unavailable. If you are configuring multiple alternate systems, set this value to 2 for the system being used when the primary and the first alternate are unavailable, and so forth.

5 When you are through configuring the alternate system, click **Save**. You are returned to the Alt Systems tab.



6 Continue adding alternate systems as appropriate. When you are finished, click **Done**.

Creating an E-911 Phone Number Database

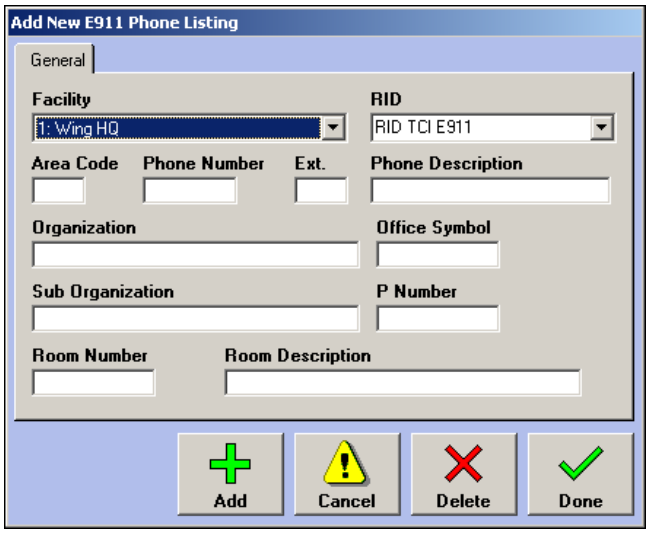
The D-21 E-911 phone number database links an incoming phone number to critical information in the D-21 database about the site, facility, and personnel. Use the D-21 E-911 database to provide operators with facility, organization, and room number information. Phone and room description fields can be used to provide special usage information that could be critical during an incident.

When the E-911 system passes a phone number to the D-21, the D-21 looks for a match with a phone number in the D-21 database. If there is a match, the D-21 displays an EMS alert with information from the D-21 E-911 database. If there is no matching number in the D-21 database, the E-911 data is used to fill the alert fields. In both cases, the actual E-911 feed is displayed in the alert window.

To add a phone number to the E-911 database

NOTE *You can edit and delete existing E-911 phone numbers in the Facility and E-911 RID dialog boxes. For more information, see "To edit a phone number in the E-911 database" on page 10-10.*

1 Select **Add > E911 Phone Listing**. The Add New E911 Phone Listing dialog box appears.



NOTE *This is the same dialog box displayed when you click the Add Phone button on the E911 tab in the Facility and E-911 RID dialog boxes.*

2 Enter the phone number and information you want to include in the E-911 database.

- **Facility** The facility where the phone is located.
- **RID** The name of the RID communicating with the E-911 system.
- **Area Code/Phone Number/Ext.** The phone number for which you want to provide information when it is received from the E-911 system.
- **Phone Description** A text field for additional information about the location or condition of the phone.
- **Organization** The administrative organization where the phone is located.
- **Office Symbol** A text field for an abbreviation or other short-hand description of the organization.
- **Sub Organization** The administrative sub-organization where the phone is located, if any.
- **P Number** The wire circuit number used by the phone provider to identify the phone line.
- **Room Number** The number of the room within the facility.

- **Room Description** A text field for additional information about the location or condition of the room where the phone is located.

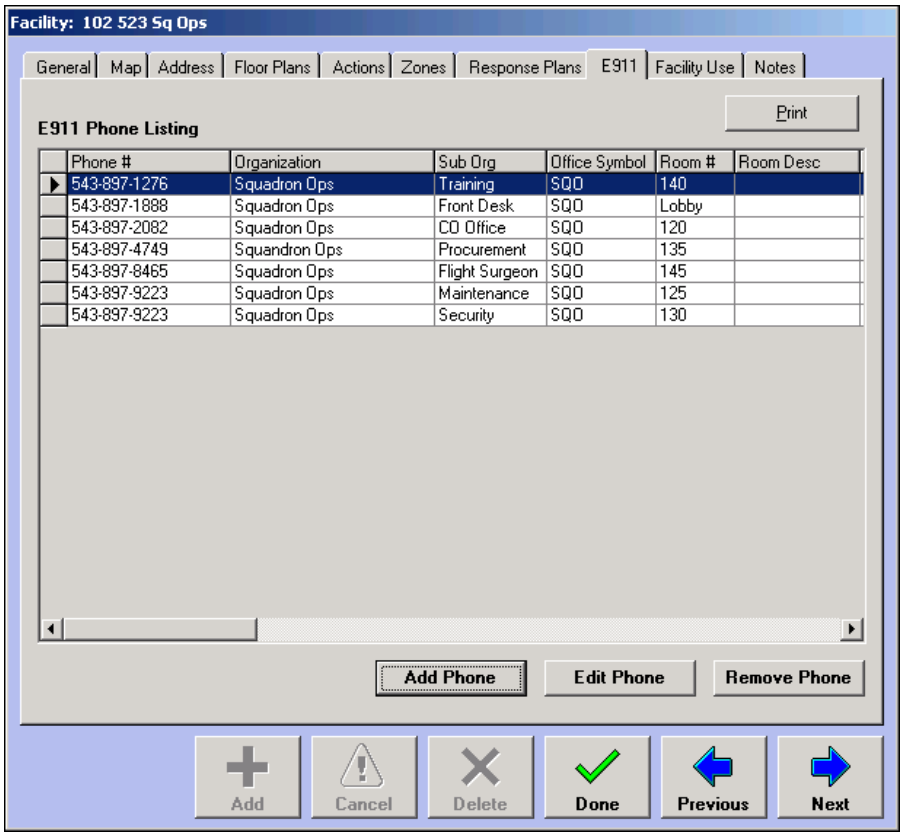
3 Click **Done**.

To edit a phone number in the E-911 database

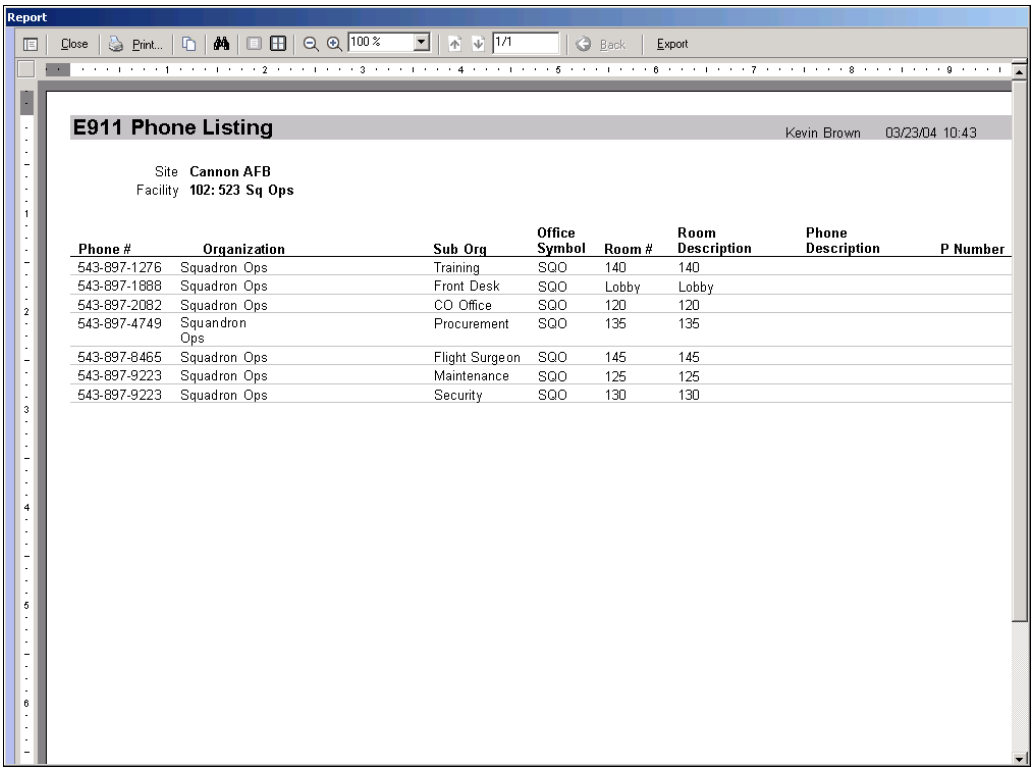
1 In the tree pane, display the E-911 RID or the facility where the phone is located.
2 Right-click the RID or facility to display the edit dialog box for the item.
3 Click the E911 tab.
4 Select the phone number you want to edit.
5 Click **Edit Phone**. The Edit E911 Phone Listing dialog box appears.
6 Make the desired changes to the phone number information.
7 Click **Done**.

To print a facility's E-911 phone numbers

1 In the tree pane, right click the facility you want to print. The Facility dialog box appears.
2 Click the E911 tab.



3 Click **Print**. The Report Viewer appears.



4 In Report Viewer, click **Print**. For more information on using the Report Viewer, see the D-21 Incident Client User Guide (P/N 001-392-00).

Section 11
Configuring Tone Alerting

Read this section to learn how to configure tone alerting with a Tone Generator or a Tone Alert Unit.

Contents

Configuring Tone Alerting with a Tone Generator 11-2
Configuring Tone Alerting with a Tone Alert Unit 11-6

Configuring Tone Alerting with a Tone Generator

The Tone Generator is a legacy interface allowing D-21 Incident Client operators to manually control a D-21 Tone Alerting Panel. The Tone Generator requires the following configuration in the D-21 Admin Client:

- Add the TGU (Tone Generator) RID and remote unit to the database. See the D-21 Remote Interface Driver Guide (P/N 001-399-01) for information on configuring this RID and remote unit.
- Create a tone sequence for each tone you want to play from the D-21 Incident Client.
- Group the sequences into sequence lists that can be displayed in the Tones viewer in the D-21 Incident Client.

A tone sequence is made up of the following components:

Pre-strobe The pre-strobe is a visual signal that precedes the audible main tone, and is optional when you create a tone sequence. If used, the duration of the strobe is set globally for all tone sequences.

Pre-tone The pre-tone is an audible signal that precedes the audible main tone, and is optional when you create a tone sequence. If used, the type of tone and duration of the pre-tone are set globally for all tone sequences.

Main tone The main tone is an audible signal and duration that are unique to the tone sequence. A main tone and duration are required when you create a tone sequence.

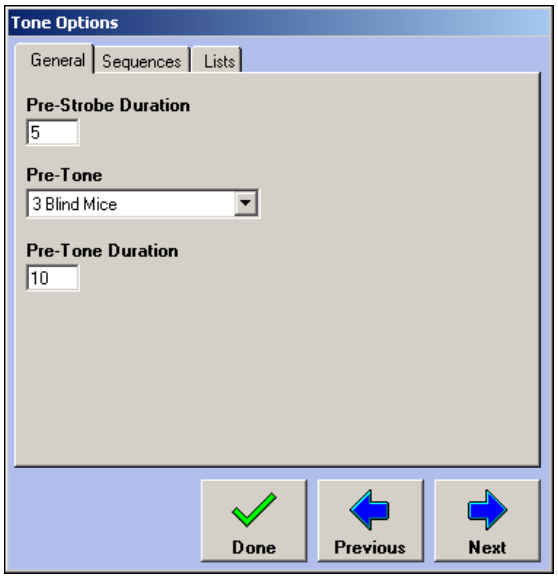
A tone sequence list is made up of multiple tone sequences that are grouped together for playing in the D-21 Incident Client.

To configure global Tone Generator settings

Before You Begin

Add the TGU (Tone Generator) RID and one TG-1 remote unit to the database. See the D-21 Remote Interface Driver Guide (P/N 001-399-01).

1 Select **Devices > Tone Generator**. The Tone Options dialog box appears.



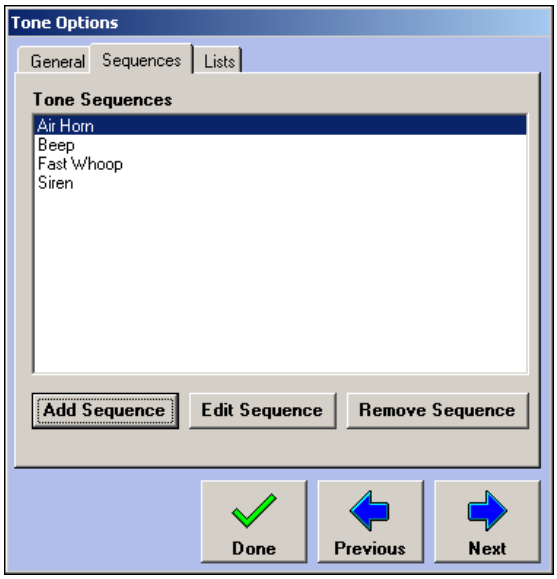
- **Pre-Strobe Duration** The duration of the optional strobe phase of a tone sequence. The duration can range from 0 to 60 seconds. If you define a tone sequence to include a pre-strobe, it will use this pre-strobe duration. See "To create a tone sequence for the Tone Generator" on page 11-3.
- **Pre-Tone** The sound that is played as the pre-tone phase of a tone sequence. If you define a tone sequence to include a pre-tone, it will play this pre-tone. See "To create a tone sequence for the Tone Generator" on page 11-3.
- **Pre-Tone Duration** The duration of the optional pre-tone phase of a tone sequence. The duration can range from 0 to 60 seconds. If you define a tone sequence to include a pre-tone, it will use this pre-tone duration. See "To create a tone sequence for the Tone Generator" on page 11-3.

2 When you have completed your changes, click **Done**.

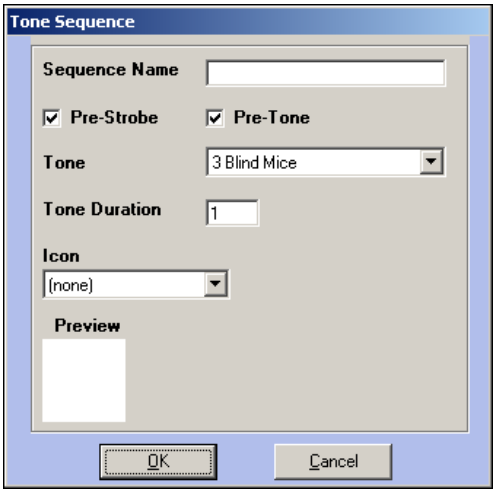
NOTE *When you edit a pre-strobe or pre-tone setting, you must reload the TGU RID before the changes take effect.*

To create a tone sequence for the Tone Generator

1 Select **Devices > Tone Generator** and click the Sequences tab.



2 Click **Add Sequence**.



- **Sequence Name** Enter a name for the tone sequence.
- **Pre-Strobe** Select this option if you want the sequence to start with the pre-strobe signal. The duration for the pre-strobe signal is set globally for all sequences. See "To configure global Tone Generator settings" on page 11-2.
- **Pre-Tone** Select this option if you want the sequence to include the global pre-tone audible signal. The pre-tone starts at the end of the pre-strobe duration, if used. The sound used for the pre-tone and its duration are set globally for all sequences. See "To configure global Tone Generator settings" on page 11-2.
- **Tone** Select the main tone for the tone sequence. This tone is played after the pre-strobe and pre-tone signals.
- **Tone Duration** Enter the number of seconds (from 1 to 90) you want the tone to play.
- **Icon** Select an icon to represent the tone sequence when it is placed on a sequence list. You can view the selected image in the Preview box. For more information on using graphic files, see "Adding Media Files" on page 5-1.

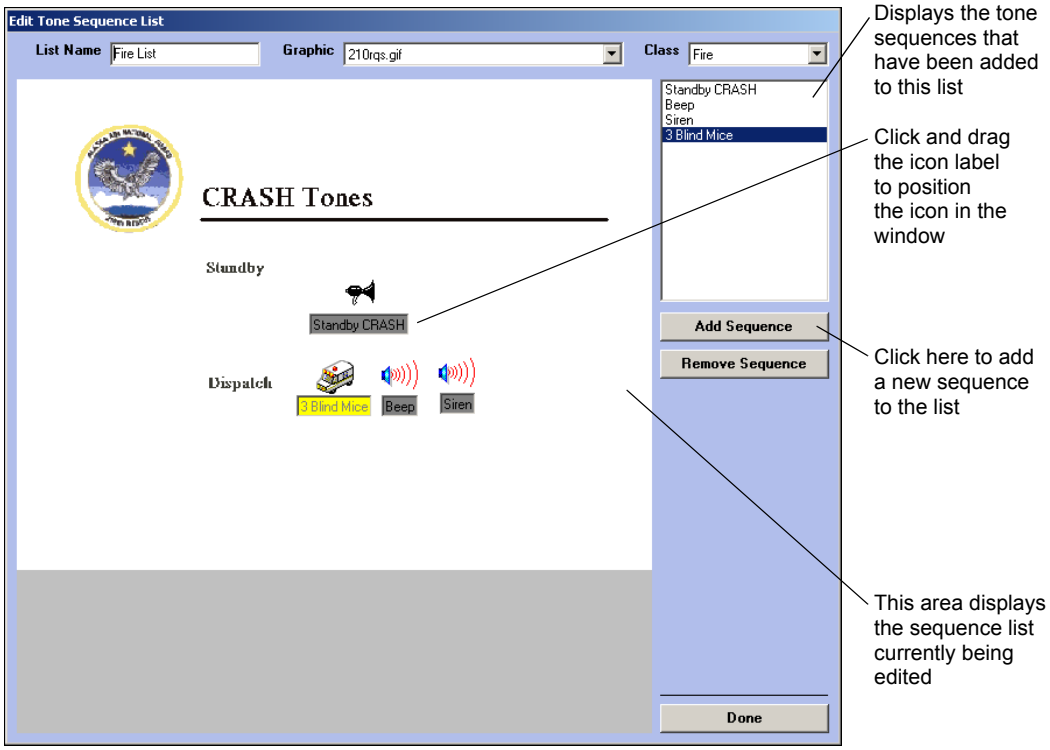
3 When you are finished, click **OK**.

NOTE *When you add a new sequence or edit an existing sequence, you must reload the TGU RID before the sequence can be activated in the D-21 Incident Client.*

To create a tone sequence list for the Tone Generator

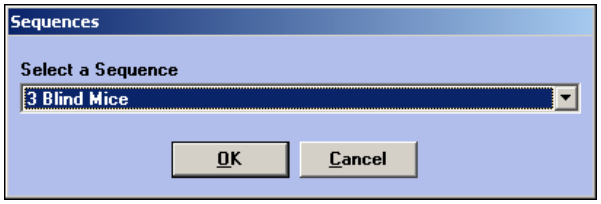
1 Select **Devices > Tone Generator** and click the Lists tab.

2 Click **Add List**. The Edit Tone Sequence List dialog box appears.



- **List Name** Enter a name for the list of tone sequences.
- **Graphic** Select a graphic for the sequence list if you want an image displayed behind the tone sequences. Place graphics you want to use for the sequence list background in `C:\Program Files\D21\Media\FloorPlans`. For more information, see "Adding Media Files" on page 5-1.
- **Class** Select Fire, Security, or All to specify which workstations will display this tone list and its sequences. If you select Fire, the tone list will only be displayed on workstations with the Fire Client enabled. If you select Security, the list is only available on workstations with the Security Client enabled. If you select All, the tone list will be available on both Fire and Security workstations.
- **Add Sequence** Displays the Sequences dialog box. Use the Sequences dialog box to select each tone sequence you want to add to the sequence list.
- **Remove Sequence** Deletes the selected tone sequence from the tone sequence list.

3 Click **Add Sequence**.



4 Select the tone sequence in the drop-down list. You can add the same tone sequence to more than one sequence list.

5 Click **OK**. The tone sequence icon and label are displayed in the sequence list area.

6 Click and drag the icon label to position the tone sequence where you want it to appear in the sequence list area. The tone sequences are displayed in the D-21 Incident Client exactly the way you arrange them here.

7 Click **Add Sequence** to add additional tone sequences to the sequence list as necessary.

8 Click **Done** when you are finished creating the sequence list.

Configuring Tone Alerting with a Tone Alert Unit

The Tone Alert Unit allows D-21 Incident Client operators to manually activate tone sequences, just as the Tone Generator does. Additionally, it allows tone sequences to be assigned to incident classes so a particular sequence will be played automatically when resources are dispatched to an incident of that class. When the D-21 Text-to-Speech option is also enabled, the Tone Alert Unit can announce the resources assigned to the incident, the incident class and topic, and the incident location after the tone sequence plays.

The Tone Alert Unit requires the following configuration in the D-21 Admin Client:

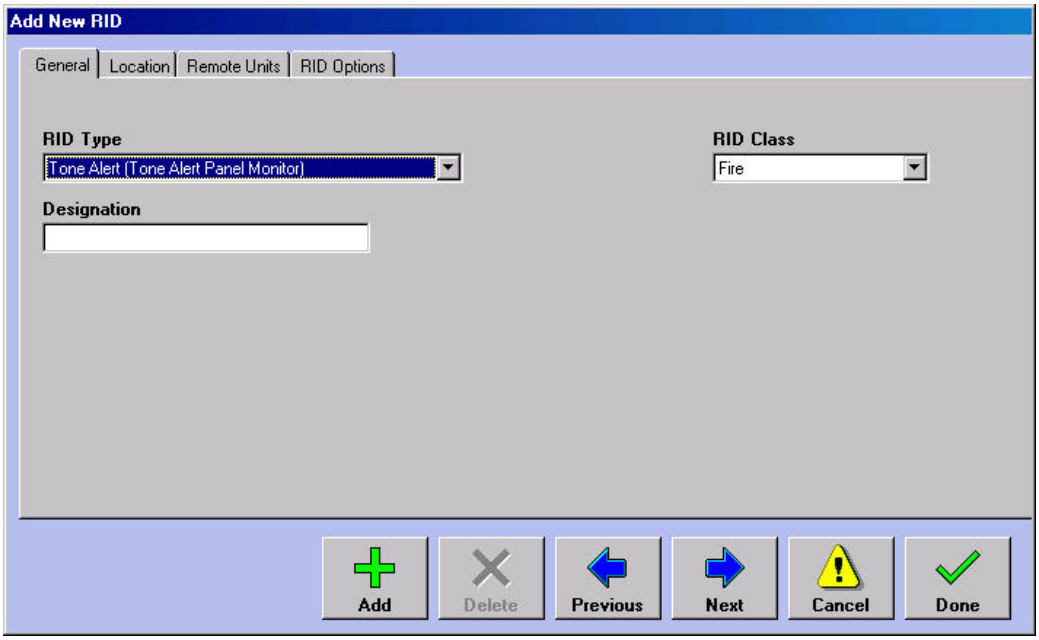
- Add the Tone Alert RID. See "To add a Tone Alert RID" on page 11-7.
- Add the Tone Alert Unit. See "To add a Tone Alert Unit" on page 11-9.
- Create a tone sequence for each tone you want the unit to play. See "To create a tone sequence for the Tone Alert Unit" on page 11-11.
- Group the sequences into tone lists that can be displayed in the Tone Alert viewer in the D-21 Incident Client. See "To create a tone sequence list for the Tone Alert Unit" on page 11-13.

For automatic activation of tone sequences when resources are dispatched, these additional configuration steps are required in the D-21 Admin Client:

- Assign tone sequences to incident classes for automatic tone alerting. See "To assign automatic tone sequences to incident classes" on page 11-15.
- Create the resources to be dispatched and designate their home facility as the facility in which the Tone Alert Unit is located. See "To add a resource" on page 2-103.
- If necessary, create custom Text-to-Speech entries for facilities to supplement the announced address information in the event of an incident. See "To create custom Text-to-Speech entries for facilities" on page 11-18.

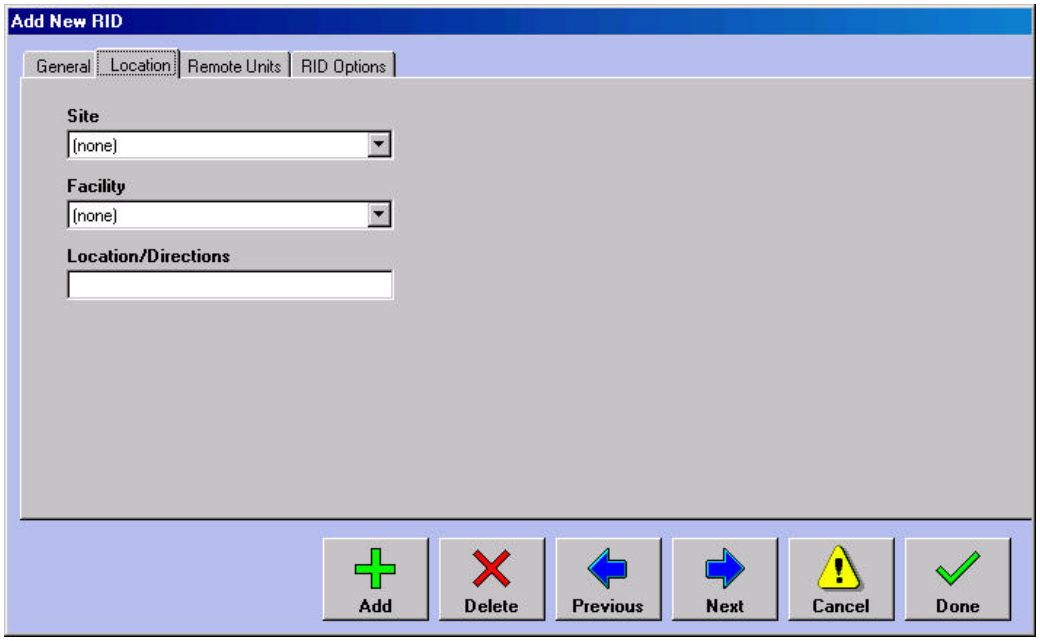
To add a Tone Alert RID

1. Select **Add > RID**. The Add New RID dialog box opens.
2. Select Tone Alert (Tone Alert Panel Monitor) from the RID Type drop-down list.



- **Designation** Provide a recognizable name for the RID.
- **RID Class** Select the appropriate class for the RID.

3 Click **Next** to advance to the Location tab.



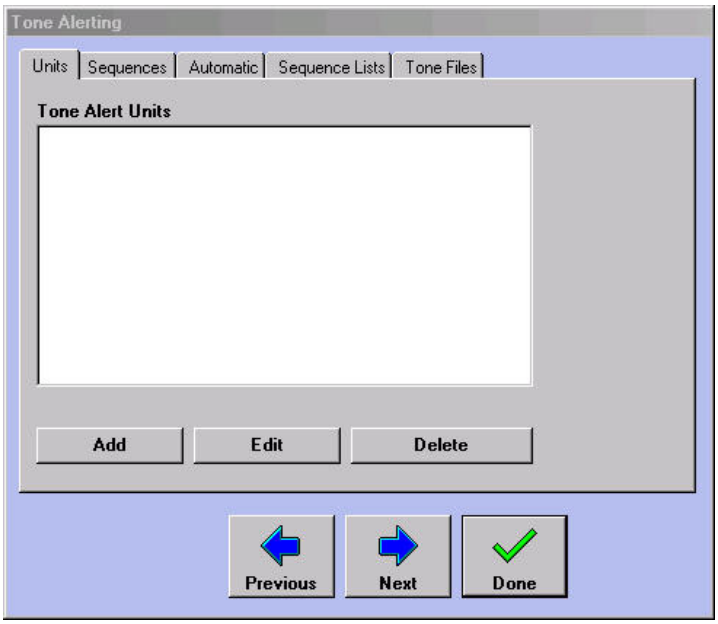
- **Site** Select the appropriate site for the RID.
- **Facility** Select the appropriate facility for the RID.
- **Location/Directions** Provide any additional information desired about the RID's location.

4 Click **Done** to create the Tone Alert RID.

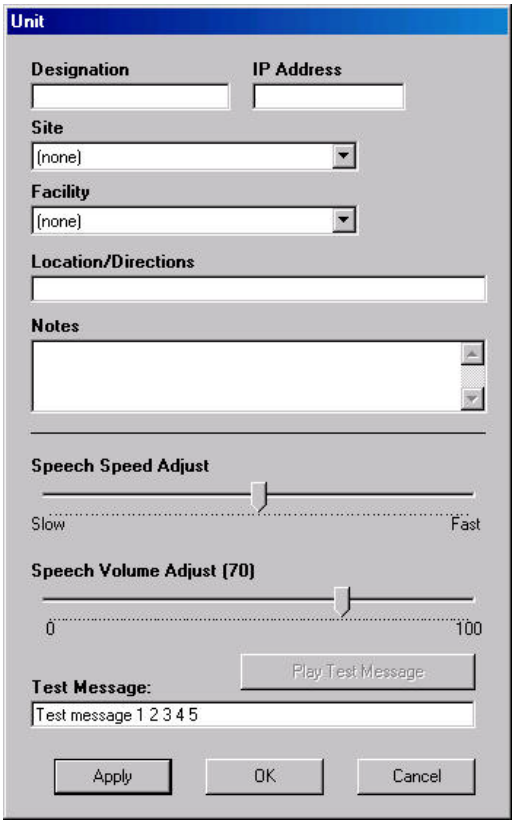
To add a Tone Alert Unit

Before You Begin: Make sure the facility where the Tone Alert Unit will be located has been entered into the D-21. See "To add a facility" on page 2-13.

1 Select **Devices > Tone Alerting**. The Tone Alerting dialog box opens with the Units tab selected.



2 Click **Add**. The Unit dialog box opens.



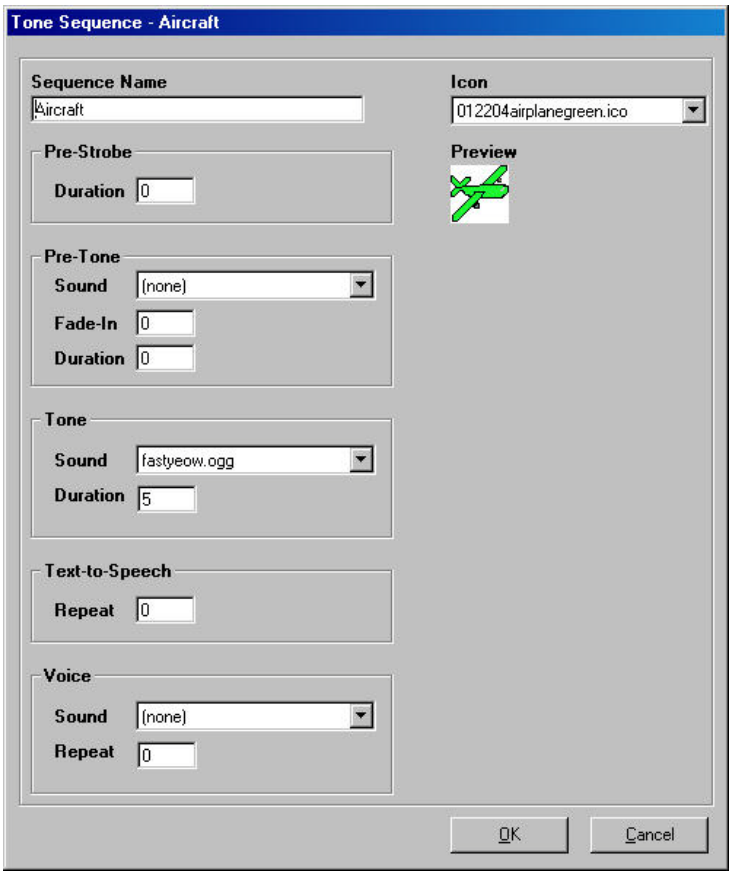
- **Designation** A recognizable name for the Tone Alert Unit.
- **IP Address** The unit's IP address, as programmed by Monaco and marked on the unit. Contact Monaco if you cannot find the unit's IP address.
- **Site** The site where the unit is located.
- **Facility** The facility where the unit is located.
- **Location/Directions** Additional information used to specify where the unit is located.
- **Notes** Any additional information about the unit.
- **Speech Speed Adjust** Click and drag the slider to adjust the speed at which dispatch information will be announced, if Text-to-Speech is enabled. See "To assign automatic tone sequences to incident classes" on page 11-15.
- **Speech Volume Adjust** Click and drag the slider to adjust the volume at which dispatch information will be announced, if Text-to-Speech is enabled. See "To assign automatic tone sequences to incident classes" on page 11-15.
- **Test Message** The text that will be announced at the Tone Alert Unit when a test of Text-To-Speech is conducted. See "To test Text-To-Speech for the Tone Alert Unit" on page 11-16.

3 Enter the following required information for the unit: Designation, IP Address, Site, Facility. Enter additional information if needed.

4 Click **OK** when you are done.

To create a tone sequence for the Tone Alert Unit

1. Select **Devices > Tone Alerting**. The Tone Alerting dialog box opens with the Units tab selected.
2. Click the Sequences tab.



- **Sequence Name** A recognizable name for the tone sequence.
- **Icon** A symbol for the sequence to appear on sequence lists in the D-21 Incident Client. The Preview area displays the icon selected in the drop-down. For more information on using graphic files, see "Adding Media Files" on page 5-1.
- **Pre-Strobe** An optional visual signal initiated when the sequence begins. A pre-strobe can be used to provide a gentle wake-up.
  - **Duration** Length of time in seconds that the pre-strobe will fire. The maximum is 60 seconds.

- **Pre-Tone** A sound that precedes the main tone. The pre-tone can be used to provide a gentle wake-up before the main tone plays.
  - **Sound** The audio file played before the main tone. This list contains all the sounds installed on the Tone Alert Unit.

NOTE *You can preview the sounds installed on the Tone Alert Unit in the D-21 Incident Client. See the D-21 Incident Client User Guide (P/N 001-392-00) for more information.*

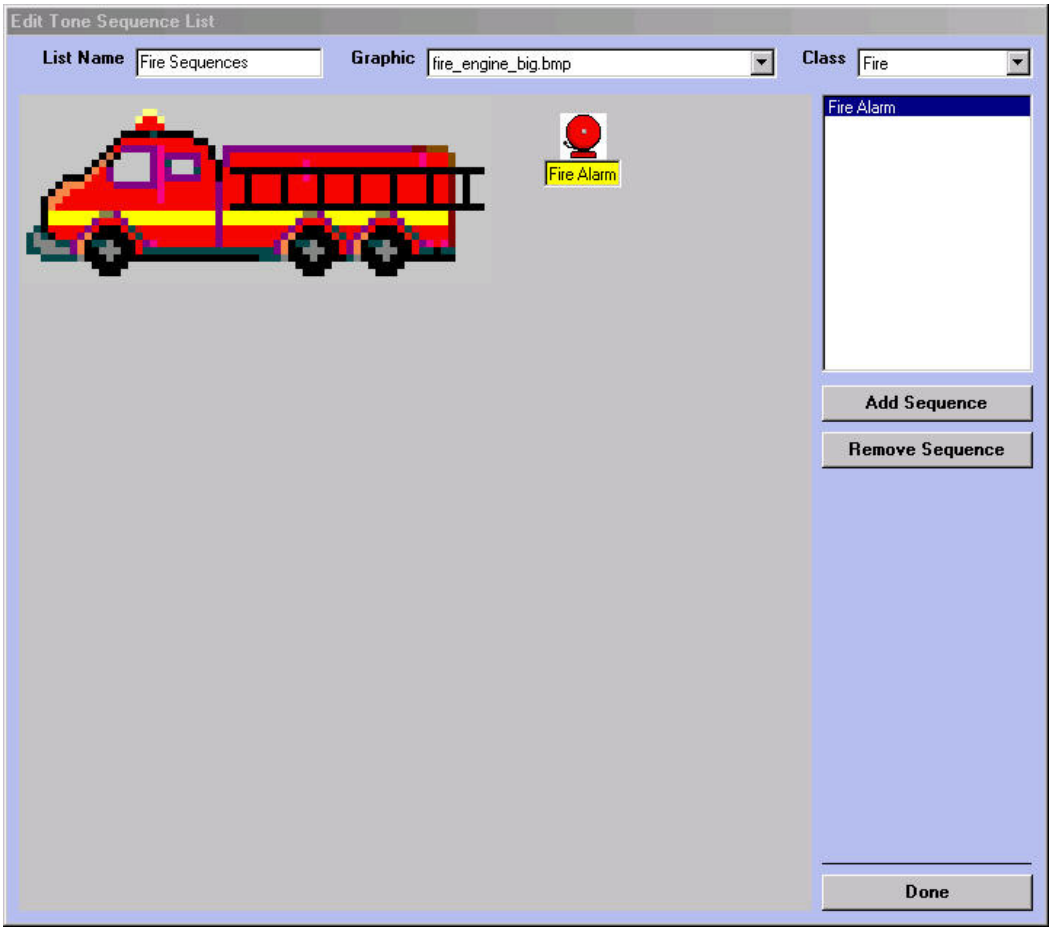
  - **Fade-In** Length of time, in seconds, the pre-tone gradually increases in volume before it reaches full volume. The maximum is 60 seconds.
  - **Duration** Length of time, in seconds, the pre-tone will play at full volume. The maximum is 60 seconds.
- **Tone** The main sound of the sequence.
  - **Sound** The audio file played as the tone. This list contains all the sounds installed on the Tone Alert Unit.
  - **Duration** The length of time in seconds the tone will play. The maximum is 60 seconds.
- **Text-to-Speech** Option that announces the resources assigned to the incident, the incident class and topic, and the incident location after the tone sequence plays.
  - **Repeat** The number of times the incident location and dispatched resource names should be repeated after the sequence plays. The default value is '0', which means the text will be annunciated only once (i.e. it will not be repeated). This setting applies only to sequences assigned to incident classes for automatic activation. See "To assign automatic tone sequences to incident classes" on page 11-15.
- **Voice** A pre-recorded voice message installed on the tone alert unit that can be added to the tone sequence and played after the main tone has finished.
  - **Sound** The voice message played after the main tone. This list contains all the voice messages installed on the Tone Alert Unit.
  - **Repeat** Number of times the voice message is repeated. The default value is '0', which means the text will be annunciated only once (i.e. it will not be repeated). The maximum is 9.

NOTE *Consult Monaco technical support if you wish to install additional sounds or pre-recorded voice messages on the Tone Alert Unit. See also "To add new sound or voice files for assignment to tone sequences" on page 11-14.*

3. Enter the following required information for the tone sequence: Sequence Name, Tone Sound and Tone Duration. Enter additional information if required.
4. Click **OK** when you are done.

To create a tone sequence list for the Tone Alert Unit

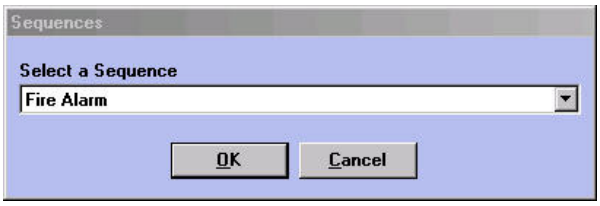
1. Select **Devices > Tone Alerting**. The Tone Alerting dialog box opens with the Units tab selected.
2. Select the Sequence Lists tab and click **Add**.



- **List Name** A meaningful name for the tone sequence list.
- **Graphic** An image file used to provide a background for the sequence icons, if needed. The files in this list are from the `C:\Program Files\D21\Media\FloorPlans` directory. The default is None.
- **Class** Governs which D-21 Incident Client workstations can view the sequence list, either Fire Client only, Security Client only, Facility Management client only, or all clients. The default is All.

3. Provide a name for the tone sequence list.

4 Click **Add Sequence** to bring up the select a sequence dialog box.



5 Select a sequence you wish to add to the sequence list from the drop-down list. The list contains all the sequences defined on the Sequences tab of the Tone Alerting dialog box. You can add the same tone sequence to more than one sequence list.

6 Click **OK** to close the dialog box. The sequence name appears in the list box above the Add Sequence button, and an icon representing the sequence appears in the sequence list area. Click and drag the icon to position it where it is needed.

7 Click **Add Sequence** again to add additional sequences to the sequence list. If you need to remove a sequence, select it in the list box and click **Remove Sequence**.

8 When you are finished, click **Done**.

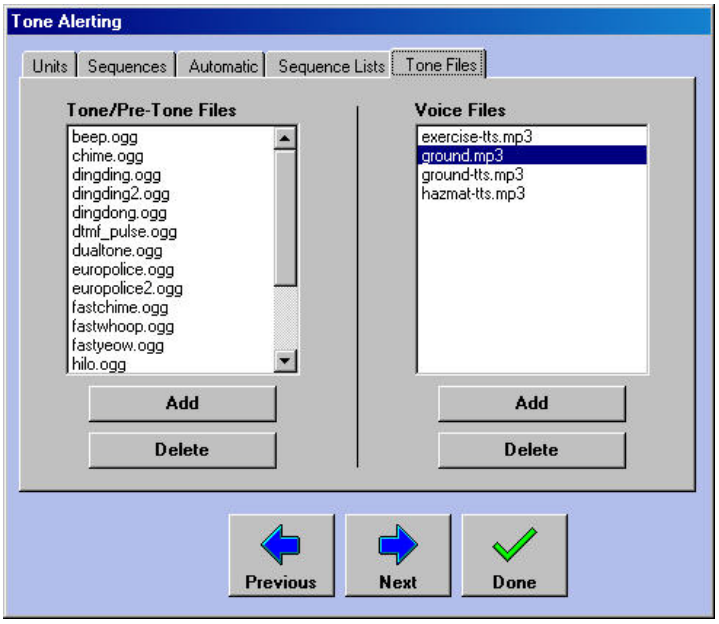
To add new sound or voice files for assignment to tone sequences

If additional sound or voice files are installed on the Tone Alert Unit, they must be recorded in the D-21 database before they can be used in a tone sequence.

NOTE *Consult a Monaco technical representative for assistance with installing new sound or voice files on the Tone Alert Unit.*

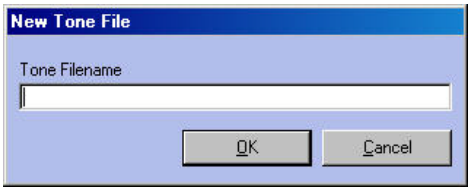
1 Select **Devices > Tone Alerting**. The Tone Alerting dialog box opens with the Units tab selected.

2 Select the Tone Files tab.



3 Two **Add** buttons are available on this tab, one for adding sound files to be used for pre-tones and tones, and one for adding voice files. Click the appropriate button.

4 Type the name of the new file exactly as it was installed on the Tone Alert Unit, including the three-letter file extension, in the dialog box that appears. Click **OK**.



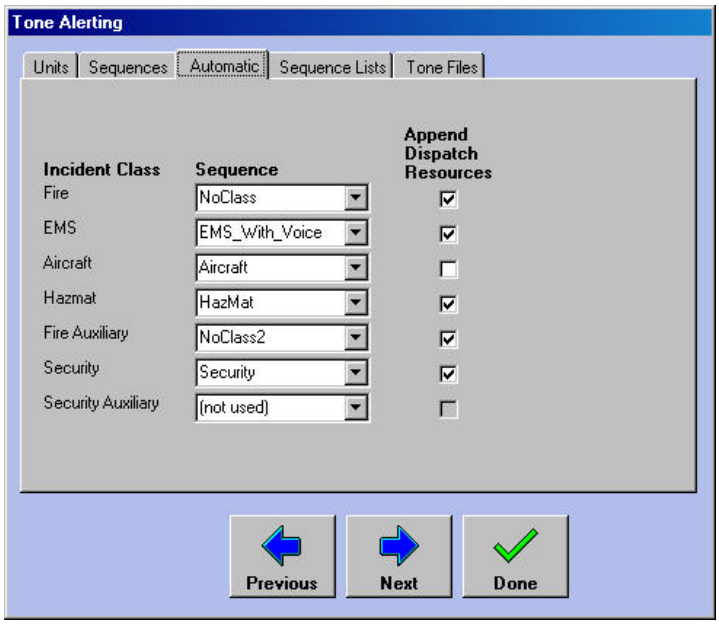
5 After the dialog box closes, the new file will appear in the appropriate list box. Continue adding files as necessary.

6 When you are finished, click **Done** to close the Tone Alerting dialog box.

To assign automatic tone sequences to incident classes

1 Select **Devices > Tone Alerting**. The Tone Alerting dialog box opens with the Units tab selected.

2 Select the Automatic tab.



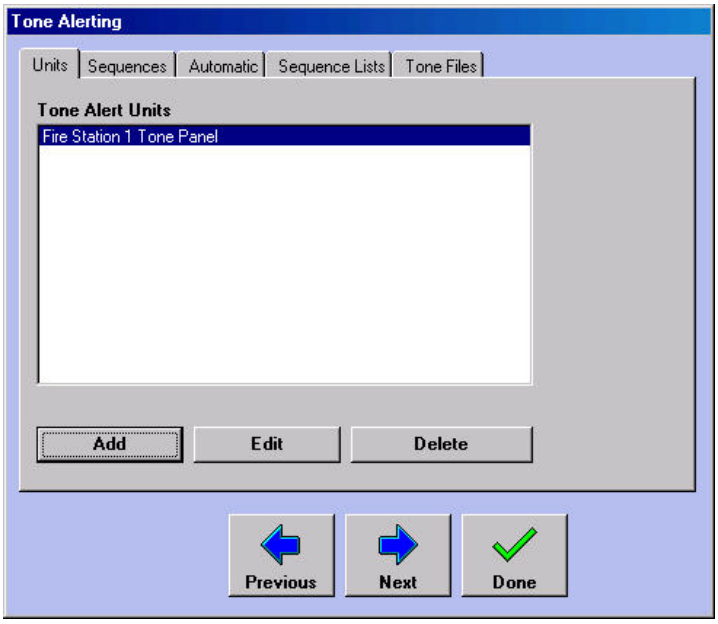
- **Sequence** The Sequence drop-down list displays the tone sequence, for each incident class, which will be automatically played when resources from the facility containing the Tone Alert Unit are dispatched to an incident. The drop-down list contains all the sequences defined on the Sequences tab. The same sequence can be assigned to more than one incident class.
- **Append Dispatch Resources** If checked, the dispatched resource names will be included in the text-to-speech announcement played after the tone sequence has completed.

3 Assign sequences to incident classes as needed. When you are finished, click **Done**.

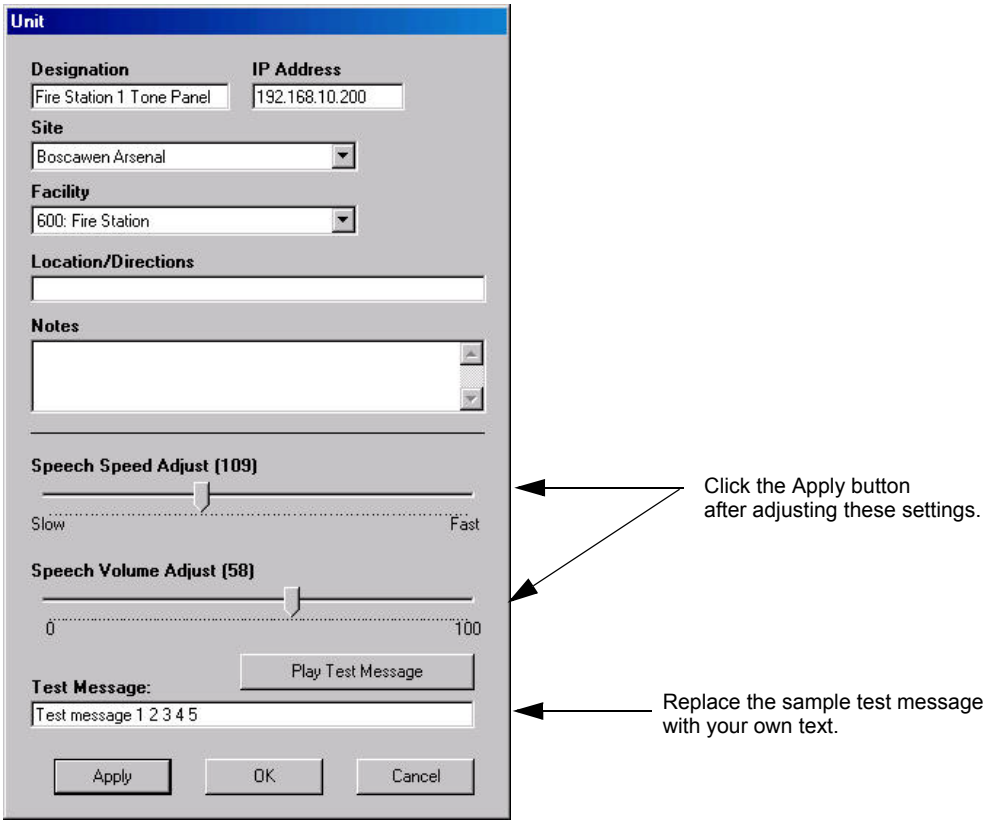
To test Text-To-Speech for the Tone Alert Unit

If you are using the Tone Alert Unit to announce the names of dispatched resources, you may need to test and adjust the Text-To-Speech feature.

1 Select **Devices > Tone Alerting**. The Tone Alerting dialog box appears with the Units tab selected.



2 Select the unit for which you are testing Text-To-Speech and click **Edit**. The Unit dialog box appears.



3 Click **Play Test Message** to hear the sample test message announced at the Tone Alert Unit. If you wish, you can replace the sample test message with your own text.

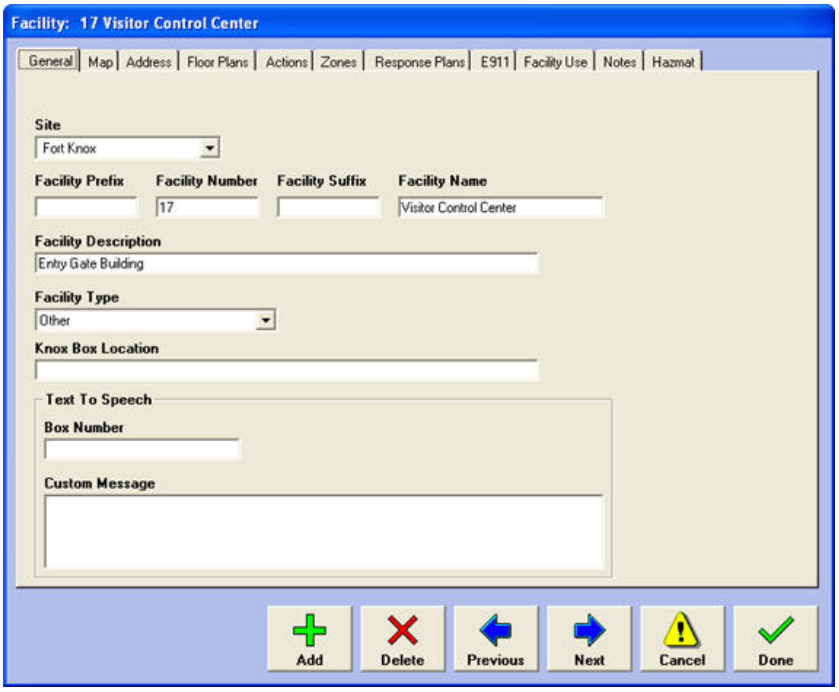
4 If necessary, use the Speech Speed Adjust and Speech Volume Adjust sliders to modify the way the test message sounds at the Tone Alert Unit. Click Apply after each adjustment and retest.

5 When you are finished, click **OK** to save the new speed and volume settings.

6 Click **Done** to close the Tone Alerting dialog box.

To create custom Text-to-Speech entries for facilities

1 Expand the Sites tree in the left pane of the Admin Client and right-click the desired facility. The facility's properties dialog box is displayed, with the General tab selected.



NOTE *Contact Monaco technical support for assistance if the Text To Speech area does not appear.*

2 In the Text to Speech area, enter the box number to be announced in the **Box Number** field.

3 Enter additional information that should be announced at the Tone Alerting Unit when resources are dispatched to an incident at the facility in the **Custom Message** text box.

4 When you are finished, click **Done**.

Section 12
Configuring Cameras and Remote Displays

Read this section for information on setting up the D-21 Incident Client's Camera Viewer and the View Generator.

Contents

Configuring the Camera Viewer 12-2
Configuring the View Generator 12-2

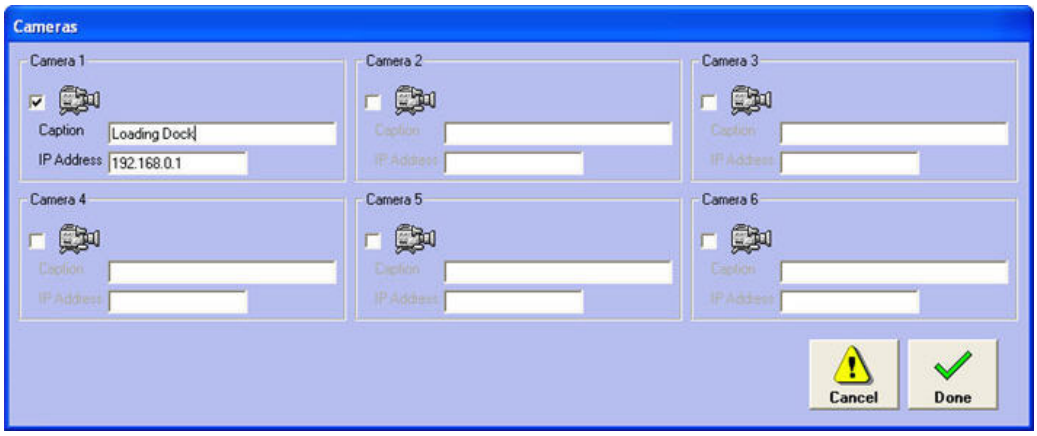
Configuring the Camera Viewer

The Camera viewer in the D-21 Incident Client displays the feed from up to six video cameras connected to the same network as the D-21. The viewer window is divided into six equal sections. To enable the camera feed in a section, you must first enable the camera, enter a caption to identify the camera feed, and enter the internet protocol (IP) address for the camera.

Refer to the online help available with the network camera software for more information about setting up the camera on the network.

To set up cameras for the Camera viewer

1 Select **Devices > Cameras**. The Cameras dialog box appears.



2 Select the check box next to the camera you want to enable. The Caption and IP Address fields become available.

3 Enter a title for the pane in the Caption field. This text will appear in a banner across the top of the camera feed.

4 Enter the IP address of the camera in the IP Address field. This is the address of the camera on the network.

5 Click **Done**.

Configuring the View Generator

A View Generator is a special client workstation designed for installation in locations where a quick status overview of D-21 activities is useful. It is a non-interactive client which automatically logs in to the D-21 and requires no user input. Once a View Generator has been configured, additional copies of its screen can be populated to View Generator Repeater Displays at other locations.

The content displayed on a View Generator varies depending on whether there are active incidents. When there are no active incidents, the View Generator can display the site map, the Notes of the Day, or the day's roster, or, if needed, the View Generator can be configured to cycle through two or all three of these views. When an active incident exists, the View Generator automatically displays a special incident view containing the site map and basic

information about the incident (incident class and topic, facility and address information). Incident notes can also be displayed. When multiple active incidents exist, the View Generator display cycles through each active incident in turn.

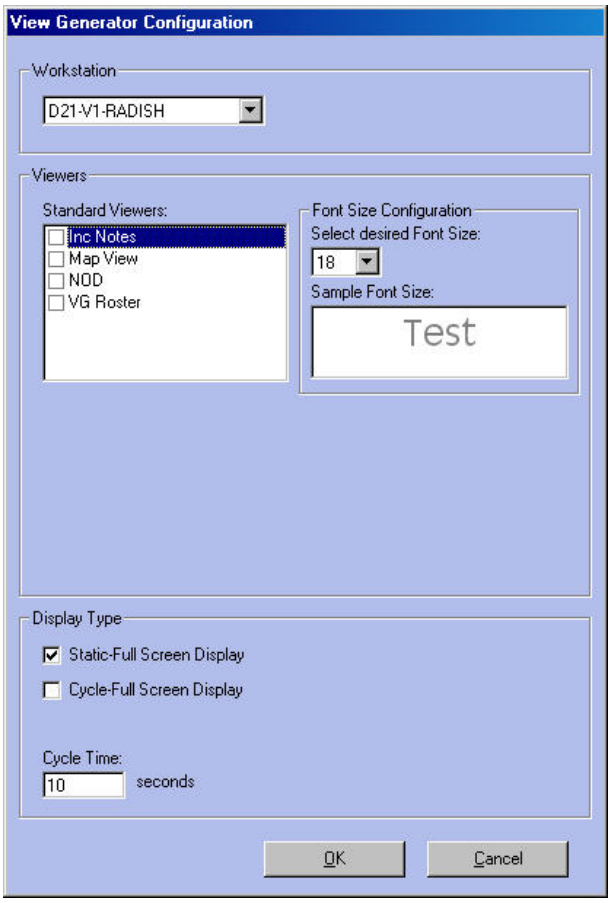
In order to configure a View Generator with Repeater Displays, the following activities must be completed in the D-21 Admin Client:

- Define the content that will appear on the View Generator. This can include the D-21 map, Notes of the Day, and rosters. The content can be static, or it can cycle through a series of screens in a preset amount of time. See "To define content for the View Generator" on page 12-4.
- Add any View Generator Repeater Displays to the D-21 database. See "To add a View Generator Repeater Display" on page 12-5.
- Assign each View Generator Repeater Display to the controlling View Generator. See "To assign a View Generator to a View Generator Repeater Display" on page 12-6.

IMPORTANT *Before a View Generator can be configured in the D-21 Admin Client, it must connect to the primary server over the network. Consult Monaco technical support for assistance with bringing a View Generator online if necessary.*

To define content for the View Generator

1 Select **Devices > View Generator**. The View Generator Configuration dialog box opens.



2 Select the View Generator from the **Workstation** drop-down list.

3 Click the check boxes in the **Standard Viewers** list box so check marks appear, if required.

- **Inc Notes** Check this option to display incident notes, if available, for any active incidents on the View Generator.
- **Map View** Checking this option will display the View Generator on the D-21 Incident Client map.
- **NOD** Checking this option will display the Notes of the Day on the View Generator, provided there are no active incidents. See the D-21 Incident Client User Guide (P/N 001-392-00) for information about adding Notes of the Day.
- **VG Roster** Checking this option will display the daily roster on the View Generator, provided there are no active incidents. See the D-21 Incident Client User Guide (P/N 001-392-00) for information about defining the daily roster.

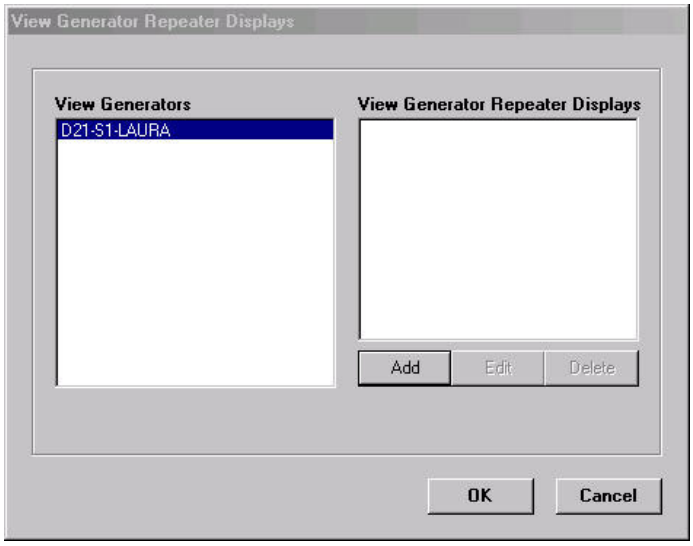
4 After checking a viewer box, set the font size for the viewer in the **Font Size Configuration** area by selecting it from the **Select Desired Font Size** drop-down list.

5 If you have checked more than one viewer box, check the **Cycle Full Screen Display** option and set a **Cycle Time**. The View Generator will automatically display each of the checked viewers, in turn, for the duration of the Cycle Time value.

6 When you are finished, click **OK**.

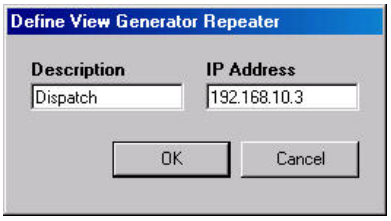
To add a View Generator Repeater Display

1 Select **Devices > View Generator Displays**. The View Generator Repeater Displays dialog box opens, and available View Generator client workstations are listed in the **View Generators** pane.



NOTE *You cannot add View Generator Repeater Displays until a View Generator client workstation has logged in to the D-21 network.*

2 Click **Add** to open the Define View Generator Repeater dialog box.



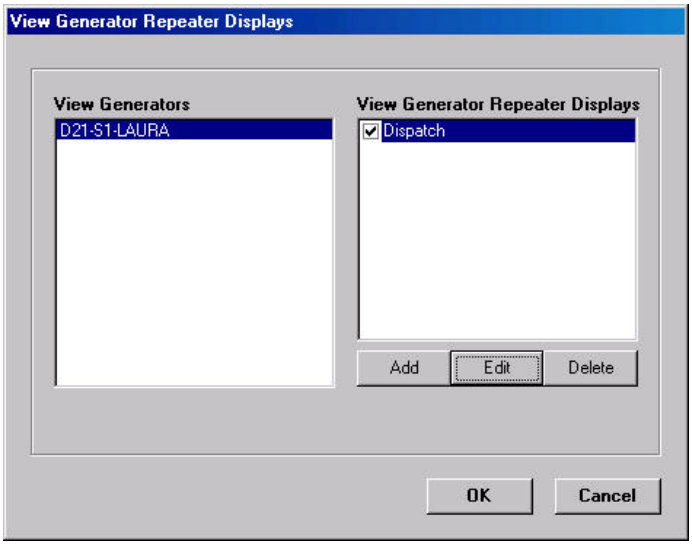
3 Enter a recognizable name for the View Generator Repeater Display in the **Description** text box.

4 Enter the **IP Address** of the View Generator Repeater Display. This address was programmed by Monaco and is marked on the View Generator Repeater Display unit. Consult Monaco support for help with this step, if necessary.

5 Click **OK** to close the dialog box and save the View Generator Repeater Display definition.

To assign a View Generator to a View Generator Repeater Display

1 Select **Devices > View Generator Displays**. Any View Generator Repeater Displays added will appear in the View Generator Repeater Displays list box. See "To add a View Generator Repeater Display" on page 12-5.



2 Select the View Generator workstation whose display will be populated to a View Generator Repeater Display in the **View Generators** list box.

3 Click the check box next to the View Generator Repeater Display to associate with the selected View Generator.

4 Click **OK**.

Section 13
Remote Access

Read this section to learn how to set up your computer for remote access by Monaco Help Desk personnel.

Contents

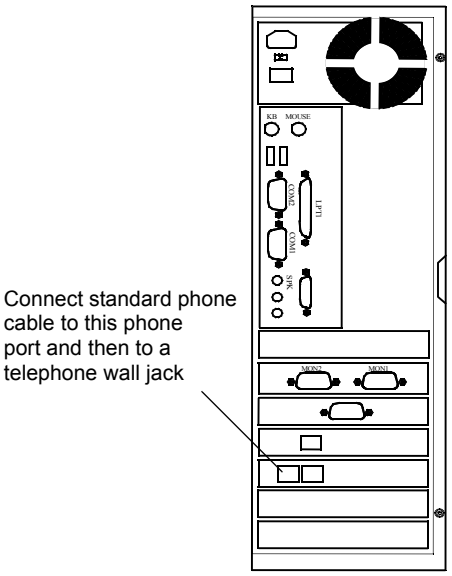
Using pcAnywhere. 13-2

Using pcAnywhere

Use Symantec pcAnywhere to allow D-21 Help Desk personnel to remotely connect to your D-21 server for troubleshooting and problem-solving purposes. A Monaco representative will tell you when use of this tool is recommended.

To make your computer accessible to a Monaco product support specialist

1. Connect the Line In phone port on the back of the computer to a telephone wall jack using a standard telephone cable.



2. Log in to Windows as the Administrator.
3. Double-click the Monaco pcAnywhere icon on the Windows Desktop. This icon is only visible on the Desktop if you are logged in as Administrator.
4. Provide the Monaco representative with the phone number for the telephone wall jack to which the D-21 computer is connected.

Appendix A
Glossary of Terms

Contents

Glossary of Terms A-2

Glossary of Terms

Name	Description
ACS	Access Control System
Action	An administrator-defined process that can be manually or automatically initiated
Bi-State Output	Output type that toggles on and off with successive activations
BT	Building Transceiver
Carrier Delay	Time during which the transceiver pauses to await a transmission
CPS-484	Monitored charger for backup power supply
CPU	Central Processing Unit
Dongle	Hardware device that prevents illegal software use by rendering the software inoperable when the device is not plugged into a printer port
DTMF	Dual Tone Multi-Frequency (radio transmission protocol)
EMS	Emergency Medical System
FACP	Fire Alarm Control Panel
FSK	Frequency Shift Keying (radio transmission protocol)
ID	Identification
IDS	Intrusion Detection System
IOM	Installation, Operation, and Maintenance
IP	Internet Protocol
MNS	Mass Notification System
Momentary Output	Output type that activates briefly and then deactivates
NFIRS	National Fire Incident Reporting System
NFPA	National Fire Protection Association
Output	Relay device that can be activated from the D-21
PACAF	Pacific Air Force
PDF	Portable Document Format
Poll	D-21 request for information from one or more remote units
Remote Interface Driver	Software that enables the D-21 to communicate with hardware such as RFMs, hardwire modems, and the CPS-484
Remote Signal Activation	Radio activation of a circuit on a remote unit
Remote Unit	Device that includes a transceiver or other mechanism for communicating with the D-21
Response Plan	Administrator-generated emergency course of action associated with a facility, zone, or topic
RFM	Radio Frequency Modem
RID	See Remote Interface Driver
Roster	A list of shifts and duty assignments
RSA	See Remote Signal Activation
SOP	See Standard Operating Procedure

Name	Description
Standard Operating Procedure	A standard or customizable form that can be used to enter information during an incident
Topology	The arrangement in which RFMs are associated with each other
ZID	Identification number for zones on DTMF remote units. Because DTMF zones are recognized by only their ZID number, each ZID number associated with a single RID must be unique.
Zone Position	Identification number for zones on FSK remote units. Because FSK zones are recognized by the remote unit number *and* the zone position number. Zone position numbers start with 1 on each FSK remote unit.
Zone	Physical area associated with a single zone input on a remote unit

Appendix B
Configuration Tables

Contents

Servers B-2
Clients B-3

Servers

Enter the requested information for the main D-21 server computer and, if applicable, the redundant server in this table.

NOTE *There are separate tables for client data. Enter client data in this table only if the server is also used as a client. Otherwise, leave the client boxes blank.*

Date completed _____

Category		Main Server		Redundant Server	
Computer	Monaco P/N				
	Serial Number				
	Windows 2000/XP Product Key				
	IP Address				
	Name				
	Workgroup				
D-21 Software Version	Server				
	D-21 Admin Client				
	D-21 Incident Client				
Printer Brand/Model					
Dual Monitors		Yes	No	Yes	No
Server Key Configuration	Graphics	Yes	No	Yes	No
	Map	Yes	No	Yes	No
	Plume	Yes	No	Yes	No
	Map Centric	Yes	No	Yes	No
	Shortest Route	Yes	No	Yes	No
	Perimeters	Yes	No	Yes	No
	Map Dispatch	Yes	No	Yes	No
	Shared Frequency	Yes	No	Yes	No
	Fire	Yes	No	Yes	No
	Security	Yes	No	Yes	No
	Mass Notification	Yes	No	Yes	No
	Training Version	Yes	No	Yes	No

Category		Main Server	Redundant Server
Client Key Configuration	Fire	Yes No	Yes No
	Security	Yes No	Yes No
	Law Enforcement	Yes No	Yes No
	Mass Notification	Yes No	Yes No
	Map	Yes No	Yes No
	Plume	Yes No	Yes No
	Map Centric	Yes No	Yes No
Version	Shortest Route	Yes No	Yes No
	Perimeters	Yes No	Yes No
	Map Dispatch	Yes No	Yes No
	RFM 5000 Firmware		
	IP Address		
	Alternate IP		
	CPS-484		
Lighthouse Software		Yes No	Yes No
Database Backup/Restore path			

Clients

Enter the data for the D-21 client computers in the following table. Use pencil so the data can be changed. If you use more than two clients, photocopy this page for additional tables

Date completed _____ .

Data Category		Client #1	Client #2
Computer	Monaco P/N		
	Serial Number		
	Windows 2000/XP Product Key		
	IP Address		
	Name		
	Workgroup		
D-21 Software Version	D-21 Admin Client		
	D-21 Incident Client		
Printer Brand/Model			
Dual Monitors		Yes No	Yes No

Data Category		Client #1		Client #2	
Client Key Configuration	Fire	Yes	No	Yes	No
	Security	Yes	No	Yes	No
	Law Enforcement	Yes	No	Yes	No
	Mass Notification	Yes	No	Yes	No
	Map	Yes	No	Yes	No
	Plume	Yes	No	Yes	No
	Map Centric	Yes	No	Yes	No
	Shortest Route	Yes	No	Yes	No
	Perimeters	Yes	No	Yes	No
	Map Dispatch	Yes	No	Yes	No
	Responder Display	Yes	No	Yes	No
	Training Version	Yes	No	Yes	No
Lighthouse Software		Yes	No	Yes	No
Database Backup/Restore path					

Index

A

access control (ACS)
- access groups . . . 8-4
- adding BT-X/ACS (M) . . . 2-53
- assigning cards and PINs . . . 8-24
- aux input status . . . 8-11
- cards and PINs . . . 8-23
- changing card/PINs . . . 8-27
- configuring the BT-X . . . 8-10
- deactivating cards . . . 8-28
- diddled status . . . 8-11
- Door Strike Control readers . . . 8-15
- downloading to remote units . . . 8-20
- duress status . . . 8-11
- forced open status . . . 8-11
- held open status . . . 8-11
- inactive cards . . . 8-29
- intervals . . . 8-7
- lost cards . . . 8-32
- No Entry Confirmation option . . . 8-15
- reader zones . . . 8-11
- schedules . . . 8-6
- stolen cards . . . 8-32
- tamper status . . . 8-11
- tracking active cards . . . 8-30
- tracking card and PIN usage . . . 8-16
- unassigning cards and PINs . . . 8-27, 8-28
- zone types . . . 8-11

access/secure alerts
- acknowledging automatically . . . 3-48

acknowledging alerts automatically . . . 3-45

actions
- adding to facilities . . . 2-17
- adding to response plans . . . 3-15
- adding to zones . . . 2-67
- attaching to custom buttons . . . 3-36
- attaching to RFM 5000 RID . . . 2-36
- attaching to RFM 7000 RID . . . 2-48
- attaching to status changes . . . 3-37
- configuring for BT2-8S zones . . . 9-7
- configuring for BT-XS (M) zones . . . 9-17, 9-21, 9-23
- creating . . . 3-27
- reminders . . . 3-34
- removing . . . 3-35
- renaming . . . 3-35
- RID remote commands . . . 3-29
- running external programs . . . 3-32
- types . . . 3-27

ACU-1000 Radio Switch
- adding RID for . . . 2-30
- configuring for MNS . . . 7-13
- workstation input sources . . . 7-16

ACU-1000 radio switch . . . 7-2

adding
- emergency cards . . . 3-20
- facilities . . . 2-13
- floor plans . . . 2-16
- HazMats . . . 2-106
- hydrants . . . 2-109
- IDS Master unit . . . 9-14
- operators . . . 2-97
- outputs . . . 2-74
- personnel . . . 2-86
- pre-plan templates . . . 3-23
- remote unit groups . . . 2-62
- remote units . . . 2-55
- resources . . . 2-103
- response plan actions . . . 3-15
- response plan HazMats . . . 2-23
- response plans . . . 3-3
- response plans hydrants . . . 3-13
- RFM 5000 RID . . . 2-31
- RFM 7000 RID . . . 2-38
- sites . . . 2-3
- SOPs . . . 3-38
- units . . . 2-51
- vehicles . . . 2-101
- zones . . . 2-65

addresses
- entering . . . 4-3
- fire hydrants . . . 2-110
- General Lists dialog box . . . 2-13
- home addresses for personnel . . . 2-90
- numbering units . . . 2-54
- work addresses for personnel . . . 2-88

Admin Mode operator privileges . . . 2-98

administrators (IDS)
- enrolling iButtons . . . 9-25
- enrolling primary . . . 9-25

aerial
- specifying map zoom levels . . . 2-6

aerial zoom level
- specifying for aerial view on maps . . . 2-6

alarms
- access control . . . 8-11
- actions performed in response to . . . 3-27
- carrier delay . . . 2-33
- customizing sounds for . . . 4-55
- displayed in Alert Manager . . . 3-50
- highest priority alert . . . 3-45
- multiple . . . 3-50
- not acknowledged automatically . . . 3-45
- response plan for . . . 3-2
- security . . . 9-3
- supervisory . . . 2-65
- tamper . . . 9-3

Alert Manager . . . 4-54
- customizing . . . 3-50
- minimized beep interval . . . 3-50

alerts . . . 2-65, 3-46
- acknowledging automatically . . . 3-45
- customizing Alert Manager . . . 3-50
- customizing color of . . . 3-55
- customizing phrases . . . 2-69
- disabling for undefined unit . . . 2-49
- disabling from relay outputs . . . 3-47

displaying alarm ID 3-51
displaying box number 3-51
enabling status change 2-76
from points 3-48
managing multiple 3-50
operator permissions 2-99
output 2-76
playing .wav files 4-55
setting trouble resounds 3-51
suppress duplicate 3-49
workstation options 4-53
alias, changing site label 4-7
apostrophes 1-11
assigning vehicles to personnel 2-94
assignments, rosters 2-86
ATI equipment
adding a BT-X/WAC+ for wide area MNS 2-54
Automatic Vehicle Location (AVL)
selecting resource icons 3-66
Automatic zones
on the BT2-8S 9-3, 9-4
on the BT-XS (M) 9-11, 9-12, 9-21
automating tasks 3-27
auxiliary input, reader status 8-11
auxiliary zones 2-64
disabling alerts and logging 3-46

B

backing up
before quitting 1-5
badging 2-93
entering ID numbers 2-95
battery faults
setting delays 2-61
beeps
customizing for Alert Manager 3-50
bi-state output type 2-75
box numbers 3-51
BT2
adding transceivers 2-55
RFM 5000 ranges 2-33
RFM 7000 ranges 2-44
BT2-0/1/2 2-52
BT2-3 . . . . . 2-52, 2-58
using for DTMF siren controller 2-52
BT2-4 2-52
BT2-7 2-52
BT2-8 2-52
BT2-8S 2-52, 9-4
about 9-2
Automatic zones 9-3, 9-4
Central Initiate zones 9-3
configuring actions for 9-7
Constant Secure zones 9-3
downloading intrusion detection configuration 9-10
Entry/Exit Delay zones 9-3
fire zones on 9-5
Master zones 9-2, 9-4
Two Man Access/Secure zones 9-3
zone types 9-3
BT2-8S-MC 9-2
BT2-R 2-52
BT2-SC 2-33
BT2-SC (DTMF siren controller) 2-52
BT-X
see also *remote units*
adding remote units 6-2
bi-state output type 2-75
Communicator unit 6-2
configuring ACS 8-10, 8-12
configuring BT-X keypads 9-13
configuring IDS 9-14
configuring MNS 7-2
enabling dual comm channels 2-49
using with access control 8-10
BT-X Communicator 2-53
about 6-3, 6-4
dual communication mode 6-3
BT-X iButton Keypads
enrolling 9-24
BT-X/ACS (M) 2-53
BT-X/WAC+
adding for wide area MNS 2-54
BT-XF (16) 2-53
BT-XF (M) 2-53
BT-XM transceivers 7-18
BT-XS (16) 2-53
BT-XS (M) 2-53, 9-21
Automatic zones 9-11
Central Initiate zones 9-11
configuring actions for 9-17, 9-21, 9-23
configuring intrusion detection 9-11
Constant Secure zones 9-11
downloading intrusion detection configuration 9-24
Entry/Exit Delay zones 9-11
Keyswitch zones 9-11
Master zones 9-12
Pre-Authorized EE zones 9-12
Pre-Authorized zones 9-12
recording local settings 9-17, 9-21, 9-23
Two Man Access/Secure zones 9-12
zone types 9-11
BT-XWAC+ 7-18
buttons
attaching actions to 3-36
editing custom 3-37
removing custom 3-36

C

call groups 4-23
call lists, adding to response plans 3-4
Camera Viewer, configuring 12-2
card granted/denied alerts
acknowledging automatically 3-48
Card Templates 4-23
cards (ACS)
assigning 8-24
assigning for access control 8-23
deactivating 8-28
editing assignments 8-27

making inactive for access control 8-29
tracking lost and stolen 8-32
tracking usage 8-30
unassigning 8-27, 8-28
carrier delay time
RFM 5000 2-33
RFM 7000 2-41
central enrollment. See iButton assignments (IDS)
Central Initiate zones
on the BT2-8S 9-3
on the BT-XS (M) 9-11
class
fire auxiliary 2-64
floor plans 2-28
incident 2-99
security auxiliary 2-64
unit 2-52, 2-56
client configuration table B-3
colors, customizing alert classes 3-55
commands
Access Control 8-20
Enable/Disable 2-50
Reload All RIDs 2-50
Reset Edit Incident Control 3-58
communication
dual channels 6-3
verification delay 2-41
Communicator
adding the BT-X 6-2
conditional activation of outputs 2-77
configuration table
client B-3
server B-2
Constant Secure zones
on the BT2-8S 9-3
on the BT-XS (M) 9-11
conventions for naming media files 5-4
coordinates
using on maps 2-6
copying roster shifts 4-44
customizing
action buttons 3-36
alert colors 3-55
Alert Manager 3-50
alert phrases 2-69
log entries 4-4
permit drop-down lists 4-28
personnel fields 4-23, 4-24
Security Desk Journal 4-14
SOPs 3-41, 3-43
work order drop-down lists 4-25

D

data security levels 2-98
databases
about 2-2
adding facilities to D-21 database 2-13
backup up before quitting 1-5
deleting
see also *removing*
emergency cards 3-23
facilities on maps 2-120
HazMats 2-106
hydrants from maps 2-120
operators 2-100
outputs 2-78
remote units 2-61
resources 2-105
RIDs 2-50
vehicles 2-103
zones 2-70
Desk Journal 4-14
details pane, about 1-7
diddled reader status 8-11
DIO
Dual Input Output RID 2-30
DIO (Dual Input/Output) modules 2-54
disabling
auxiliary zone alerts 3-46
devices 2-50
output alerts and logging 3-47
dispatching
automatically prompt to dispatch 4-52
enabled 4-52
response plans 3-9
setting priorities in response plans 3-11
dispositions
Law Enforcement 4-16, 4-17
districts, creating 4-12
Door Strike Control readers 8-15
downloading
access control unit configuration 8-20
IDS iButton authentications 9-43
intrusion detection to BT2-8S 9-10
intrusion detection to BT-XS (M) 9-24
drivers
see *RIDs*
dual comm channels
enabling 2-49
dual communication mode 6-3
dual communication status
displaying on floor plans 2-29
duration, specifying for momentary outputs 2-75
duress reader status 8-11
duty types, creating 4-43
DZI (Dual Zone Input) modules 2-54
DZI (Dual Zone Interface) RID 2-30

E

E-911
adding phone numbers to D-21 database 2-20, 10-9
Outside Map Boundary warning 3-51
printing facility phone numbers 10-10
specifying alert priorities 10-3
TCI RID 2-30
Verizon RID 2-30
edit control, resetting lock in Incident Client 3-58
editing
custom buttons 3-37
emergency cards 3-22

facilities 2-26
HazMats 2-107
iButtons (IDS) 9-37
operators 2-100
output groups 2-84
outputs 2-77
remote unit groups 2-63
remote units 2-61
resources 2-105
sites 2-3
SOPs 3-38
zones 2-70
emergency cards
about 3-20
adding 3-20
deleting 3-23
editing 3-22
using for Law Enforcement 3-20, 3-21
enabling
devices 2-50
dual comm channels 2-49
live-voice messages 7-5
pre-recorded messages 7-5
enrolling (IDS)
iButtons 9-24
primary administrator 9-25
secondary administrator 9-25
user iButtons 9-29
entering data 2-2
Entry/Exit Delay zones
on the BT2-8S 9-3
on the BT-XS (M) 9-11
exiting D21 Admin Client 1-5
exporting
NFIRS categories used in 2-21
secondary incident ID useful in 3-53
extent, setting map zoom levels 2-5
external programs, creating actions to run 3-27, 3-32

F

facilities
adding 2-13
adding actions 2-17
adding floor plans 2-16, 2-27
adding response plans 2-19
adding to maps 2-14, 2-113
adding to site 2-11
adding zones 2-18
customizing types 4-8
deleting from maps 2-115, 2-120
editing 2-26
importing floor plans 5-8
Knox box location 2-13
mixed use 2-21
NFIRS categories 2-21
notes 2-22
numbering 2-13
placing on maps 2-112, 2-119
property use 2-21
street addresses 2-15
FACPs
M-1 2-54
M-1 Addressable 2-54
M-2 2-54
M-2 Addressable 2-54
fallback
displaying dual comm status on floor plans 2-29
enabling dual comm channels 2-49
file names, conventions for media files 5-4
find
HazMats 2-107, 3-21, 3-22
job title, personnel, or resource to add to roster 4-45
fire auxiliary class 2-64
Firehouse Software
setting up workstation 4-50
floor plans
adding labels to 2-17, 2-27
adding outputs 2-29
adding remote units 2-29
adding to facilities 2-16, 2-27
adding zones 2-29
displaying status of dual comm units 2-29
importing 5-3, 5-5, 5-8
specifying class 2-28
forced open reader status 8-11
frequency
setting up shared 2-34
two RFMs sharing 2-46

G

General Status RID 2-30
General Status units 2-54
Geographic Information
sunrise and sunset times 2-4
GPIO
adding RID for 2-30
configuring outputs 2-74
graphics
see also *media files*
conventions for naming files 5-4
file types 5-3
icons 9-10
importing 5-3, 5-5
in response plans 3-12
placing output icons on 2-82
placing zones on 2-84
stored in media folder 5-2
support file formats 5-3
grid coordinates
configuring map for 2-6
groups
access control 8-4
creating MNS message 7-7
editing MNS message 7-10
editing output 2-84
editing remote unit 2-63
output 2-78
remote unit 2-62
removing MNS message 7-10
removing output 2-84

removing remote unit 2-63
GuardCard 2-96

H

HA7NetHub iButton unit 2-54
HazMats
adding to database 2-106
adding to response plans 2-23
deleting 2-106
editing 2-107
held open reader status 8-11
holiday schedules (ACS) 8-8
hubs (iButton)
adding RID for 2-31
adding to workstation 4-50
hydrants
adding 2-109
address for 2-110
color based on flow 4-37
deleting from maps 2-118, 2-120
in response plans 3-13
placing on maps 2-112, 2-119

I

iButton assignments (IDS)
about 9-24
adding administrators 9-25
adding or removing facilities 9-34
adding or removing keypads 9-34
administrators 9-25
ageing a PIN 9-40
authentication defined 9-24
authentication watch 9-34
central enrollment defined 9-24
central enrollment switchboard 9-28
Clear Credentials command 9-45
deactivating 9-37
deactivating, reactivating 9-34
determining if assigned 9-40
Download Manager 9-43
downloading 9-43
downloading to a specific unit 9-44
editing 9-37
enabling operators for 2-99
enrolling users 9-29
Facility Access Report 9-42
reactivating 9-38
removing 9-36
resetting a PIN 9-34
temporary PIN 9-34
transferring 9-39
unit watch 9-47
viewing download results 9-46
viewing users with access to Master Zone 9-41
iButtons
adding Analog Points RID 2-30
adding iButton Hub RID 2-31
adding workstation hub 4-50
HA7NetHub unit 2-54
icons
adding to media files 5-12
adding to output groups 2-78
output 2-77
placing on maps 2-112
zone status 2-70
IDS Master unit 2-53, 9-22
about 9-12
adding 9-14
check box 9-14, 9-18
images
facility floor plans 2-27
personnel 2-95
response plan graphics 3-12
vehicle 2-102
importing
files 5-3
floor plans 5-5, 5-8
map layer files 2-6
pre-plan files 3-23, 5-10
response graphics 5-5
incident classes
operator privileges 2-99
Incident Client
operator privileges 2-99
incident types
enabling PACAF codes 3-64
Law Enforcement 3-20, 3-21
incidents
colors for 3-55
default map location 4-36
incident icon flashing 4-36
numbering 3-53
reporting by district 4-12
reset editing lock in Incident Client 3-58
secondary numbers 3-54
specifying map zoom levels 2-6
using two numbers 3-53
without map location 4-36
interact ranges
RFM 7000 2-44
intervals
access control 8-7
holidays (ACS) 8-8
keep-alive (MNS) 7-4
intrusion detection (IDS)
about 9-2
adding IDS application units 9-21
adding IDS Master units 9-14
adding the BT-XS (M) 9-14
BT2-8S Master zones 9-4
BT2-8S zone types 9-3
BT-XS (M) Master zones 9-12
configuring application units 9-14
configuring the BT2-8S 9-2, 9-4
configuring the BT-XS (M) 9-11
IDS Master units 9-12, 9-14, 9-18, 9-22
response plans 9-9
security zone types 9-11
specifying the Master for an Automatic zone 9-23
status phrases 9-9

using keypads 9-13
IP address
alternate IP address 2-32, 2-38

J

job titles
adding 4-23
using in rosters 4-38

K

keep-alive timeout (MNS) 7-3, 7-4, 7-5
keypads
configuring for IDS 9-13
specifying for Master zones 9-16, 9-21
Keyswitch zones
on the BT-XS (M) 9-11
Knox box, specifying location of 2-13

L

labels
adding floor plan 2-17, 2-27
customizing personnel fields 4-23, 4-24
launching
Admin Client 1-2
Server 1-2
Law Enforcement
creating incident types 3-21
dispositions 4-16, 4-17
incident types 3-20
mutual aid 4-16, 4-20
notifications 4-16, 4-19
setting up lists 4-16
sources 4-16, 4-18
weapons 4-21
layer files, importing 2-6
listen ranges
RFM 7000 2-44
lists
customizing for Law Enforcement 4-16
live-voice (MNS)
configuring ACU-1000 RID 7-13
enabling 7-4, 7-5
keep alive 7-5
local microphone 7-5
timeout 7-3
live-voice timeout (MNS) 7-4
local microphone
enabling 7-4
using for live voice 7-5
Log, custom entries 4-4
logging
disabling for auxiliary zones 3-46
disabling for outputs 3-47
output status changes 2-76
logical position numbers 2-66
login
Admin 1-2
multi-server client 1-3
operator 1-2
login options 4-51
lost cards (ACS) 8-32

M

M-1 Addressable 2-54
M-1 FACP 2-54
M-2 Addressable FACP 2-54
M-2 FACP 2-54
map
default map view 4-50
Map Options 4-33
Auto-Addressing 4-33, 4-36
Incident Relocating 4-33, 4-36
Shortest Route 4-33
maps
adding facilities to 2-14
adding site 2-5
background color 2-5
defining facility types 4-8
deleting facilities from 2-14, 2-120
deleting hydrants from 2-120
facility icon display 2-6
file locations 2-5
grid coordinates 2-6
hydrant colors based on flow 4-37
importing layer files 2-6
placing hydrants and facilities on 2-112, 2-119
setting map extent 2-5
zoom levels 2-5
mass notification (MNS)
about 7-2
adding a BT-X Communicator 2-53
adding a BT-X Wide Area Communicator 2-54
adding a BT-XF (program chip A.9) 2-53
editing groups 7-10
enabling live-voice messages 7-4, 7-5
enabling pre-recorded messages 7-4, 7-5
keep-alive signal 7-4
live-voice timeout 7-4
message groups 7-8
multiple input sources 7-13
pre-configured messages 7-24
pre-recorded timeout 7-4
removing groups 7-10
setting up pre-recorded messages 7-6
setting up remote units for 7-18
timeouts 7-3
unit numbering 7-18
workstation input sources 7-16
Master
IDS Master unit 2-53
Master zones
adding IDS Master unit 9-14
configuring for IDS 9-23
on the BT2-8S 9-2, 9-4
on the BT-XS (M) 9-12
specifying keypad associations 9-16, 9-21
media files
about 5-2
file types 5-3

floor plans 5-4
icons 5-12
naming conventions 5-4
sounds 5-12
vehicles 2-102
menu commands 1-8
Add 1-9
Commands 1-10
Devices 1-10
File 1-8
Help 1-10
messages (MNS)
adding pre-recorded 7-6
creating groups 7-7
editing groups 7-10
pre-configuring 7-24
removing groups 7-10
mixed use facilities 2-21
MNS
broadcast Messages 7-11
broadcast messages 7-2
live voice messages 7-2
pre-recorded messages 7-2
momentary outputs 2-75
Monaco, communicating with through pcAnywhere 13-2
monitor
incident viewer on second monitor 4-50
secondary 4-50
startup 4-49
multiple alerts
customizing display in Alert Manager 3-50
multi-server client
starting 1-3
mutual aid
in response plans 3-11
Law Enforcement 4-16, 4-20

N

NCD relays
adding outputs 2-74
adding RID for 2-31
NFIRS categories
facilities 2-21
resources 2-104
normals
acknowledging automatically 3-48
notes
adding facility 2-22
Pass On Log 4-5
Standard 4-5
types 4-5
Notes of the Day 12-2, 12-4
notification threshold 3-50
notifications
Law Enforcement 4-16, 4-19
numbering
facilities 2-13
incidents 3-53, 3-54
mass notification units 7-18
outputs 2-75
remote units 2-54
zones reporting to an RFM 5000 2-66
zones reporting to an RFM 7000 2-66

O

offline verification delay 2-41
operators
adding 2-97
alerts displayed 2-99
assigning administration privileges to 2-98
assigning data security levels to 2-98
assigning incident class privileges to 2-99
assigning Incident Client privileges to 2-99
assigning site privileges to 2-100
deleting 2-100
editing 2-100
incident class permissions 2-99
logging into multi-server client 1-3
making iButton assignments 2-99
options
operator login 4-51
workstation 4-49
output groups
adding zones to 2-83
editing 2-84
removing 2-84
outputs
about 2-74
activation condition 2-77
adding 2-74
adding GPIO 2-74
adding icons for 2-77
adding to floor plans 2-27, 2-29
adding to graphics 2-78
bi-state type 2-75
class of 2-76
creating groups 2-78
deleting 2-78
description needed 2-75
disabling alerts 3-47
duration of momentary 2-75
editing 2-77
enabling alerts from 2-76
enabling and disabling 2-50
logging status changes 2-76
momentary type 2-75
NCD relays 2-74
numbering 2-75
RSA relays 2-75
status change alerts 2-76

P

PACAF
enabling incident codes 3-64
panes
details 1-7
tree 1-7

Pass On Log 4-5
pcAnywhere 13-2
permits
  customized drop-down lists 4-28
  defining permit types 4-31
personnel
  adding 2-86
  adding job titles 4-23
  adding vehicles for 2-101
  assigning to rosters 4-38
  assigning vehicles to 2-94
  badging 2-93
  custom fields 4-23, 4-24
  home address for 2-90
  identification 2-95
  work address for 2-88
PINs (ACS)
  assigning 8-24
  editing assignments 8-27
  unassigning 8-27
PINS (IDS)
  ageing 9-40
  resetting 9-34
  temporary 9-34
PINs (IDS) 9-24
points 2-71, 3-48
  on floor plans 2-73
  properties 2-71
polling modes
  RFM 5000 2-35
  RFM 7000 2-40
polling ranges
  RFM 5000 2-33
  RFM 7000 2-44
position numbers 2-66
power status verification time 2-61
Pre-Authorized EE zones
  on the BT-XS (M) 9-12
Pre-Authorized zones
  on the BT-XS (M) 9-12
pre-configured messages (MNS)
  setting up 7-24
pre-plans
  adding to response plans 3-5
  importing 5-3
  importing files 5-10
  templates 3-23
pre-recorded messages (MNS) 7-6
  enabling 7-4, 7-5
  timeout 7-3
pre-recorded timeout (MNS) 7-4
pre-strobe 11-2, 11-11
pre-tone 11-2, 11-12
primary administrator (IDS) 9-25
primary communication 6-3
primary RFM 7000 2-43
priority
  E-911 alert reporting 10-3
  setting resource dispatch 3-11
  zone reporting 2-65
privileges
  Admin Mode 2-98
  assigning to operators 2-98
  data security levels 2-98
  incident classes 2-99
  Incident Client access 2-99
  sites 2-100
product support specialists 13-2
property use, facilities 2-21

Q

quitting
  Admin Client 1-5
  backing up before 1-5
quotation marks 1-11

R

RDU (Remote Display Unit)
  adding RID for 2-31
readers (ACS)
  auxiliary input status 8-11
  configuring zones 8-16
  diddled status 8-11
  Door Strike Control type 8-15
  duress status 8-11
  forced open status 8-11
  held open status 8-11
  No Entry Confirmation option 8-15
  tamper status 8-11
recovery path
  backing up to 1-5
redundant RFMs 2-46
  RFM 5000 2-33
  RFM 7000 2-43
relays
  see also *outputs*
  adding 2-74
  adding momentary outputs 2-75
  adding to output graphics 2-78
  remote signal activation (RSA) 2-75
reloading RIDs 2-50
reminders, creating actions to run 3-27, 3-34
remote access, setting up pcAnywhere 13-2
Remote Annunciator
  adding RID for 2-31
remote commands
  creating actions to run 3-27
  running with actions 3-29
Remote Interface Driver (RID)
  CPS 484 Power Supply 2-30
  DIO (Dual Input/Output) 2-30
  DZI (Dual Zone Interface) 2-30
  General Status 2-30
  GPIO (General Purpose Input/Output) 2-30
  iButton Analog Points 2-30
  iButton Hub 2-31
  NCD Relay Control 2-31
  RDU (Remote Display Unit) 2-31
  Remote Annunciator 2-31
  Tone Alert (Tone Alert Panel Monitor) 2-30

Tone Generator (TGU) RID 2-31
Verizon E-911 2-30
Zetron E911 2-30
remote interface drivers
see *RIDs*
remote signal activation (RSA) relays, numbering 2-75
remote unit groups
adding 2-62
removing 2-63
remote units
about 2-51
adding 2-55
adding BT-X units 6-2
adding outputs 2-59
adding to floor plans 2-27, 2-29
adding zones 2-58
BT2-0/1/2 2-52
BT2-3 2-52
BT2-4 2-52
BT2-7 2-52
BT2-8 2-52
BT2-8S 2-52, 9-4
BT2-R 2-52
BT2-SC (DTMF siren controller) 2-33, 2-52, 2-58
BT-X Communicator 2-53
BT-X Wide Area Communicator 7-18
BT-X with MNS 2-53
BT-X/ACS (M) 2-53, 8-10, 8-12
BT-XF (16) 2-53
BT-XF (M) 2-53
BT-XS (16) 2-53
BT-XS (M) 2-53, 9-21
class 2-52, 2-56
configuring the BT-X for access control 6-4, 8-10
configuring the BT-X for fire reporting 6-2, 6-4
configuring the BT-X for intrusion detection 6-4, 9-14
configuring the BT-X for mass notification 6-4, 7-18
creating groups 2-62
deleting 2-61
DIO (Dual Input/Output) modules 2-54
download access control settings to 8-20
DZI (Dual Zone Input) modules 2-54
editing 2-61
editing groups 2-63
enabling and disabling 2-50
General Status 2-54
HA7NetHub iButton hub 2-54
IDS application units 9-14
IDS Master unit 2-53
M-1 Addressable FACP 2-54
M-1 FACP 2-54
M-2 Addressable FACP 2-54
M-2 FACP 2-54
MAAP(+) 2-54
numbering 2-54
repeaters 2-58
RFM 5000 tones 2-57
setting power status delay 2-61
tone alerting panel 2-54
removing
see also *deleting*
actions 3-35
custom buttons 3-36
custom SOPs 3-43
iButtons (IDS) 9-37
output groups 2-84
remote unit groups 2-63
renaming actions 3-35
repeater (DTMF) 2-52
repeaters
remote units 2-58
RFM 7000 2-43
reports
Facility Access Report (IDS) 9-42
Security Desk Journal 4-14
Summary Statistics Log 4-46
resounding troubles 3-51
resources
adding 2-103
deleting 2-105
dispatching in response plans 3-9
editing 2-105
NFIRS categories 2-104
using in rosters 4-38
response graphics
importing 5-3
response graphics, importing 5-5
response plans
about 3-2
actions 3-15
adding to facilities 2-19
adding to sites 2-10
adding to zones 2-68
call lists 3-4
creating 3-3
dispatching resources 3-9
emergency cards 3-20
graphics 3-12
HazMats 2-23
hydrants 3-13
importing graphics 5-5
importing pre-plan files 5-10
intrusion detection (IDS) 9-9
mutual aid 3-11
pre-plans 3-5
setting dispatch priorities 3-11
RFM 5000
adding RID for 2-31
attaching RID actions 2-36
enabling siren control 2-33
polling ranges 2-33
RID topology 2-33
setting carrier delay times 2-33
specifying polling modes 2-35
specifying redundant 2-33
specifying tones for remote units 2-57
zone numbering 2-66
RFM 7000
adding RIDs for 2-38
attaching RID actions 2-48
BT2 ranges 2-44
interact ranges 2-44

listen ranges 2-44
offline verification delay 2-41
polling modes 2-40
primary 2-43
redundant repeater 2-43
repeaters 2-43
secondary 2-43
setting carrier delay times 2-41
specifying upline 2-43
topology 2-41
zone numbering 2-66
RFM7000
disabling alerts for undefined unit 2-49
RFMs
adding RIDs for 2-30
using redundant 2-46
RFM-X
adding RID for 2-38
enabling local microphone 7-4, 7-5
RID Options, MNS settings 7-4
RIDs
about 2-30
ACU-1000 Radio Switch 2-30, 7-13
adding RFM-X 2-38
deleting 2-50
DIO (Dual Input Output) 2-30
enabling and disabling 2-50
enabling dual comm channels 2-49
iButton Analog Points 2-30
reloading 2-50
remote command actions 3-29
RFM 5000 . . . . . 2-30, 2-31
RFM 7000 . . . . . 2-30, 2-38
TCI E-911 2-30
road closure color, setting 4-35
roster
about 4-38
adding job titles 4-23
copying shift templates 4-44
creating shift templates 4-40
deleting shift templates 4-46
duty types 4-43
editing shift templates 4-44
rosters
displayed on View Generator 12-4
routes
alternate 4-34
alternate route 4-34
Auto-Routes 4-33
configuring shortest routes 4-33
hide routes 4-53
primary 4-34
setting colors 4-34
RSA relays, momentary output type 2-75
Run ID 3-53

S

schedules
access control 8-6
intervals 8-7
secondary administrator (IDS) 9-25
secondary communication 6-3
secondary incident numbers 3-53, 3-54
secondary RFM 7000 2-43
security
adding the BT2-8S 9-4
adding the BT-XS 9-21
assigning operators 2-98
auxiliary class 2-64
BT-XS (M) Master zones 9-12
configuring actions for zones 9-17, 9-21, 9-23
configuring the BT-XS (M) 9-11
customizing Desk Journal 4-14
customizing Law Enforcement 4-16
server configuration table B-2
settings
recording local BT-XS (M) 9-17, 9-21, 9-23
shared frequencies 2-34, 2-46
shifts
copy templates 4-44
creating templates 4-38, 4-40
Shortest Route
Network Layer 2-9
siren controller (BT2-SC) 2-33, 2-52, 2-58
sites
adding 2-3
adding facilities to 2-11
adding map to 2-5
customizing site label 4-7
editing 2-3
operator access privileges for 2-100
response plans 2-10
social security numbers, adding 2-95
SOPs
adding 3-38
customizing 3-41
editing 3-38
removing custom 3-43
sounds, playing .wav files 4-55
sources
Law Enforcement 4-16, 4-18
live-voice inputs (MNS) 7-13
specifying priorities for zones 2-65
Standard notes 4-5
standard operating procedures
see *SOPs*
starting
Admin Client 1-2
Server 1-2
statistics, using the Summary Statistics Log 4-46
status changes, attaching actions to 3-37
stolen cards (ACS) 8-32
Summary Statistics Log, creating 4-46

T

tamper reader status 8-11
templates, pre-plan 3-23
TG-1 (Tone Generator) 2-54
timeouts
live-voice (MNS) 7-4

pre-recorded (MNS) 7-4
timeouts (MNS) 7-3
keep-alive 7-3, 7-5
live-voice 7-3
pre-recorded 7-3
Tone Alert Unit
adding 11-9
tone alerting
tone alerting
with a Tone Alert Unit 11-6
tone alerting
automatic 11-15
pre-recorded voice messages 11-12
with Text-to-Speech 11-6, 11-12, 11-18
with Tone Generator 11-2
Tone Generator
tone alerting 11-2
tone sequence list
creating for the Tone Alert Unit 11-13
creating for the Tone Generator 11-5
defined 11-2
tone sequences
assigned to incident classes 11-15
creating for the Tone Alert Unit 11-11
creating for the Tone Generator 11-3
topics
see also *emergency cards*
creating response plans for 3-20
using with Law Enforcement 3-20
topologies
interact ranges 2-44
listen ranges 2-44
RFM 5000 2-33
RFM 7000 2-41
towers
adding a BT-X/WAC+ for MNS 2-54
tracking access card usage 8-30
transceivers
see *remote units*
tree pane
about 1-7
navigating 1-7
troubles
acknowledging automatically 3-48
actions performed in response to 3-27
automatically acknowledging 3-45, 4-54
auxiliary 8-16
custom sounds for 4-55
diddled/duress 8-16
disabling for undefined unit 2-49
door held or forced open 8-16
priority of 3-45
setting resound intervals 3-51
tamper 8-16
Two Man Access/Secure zones
on the BT2-8S 9-3
on the BT-XS (M) 9-12
types
duty 4-43
facility 4-8
notes 4-5

U

upline RFM 7000, specifying 2-43
users (IDS)
enrolling iButtons 9-29

V

vehicles
adding 2-101
assigning to personnel 2-94
deleting 2-103
images 2-102
verification delays
battery faults 2-61
Comm 2-41
offline 2-41
RFM 5000 carrier 2-33
RFM 7000 carrier 2-41
View Generator 12-2
adding Repeater Display 12-5
assigning Repeater Display 12-6
defining content 12-4
Repeater Displays 12-2

W

wave files (.wav), playing 4-55
weapons
Law Enforcement 4-21
work orders
customized drop-down lists 4-25
workstation options
about 4-49
adding iButton hubs (IDS) 4-50
incident auto-display viewer 4-50
installing Firehouse Software 4-50
live-voice input sources (MNS) 7-16
playing sound files 4-55
secondary monitor 4-50
startup monitor 4-49

Z

ZID
numbering 2-66
specifying for RFM 5000 2-33
zone cards
adding GPIO outputs 2-74
zone types
for the BT2-8S 9-3
for the BT-XS (M) 9-11
zones
actions for security 9-17, 9-21, 9-23
adding 2-65
adding actions for 2-67
adding IDS Master zones 9-14
adding response plans to 2-68
adding to facilities 2-18
adding to floor plans 2-27, 2-29
adding to output groups 2-83
adding to remote units 2-58
auxiliary (ACS) 8-11

BT-XS (M) Master zones 9-12
configuring for readers 8-16
customizing alert phrases 2-69
deleting 2-70
diddled/duress (ACS) 8-11
disabling auxiliary alerts 3-46
editing 2-70
enabling and disabling 2-50
fire auxiliary 2-64
fire zones on BT2-8S 9-5
held/forced open (ACS) 8-11
icons for status 2-70
keypads used with 9-16, 9-21
logical position numbers 2-66
Master zones (IDS) 9-2
point reporting 2-71
reader 8-11
RFM 5000 ZID ranges 2-33
security auxiliary 2-64
specifying priorities for alerts 2-65
tamper (ACS) 8-11
zoom level
setting on maps 2-5
specifying for hydrants and facilities on maps 2-5
specifying for incidents on maps 2-6