

GE  
Security

Facility Commander  
**Administration Guide**



**Copyright** Copyright © 2009, GE Security Inc. All rights reserved.

This document may not be copied or otherwise reproduced, in whole or in part, except as specifically permitted under US and international copyright law, without the prior written consent from GE Security.

Document number/revision: 460571003B (April 2009).

**Disclaimer** THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. GE ASSUMES NO RESPONSIBILITY FOR INACCURACIES OR OMISSIONS AND SPECIFICALLY DISCLAIMS ANY LIABILITIES, LOSSES, OR RISKS, PERSONAL OR OTHERWISE, INCURRED AS A CONSEQUENCE, DIRECTLY OR INDIRECTLY, OF THE USE OR APPLICATION OF ANY OF THE CONTENTS OF THIS DOCUMENT. FOR THE LATEST DOCUMENTATION, CONTACT YOUR LOCAL SUPPLIER OR VISIT US ONLINE AT [WWW.GESECURITY.COM](http://WWW.GESECURITY.COM).

This publication may contain examples of screen captures and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual businesses or persons is entirely coincidental.

**Trademarks and patents** GE and the GE monogram are registered trademarks of General Electric. Facility Commander and logo are registered trademarks of GE Security.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

**Intended use** Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at:

[www.gesecurity.com](http://www.gesecurity.com).

# Contents

<b>About This Document .....</b>	<b>ix</b>
Who Should Use This Document .....	ix
How This Document Is Organized .....	ix
Using This Document .....	xi
Conventions Used In This Document .....	xii
Related Documents .....	xiii
 <b>Chapter 1. Introduction .....</b>	 <b>1</b>
Overview .....	2
Video management .....	3
Centralized video management .....	3
Distributed video management .....	4
 <b>Chapter 2. Getting Started .....</b>	 <b>7</b>
Overview .....	8
Starting and Stopping Facility Commander Server and Media Server Services .....	8
Facility Commander Launcher .....	9
Minimizing Facility Commander Launcher .....	11
Logging In from a Workstation .....	12
Logging In Using the Web Application .....	14
Using the Web Browser Application .....	14
List Page .....	15
Browser Menu .....	18
Configuration Page .....	19
Managing Multiple Windows .....	20
Client Application Title Bars .....	21
Customizing Window Name and Contents .....	22
Error Messages .....	23
Navigating the Multi Viewer .....	24
Customizing the Multi Viewer .....	25
 <b>Chapter 3. Configuring the System .....</b>	 <b>27</b>
Checklist .....	28
Facility Commander Servers .....	31
Viewing Facility Commander Servers .....	31
Adding a Facility Commander Server .....	32

Access Control Systems .....	38
Viewing Access Control Systems .....	38
Adding an Access Control System .....	39
Workstations .....	45
Configuring the Alarm Alert Window .....	45
Launching the Video Console Automatically .....	45
Intercom Stations .....	45
Viewing Defined Workstations .....	46
Adding a Workstation .....	47
System Parameters .....	50
Launch Video Console by Alarm Priority .....	50
Require an Alarm Response .....	50
Configure Video Pre-Play Time .....	50
Configuring System Parameters .....	51
System Shutdown .....	53
Shutdown Notification to Client Applications .....	53
Shutdown Notification to Browser Configuration Clients .....	53
Shutting Down the System .....	53
<b>Chapter 4. Importing Records .....</b>	<b>55</b>
Overview .....	56
Tag Names, Descriptions, and Record IDs .....	56
Time Zones .....	56
Synchronize Records .....	57
Terminology .....	57
Operator Records .....	58
Operator Passwords .....	58
Operator Preferences .....	58
Viewing Facility Commander Operators .....	59
Adding Operators .....	60
Removing Default Account .....	64
Importing Operators .....	65
Changing Operator Preferences .....	66
Facilities .....	67
Viewing Facilities .....	68
Importing Facilities .....	68
Creating a Facility .....	70
Members Tab .....	71
Parent Facility Tab .....	72
Window Filter .....	73
Changing Contents of View .....	73
Access Points .....	74
Viewing Imported Access Points .....	74
Importing Access Points .....	75
Editing Access Points .....	76
Synchronizing Access Points .....	79
Digital Inputs and Outputs .....	80
Viewing Digital Inputs .....	80
Importing Digital Inputs .....	81
Editing Digital Inputs .....	82
Synchronizing Digital Inputs .....	85
Viewing Logical Inputs .....	86
Importing Logical Inputs .....	87
Editing Logical Input Records .....	88
Synchronizing Logical Inputs .....	91
Viewing Digital Outputs .....	92

Importing Digital Outputs .....	92
Editing Digital Outputs .....	94
Synchronizing Digital Outputs .....	97

## **Chapter 5. Assigning Permissions and Context ..... 99**

Overview .....	100
Facilities .....	100
Permissions .....	100
Context .....	100
Pre-Defined Permissions and Context .....	101
Examples .....	101
Checklist .....	101
Facility Permissions .....	102
Using Pre-Defined Facility Permissions .....	102
Viewing Facility Permissions .....	103
Adding Facility Permissions .....	104
System Permissions .....	108
Using Pre-defined System Permissions .....	108
Viewing System Permission .....	109
Adding System Permissions .....	110
Contexts .....	113
Viewing Context Definitions .....	113
Adding Context Definitions .....	114
Pre-defined Contexts .....	117
Examples .....	118

## **Chapter 6. Configuring Video Devices ..... 121**

Overview .....	122
Define digital video recorders .....	123
Video Devices .....	124
Configuring Digital Video Recorders .....	124
Viewing DVRs .....	125
Adding DVRs .....	126
Configuring Cameras .....	132
Viewing Cameras .....	132
Adding Cameras .....	133
Configuring IP Cameras .....	137
Configuring Camera Preset Positions .....	138
Viewing Camera Preset Positions .....	138
Adding Camera Preset Positions .....	139
Linking Cameras to DVRs .....	141
Configuring Analog Video Switchers .....	143
Viewing Analog Video Switchers .....	143
Adding an Analog Video Switcher .....	144
Configuring CCTV Monitors .....	150
Viewing CCTV Monitors .....	150
Adding CCTV Monitors .....	151
Associating Analog Video Switcher Devices .....	153
Troubleshooting Steps .....	155
Configuration .....	155
Client Path Settings .....	156
Communication Failure .....	156

## **Chapter 7. Using the Video Console ..... 157**

Overview .....	158
----------------	-----

Automatically Launch by Alarm Priority .....	158
Navigating the Multi Viewer .....	159
Drag and Drop Cameras .....	159
Navigating the Video Console .....	160
Controlling Cameras .....	163
Live Video .....	164
Recorded Video .....	164
Event Action Mapping .....	164
Viewing Live Video .....	165
Viewing Recorded Video .....	165
View a Single Video Frame .....	165
Create an Evidence CD .....	166
Searching for Video .....	167
System Event Search .....	167
DVR Event Search .....	169
DVR General Playback Search .....	171
DVR Motion Search .....	173
Customizing the Video Console .....	175
Creating Custom Views .....	175
Create a window filter .....	176
Display Additional Video Panes .....	177
<b>Chapter 8. Event Action Mapping .....</b>	<b>179</b>
Overview .....	180
Viewing Event Action Mappings .....	181
Tagging Video Events for Access Points .....	182
Tagging Video Events for Intercom Calls .....	183
Activating Digital Outputs .....	184
Sending Automatic E-mails .....	185
Events in Event Action Mapping .....	186
Actions in Event Action Mapping .....	190
<b>Chapter 9. Configuring Alarms .....</b>	<b>193</b>
Overview .....	194
Configuring the Alarm Monitor .....	196
Synchronization .....	196
Setting Alarm Colors .....	197
Creating Alarm Instructions .....	199
Creating Alarm Profiles .....	201
Adding an Alarm Profile .....	202
<b>Chapter 10. Using the Alarm Monitor .....</b>	<b>205</b>
Overview .....	206
Automatically Launch Video Console by Alarm Priority .....	206
Alarm Alert .....	207
Navigating the Alarm Monitor .....	208
Customizing the Alarm Monitor .....	211
Changing Window Name and Contents .....	211
Display Multiple Time Zones .....	212
Launch Video Automatically .....	214
Responding to Alarms .....	215
Alarm Response Required .....	215
<b>Chapter 11. Using the Event Monitor .....</b>	<b>219</b>
Overview .....	220

Navigating the Event Monitor .....	220
Alarm Events List .....	223
Badge Events List .....	224
System Events List .....	225
Setting Event Monitor Options .....	226
Changing the Event Types Filter .....	227
Event Types List .....	228
Customizing Window Name and Contents .....	230
<b>Chapter 12. Configuring Intercom Devices .....</b>	<b>231</b>
Overview .....	232
Terminology .....	232
Checklist .....	232
Configuring Intercom Exchanges .....	233
Viewing Intercom Exchanges .....	233
Adding an Intercom Exchange .....	234
Configuring Intercom Stations .....	240
Viewing Intercom Stations .....	240
Adding Intercom Stations .....	241
Tips for Creating Symbol Schemes .....	246
Intercom Exchange Symbol Scheme .....	246
Intercom Master Station Symbol Scheme .....	247
Intercom Substation Symbol Scheme .....	248
<b>Chapter 13. Configuring Intrusion Devices .....</b>	<b>249</b>
Overview .....	250
Terminology .....	250
Configuring Intrusion Devices .....	251
Connecting Intrusion Panels .....	251
Ethernet Connection .....	251
RS-232 Connection .....	253
Configuring Intrusion Panels .....	254
Viewing Intrusion Panels .....	254
Adding Intrusion Panels .....	255
Configuring Intrusion DGPs .....	261
Viewing Intrusion DGPs .....	261
Adding Intrusion DGPs .....	262
Configuring Intrusion Keypads .....	266
Viewing Intrusion Keypads .....	266
Adding Intrusion Keypads .....	267
Configuring Intrusion Areas .....	271
Viewing Intrusion Areas .....	271
Adding Intrusion Areas .....	272
Configuring Intrusion Inputs .....	276
Viewing Intrusion Input .....	276
Adding Intrusion Inputs .....	277
Configuring Intrusion Outputs .....	281
Viewing Intrusion Outputs .....	281
Adding Intrusion Outputs .....	282
<b>Chapter 14. Creating Symbol Schemes .....</b>	<b>285</b>
Overview .....	286
Using the Symbol Editor .....	287
Creating a Symbol Scheme .....	291
Creating an Intrusion Symbol Scheme .....	292

Managing Symbol Editor Files .....	294
Uploading a Symbol Scheme .....	294
Downloading a Symbol Scheme .....	294
Deleting a Symbol Scheme .....	295
State Associations and Conditions .....	295
<b>Chapter 15. Creating Graphic Displays .....</b>	<b>299</b>
Overview .....	300
Using the Graphics Editor .....	301
Drawing Tools .....	305
Graphic Attributes .....	306
Creating a Graphic Display .....	308
Associating Access Points and Other Devices .....	309
Associating Camera Devices .....	310
Associating Intercom Devices .....	311
Creating Intrusion Areas .....	312
Adding Text Labels to the Site Map .....	313
Saving the Site Map .....	314
Importing AutoCAD Drawings .....	314
Maintain Layers in AutoCAD Drawings .....	317
Linking Graphic Displays .....	318
Building Hierarchical Displays .....	320
Working with Layers .....	323
Creating a New Layer .....	323
Selecting a Layer .....	324
Renaming a Layer .....	325
Removing a Layer .....	325
Moving Objects Between Layers .....	326
Managing Graphic Display Files .....	326
Uploading Graphic Displays .....	326
Downloading Graphic Displays .....	328
Deleting Unused Files .....	329
Editing Graphic Display Records .....	330
<b>Chapter 16. Viewing Graphic Displays .....</b>	<b>333</b>
Overview .....	334
Alarm States .....	335
Navigating the Graphics Viewer .....	336
Opening Graphic Displays .....	338
Selecting Layers .....	339
Issuing Commands .....	340
Lock and Unlock Doors .....	341
View Video from a Specific Camera .....	342
View Video from Monitor Devices .....	343
Enable or Disable Input Devices .....	344
Connect and Disconnect Intercom Devices .....	345
Arm or Disarm Intrusion Areas .....	346
Customizing Window Name and Contents .....	347
Printing Graphic Displays .....	348
<b>Chapter 17. Backup/Restore Informix Databases .....</b>	<b>349</b>
Overview .....	350
Backup Modes .....	350
Backup Types .....	351
Requirements (Tape Backups) .....	351



Tape Labels .....	351
Backing Up Database Records .....	352
Informix Database .....	353
Backing Up Files .....	355
Restore Procedures .....	357
Restore Incremental Backups .....	361
Restore Database .....	362
<b>Chapter 18. Viewing Diagnostics .....</b>	<b>367</b>
Overview .....	368
Changing Diagnostics Settings .....	369
Editing the Diagnostics Settings .....	369
Resetting Diagnostics Statistics .....	370
ATS Panel Intrusion .....	371
Database Connection Pool .....	372
Database Transactions Diagnostics .....	373
Database Queries Diagnostics .....	374
Facility Membership Cache .....	375
JVM Statistics .....	376
Media Diagnostics .....	377
Service Framework Diagnostics .....	378
System Status Diagnostics .....	379
Thread Pool Manager Diagnostics .....	380
<b>Chapter 19. Advanced Configuration .....</b>	<b>381</b>
Customizing Launcher Window .....	382
Adding Custom Icons .....	382
Adding External Applications .....	383
Verifying Computer Host Name .....	384
Changing the Host Name or IP Address .....	385
Changing the Client Encryption .....	387
Changing the Host Name on Server Record .....	387
Editing the Host File on a Client System .....	387
Editing the Client Properties File on a Client System .....	388
Editing the Picture Perfect Configuration File .....	388
Enabling SSL Encryption for Picture Perfect .....	388
Copying File from Facility Commander .....	389
Moving File to Picture Perfect .....	391
Generating Picture Perfect Key File .....	391
Generating Picture Perfect Certificate Request .....	392
Generating Picture Perfect Signed Certificate .....	393
Generating Picture Perfect PEM File .....	393
Updating EIF Event Manager Configuration File .....	393
Updating EIF Request Manager Configuration File .....	395
Copying Certificate to Facility Commander Server .....	397
Adding Picture Perfect Certificate .....	398
Enabling SSL Communication on Facility Commander .....	399
<b>Appendix A. Edit Configuration Files for Informix Backup to Disk .....</b>	<b>401</b>
Configuration Files .....	402
Editing the Informix Configuration File .....	403
Scheduling the Backup Utility .....	404
Create a Cron Task .....	404
Launch the Script Manually .....	404

---

<b>Appendix B.</b>	
<b>Troubleshooting Information .....</b>	<b>405</b>
Contacting technical support .....	408
<b>Appendix C. Error Messages .....</b>	<b>409</b>
<b>Appendix D. Facility Permissions .....</b>	<b>441</b>
All Facility Permissions .....	441
Entry Level Guard Facility Permissions .....	444
Guard Supervisor Facility Permissions .....	446
Intermediate Guard Facility Permissions .....	448
Update Configuration Facility Permissions .....	450
View Configuration Facility Permissions .....	452
<b>Appendix E. System Permissions .....</b>	<b>455</b>
All System Permissions .....	455
Entry Level Guard System Permissions .....	457
Guard Supervisor System Permissions .....	458
Intermediate Guard System Permissions .....	459

# About This Document

This document describes Facility Commander and its components. It also includes instructions to configure the system and use the client applications.

## Who Should Use This Document

This document is intended for system administrators who are responsible for planning, configuring, and operating Facility Commander.

Administrators should be familiar with personal computers, client and server relationships, databases, Web browsers, and graphical user interface (GUI) navigation. They must also have a working knowledge of the following:

- Picture Perfect application
- Digital Video (CCTV) equipment
- Intercom equipment
- Intrusion equipment
- Database operations
- Security needs of the customer's facility

Operators using the system should read the chapters relating to their duties and responsibilities.

## How This Document Is Organized

This document is organized as follows:

- [Chapter 1. Introduction on page 1](#) describes the system components, and describes how remote media servers are used to transmit video.
- [Chapter 2. Getting Started on page 7](#) describes the Facility Commander Launcher, instructions on how to log in to the system using the client application, and the Web interface.
- [Chapter 3. Configuring the System on page 27](#) describes setting

up the system by identifying the Facility Commander server, Picture Perfect server, system parameters, and more.

- [Chapter 4. Importing Records on page 55](#) describes how to import Picture Perfect operators, facilities, doors, and other records to Facility Commander.
- [Chapter 5. Assigning Permissions and Context on page 99](#) describes how to assign operator permissions.
- [Chapter 6. Configuring Video Devices on page 121](#) describes how to configure DVRs, cameras, and camera preset positions, as well as CCTV Monitors and Analog Video Switchers.
- [Chapter 7. Using the Video Console on page 157](#) describes how to view live and recorded video; and how to search for video clips.
- [Chapter 8. Event Action Mapping on page 179](#) describes how to associate events to actions. When an alarm occurs, video events can be tagged for later investigation, to send e-mails, and more.
- [Chapter 9. Configuring Alarms on page 193](#) describes how to change alarm colors, create alarm instructions, and alarm profiles.
- [Chapter 10. Using the Alarm Monitor on page 205](#) describes using the Alarm Monitor window, how to select time zones, and view maps and video of alarm events.
- [Chapter 11. Using the Event Monitor on page 219](#) describes the Event Monitor window and how to filter events.
- [Chapter 12. Configuring Intercom Devices on page 231](#) describes how to configure intercom devices.
- [Chapter 13. Configuring Intrusion Devices on page 249](#) describes how to configure intrusion devices and instructions to use when connecting the intrusion equipment to Facility Commander.
- [Chapter 14. Creating Symbol Schemes on page 285](#) describes how to create a symbol scheme to use with graphic displays. Also included are instructions to upload and download files.
- [Chapter 15. Creating Graphic Displays on page 299](#) describes how to use the Symbol Editor and Graphic Editor to associate icons representing devices with graphical displays, or site maps.
- [Chapter 16. Viewing Graphic Displays on page 333](#) describes how to use the Graphics Viewer, display different layers, and issue commands such as locking and unlocking doors.
- [Chapter 17. Backup/Restore Informix Databases on page 349](#) describes the information needed to backup/restore Informix databases.
- [Chapter 18. Viewing Diagnostics on page 367](#) describes the information needed to monitor the system.
- [Chapter 19. Advanced Configuration on page 381](#) provides advanced system configuration information.
- [Appendix A. on page 401](#) lists configuration files for Informix backup.
- [Appendix B. on page 405](#) lists miscellaneous problems and describes the causes and appropriate actions.

- 
- [Appendix C.on page 409](#) lists Facility Commander error messages and suggestions to resolve the errors.
  - [Appendix D.on page 441](#) lists facility permission configurations for this application.
  - [Appendix E.on page 455](#) lists permission configurations for each Facility Commander component.

## Using This Document

This document is available in portable document format (PDF). The PDF document has been designed for online, interactive viewing with Adobe® Acrobat® Reader.

The Acrobat Reader is available for the Windows®, Macintosh®, Unix®, Linux®, and IBM® AIX®. The Acrobat Reader can be obtained for free from Adobe Systems Incorporated (<http://www.adobe.com>).

The table of contents, bookmarks, cross-references, index entries, and thumbnail pages are active navigation elements. Cross-references and links are displayed in blue. Select these elements to quickly move through the document. Any page in the document or the entire document can be printed while viewing it in Acrobat Reader.

# Conventions Used In This Document

The following conventions are used in this document:

<b>Bold</b> type	<ul style="list-style-type: none"><li>• Text to be entered by the reader.</li><li>• Menu items, buttons, programs, and other GUI elements selected with a mouse or keyboard by the reader.</li></ul>
<i>Italic</i> type	<ul style="list-style-type: none"><li>• Titles of books and various documents.</li><li>• Cross-references to headings within a document.</li><li>• E-mail and Web site (or URL) addresses.</li><li>• Emphasis of an instruction or point.</li><li>• Variables.</li></ul>
<b>Monospace</b> type	<ul style="list-style-type: none"><li>• Text that displays on the computer screen</li><li>• Examples of path names or coding sequences</li></ul>
<a href="#">Blue</a> , <i>blue</i> , or <u>blue</u> type	<ul style="list-style-type: none"><li>• In online versions of this document, hyperlinked elements that take the reader directly to the cross-references, related topics, and URL addresses.</li></ul>

---

## Related Documents

The following documents contain information about Facility Commander:

- *Facility Commander 2.2 Release Notes*  
This document includes late-breaking information on Facility Commander and notes on new enhancements and fixes.
- *Facility Commander 2.2 Installation Manual*  
This document describes how to install Facility Commander and its components. It also includes instructions to connect hardware and other peripheral devices.
- *Facility Commander 2.2 with VisioWave Setup Guide*  
This document describes how to install and configure VisioWave for Facility Commander.

The following documents contain information about the Picture Perfect access control application:

- *Picture Perfect 4.0 Installation Manual*  
This document describes how to install and configure the Picture Perfect application.
- *Picture Perfect 4.0 User Manual*  
This document describes how to configure, and manage the Picture Perfect application. It describes the Picture Perfect interface and contains step-by-step procedures to use the application.
- *Picture Perfect Enterprise Edition User Manual*  
This document describes how to configure, and manage the Picture Perfect Enterprise application. It describes the Picture Perfect interface and contains step-by-step procedures to use the application.
- *Picture Perfect Redundant Edition User Manual*  
This document describes how to configure, and manage the Picture Perfect Redundant (PPRS) application. It describes the Picture Perfect interface and contains step-by-step procedures to use the application.





# Chapter 1. Introduction

This chapter describes Facility Commander and its features, including integrated video and video management. Readers should familiarize themselves with this chapter before proceeding to other chapters in this document.



---

**In this chapter:**

[Overview on page 2](#)

[Video management on page 3](#)

## Overview

Facility Commander is a security integration platform that provides integrated digital video, analog video switchers, intercom, and intrusion with access control. It interfaces with Picture Perfect, which continues to perform all access control, alarm, and reporting tasks.

The main features of Facility Commander include a comprehensive alarm management system with direct access to graphical maps and video clips from the Alarm Monitor, and a high-level command and control interface to Digital Video Recorders (DVRs) and their connected cameras.

Configuring Facility Commander is accomplished using a Web browser, such as Internet Explorer. Operators select which facilities, doors, inputs, and outputs they want to control from Facility Commander and import these records from the access control system.

The alarm events associated with these devices can be configured to perform any number of actions in Facility Commander. For example, if a door has a video camera monitoring it, whenever a Door Forced alarm occurs, the system can be configured to send an e-mail notice to the Security Supervisor, and also tag the video clip so it can be reviewed later.

Monitoring the system is accomplished using the Facility Commander Launcher, which provides the capability to monitor alarms and control video cameras. All alarms generated by Picture Perfect are sent to the access control system's Alarm Monitor, and also to the Facility Commander Alarm Monitor. From the Facility Commander Alarm Monitor, security personnel can perform all of the operations that they can do on Picture Perfect, and more.

The Facility Commander Command and Control client features include:

- Create or import site maps for graphical representation of device and alarm locations
- Associate symbols and icons with devices, such as doors, intercoms, intrusion devices, and cameras
- Display a graphical map showing the location of an alarm and the alarm state
- Control devices from graphical maps, such as locking or unlocking a door
- Acknowledge alarms from either the graphical map or from the alarm monitor
- View recorded video clips associated with alarm events
- View live video from fixed or PTZ cameras
- Control a PTZ camera on-screen by using the mouse to pan, tilt, and zoom
- Search for video clips stored on a DVR by event, event type, camera, DVR, or motion

## Video management

The key feature of Facility Commander is integrated digital video. There are two architectural configurations available, depending on the organization's size and geographic locations.

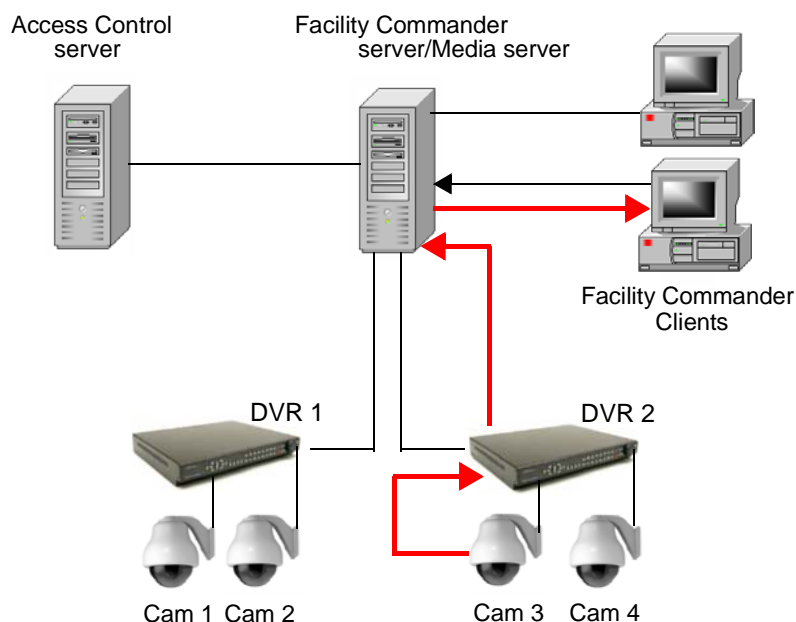
If the site is relatively small or in one central location, then the Media server can be installed on the Facility Commander Application server to manage the video services.

In large environments with several geographically distributed sites, it may be undesirable to transmit video clips across the network. In this case, adding a Remote Media server to the system improves the video transmission process.

### Centralized video management

Using a single server configuration, this example describes the events that occur when an operator wants to view video. The Media server, installed on the Facility Commander Application server shown in [Figure 1](#), has two DVRs with four cameras and two client workstations.

**Figure 1.** Single server with centralized video



The illustration includes the following process:

- The client workstation sends a message to the Facility Commander Application server requesting a connection to camera three.
- The Facility Commander Application server performs a lookup in the database to identify which DVR the camera is connected to, and which system controls and manages the components. In this example, there is only one Facility Commander Application server in the network.

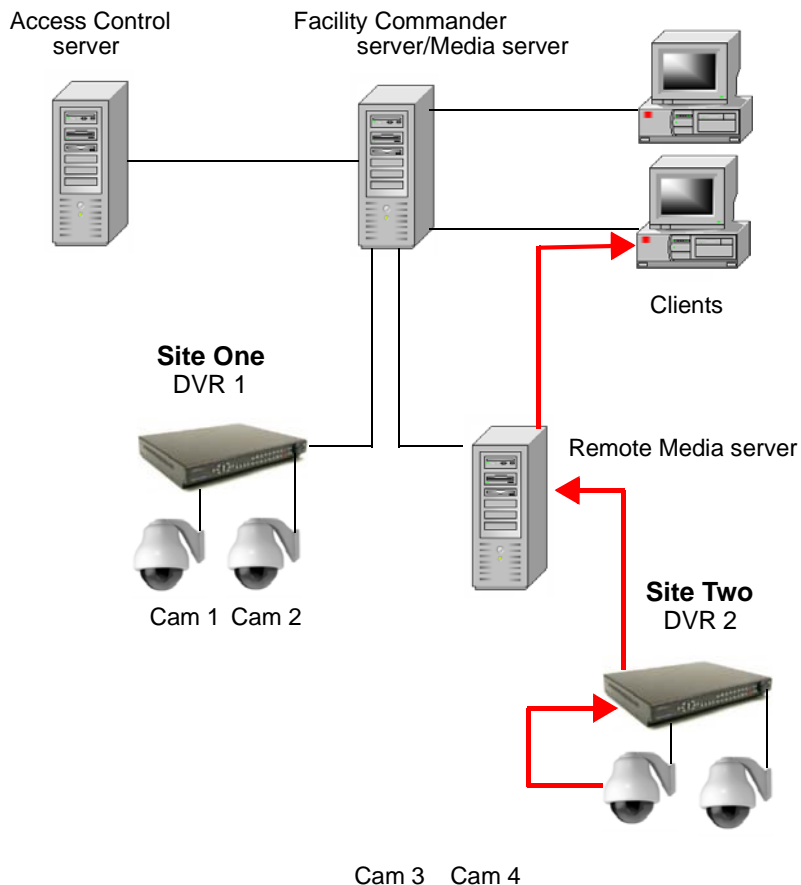
- The Facility Commander sends a message to the Media server (installed on the Facility Commander Application server) to expect a connection from the client system. The client system opens a TCP/IP connection socket to the Media server with the server configuration to receive the video stream.
- The Media server sends compressed video from the associated DVR to the client workstations. Using the Video Viewer application, the operator is able to view the video stream from camera three.

## Distributed video management

Using a Facility Commander server with a Remote Media server, this example describes the events when an operator from a remote location wants to view video. In this example, the Media server transmits the video from the camera device to the client application.

Figure 2 shows two sites that can be located anywhere — in the same city or different cities. Both sites have two DVRs, four cameras, and two client workstations.

**Figure 2.** Typical configuration with Remote Media server



This illustration describes the events when an operator using the Video Viewer on the client system requests video from camera three. This camera device is located at site two, which is managed by the Media server as shown in [Figure 2](#).

- The client system sends a message to Facility Commander server requesting a connection to camera three.
- The Facility Commander server performs a lookup in the database to identify which DVR the camera is connected to, and which system controls and manages the components.
- The Facility Commander sends a message to the remote Media server to expect a connection from the client system. The client system opens a TCP/IP connection socket to the Media server with the server configuration to receive the video stream.
- The remote Media server sends compressed video from the associated DVR to the client workstations. Using the Video Viewer application, the operator is able to view the video stream from camera three.

The Media server guarantees that local video does not have to be processed by a Facility Commander server located remotely, but by the Remote Media server that is closer to the client workstations.



## Chapter 2. Getting Started

This chapter describes how to log in and use the Facility Commander Launcher to open other applications; and how to use the Web browser to configure the system. Also included are instructions on how to navigate the browser interface and a description of the common elements, including error messages.

Readers should familiarize themselves with this chapter before proceeding to other chapters in this document.



---

**In this chapter:**

[Overview on page 8](#)

[Facility Commander Launcher on page 9](#)

[Logging In from a Workstation on page 12](#)

[Logging In Using the Web Application on page 14](#)

[Using the Web Browser Application on page 14](#)

[Managing Multiple Windows on page 20](#)

[Customizing Window Name and Contents on page 22](#)

[Error Messages on page 23](#)

[Navigating the Multi Viewer on page 24](#)

## Overview

This chapter introduces you to the Facility Commander interface and describes how to log in and access the Web browser interface and other client applications.

### Starting and Stopping Facility Commander Server and Media Server Services

Facility Commander services are started automatically in Windows and Linux/AIX operating systems. Use `http://hostname: 8085/Merlin` URL to access the Web pages to configure Facility Commander.

#### Facility Commander Server

The following procedures are used to stop and start services for the Facility Commander server. Always stop the services before restarting them to clear any lock files.

➤ **To stop services on a Linux server:**

1. You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.
2. Type the following command:

```
service facilityCommander stop
```

➤ **To start services on a Linux server:**

1. You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.
2. Type the following command:

```
service facilityCommander start
```

—or—

```
/etc/rc.d/init.d/facilityCommander start
```

➤ **To stop services on an AIX server:**

You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.

Type the following command:

```
/var/FacilityCommanderServer/server/bin/  
FCShutdown.sh
```

➤ **To start services on an AIX server:**

1. You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.
2. Type the following command:

```
/etc/rc.fcserver
```



## Media Server

The following procedures are used to stop and start services for the Facility Commander Media server:

➤ **To stop services on a Linux server:**

1. You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.
2. Type the following command:  

```
service fcmediad stop
```

➤ **To start services on a Linux server:**

1. You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.
2. Type the following command:  

```
service fcmediad start
```

—or—

```
/etc/rc.d/init.d/fcmediad start
```

➤ **To start or stop services on a Windows server:**

1. You *must* be logged in as the administrator user. If not, log out and log back in as a user with these permissions.
2. Click Start, Settings, Control Panel, Administrative Tools, and then click Services. The Services window displays. Locate the Facility Commander Media server services.
3. Right-click on Facility Commander Media server and select either Stop or Start.

## Facility Commander Launcher

When the client application is started from a workstation, it displays the Facility Commander Launcher window which allows you to launch other client applications, display Web pages to configure network parameters for client-to-server communications, and log out.

Using the Facility Commander Launcher shown in [Figure 3 on page 10](#), you can open the Web browser and other client applications, such as:

- Alarm Monitor
- Event Monitor
- Video Console
- Graphics Viewer
- Multi Viewer
- Graphics Editor
- Symbol Editor

The Facility Commander Launcher window can be minimized to display as a toolbar as shown in [Figure 4 on page 11](#). The Launcher can also be customized — you can replace the icons and you can add up-to-six additional icons to launch other applications, such as WaveReader. Refer to [Customizing Launcher Window on page 382](#).




The items appearing on the Facility Commander Launcher window depend on the Facility Commander user's context and permissions. The system administrator may be able to view all the items while another operator may only be able to view the Alarm Monitor. Refer to [Assigning Permissions and Context on page 99](#) for more information.








**Figure 3.** Facility Commander Launcher window

[Table 1](#) lists and describes the elements of the Facility Commander Launcher.

**Table 1.** Facility Commander Launcher elements

Element	Description
<b>Title Bar</b>	Displays the user's name, the Facility Commander server name, and the user's context information.
<b>Menu Bar</b>	Displays a menu bar that allows you to launch the client applications, access the Facility Commander Web browser, open the Online Help system, and exit.
<b>Login/Logoff Button</b>	Click this button to log in to or exit from Facility Commander.
<b>Toolbar Icons</b>	Select the appropriate icon from the toolbar to open a client application or Web browser interface.
	Use to launch the Multi Viewer application.
	Use to launch the Alarm Monitor application.
	Use to launch the Event Monitor application.

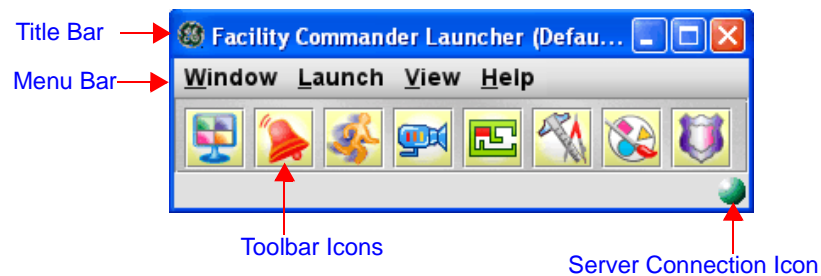
**Table 1.** Facility Commander Launcher elements

Element	Description
	Use to launch the Video Console application.
	Use to launch the Graphic Viewer application.
	Use to launch the Graphic Editor application.
	Use to launch the Symbol Editor application.
	Use to launch the Facility Commander Web browser application.
<b>Server Connection Icon</b>	Indicates if the system with the client application is connected to the Facility Commander server. <ul style="list-style-type: none"> <li>Green indicates the client application is communicating with the server.</li> <li>Red indicates the client application is no longer communicating with the server.</li> </ul>

## Minimizing Facility Commander Launcher

- To minimize the Facility Commander Launcher window, follow these steps:

1. Select **View**.
2. Select **Toolbar**. The minimized Facility Commander toolbar displays as shown in [Figure 5](#).

**Figure 4.** Facility Commander Launcher (minimized) elements

[Table 2 on page 12](#) lists and describes the elements of the Facility Commander Launcher.

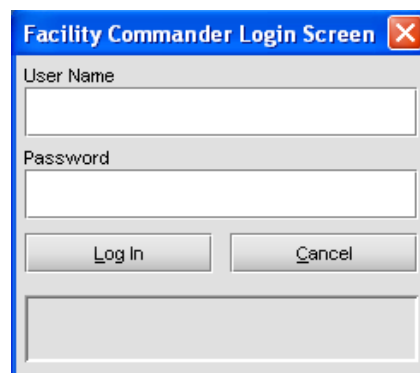
**Table 2.** Facility Commander Launcher elements (Minimized)

Element	Description
<b>Title Bar</b>	Displays the user's name, the Facility Commander server name, and the user's context information.
<b>Menu Bar</b>	Displays a menu bar that allows you to launch the client applications, access the Facility Commander Web browser, open the Online Help system, and exit.
<b>Toolbar Icons</b>	Select the appropriate icon from the toolbar to open a client application or Web browser interface. Refer to <a href="#">Toolbar Icons on page 10</a> for a description of each icon.
<b>Server Connection Icon</b>	Indicates if the system with the client application is connected to the Facility Commander server. <ul style="list-style-type: none"> <li>Green indicates the client application is communicating with the server.</li> <li>Red indicates the client application is no longer communicating with the server.</li> </ul>

## Logging In from a Workstation

➤ **To display the Launcher window, follow these steps:**

1. Click **Start, Programs**, and then **Facility Commander Client**.
2. Select **Facility Commander Client**. The Facility Commander Login window in [Figure 5](#) displays.

**Figure 5.** Facility Commander Login Screen

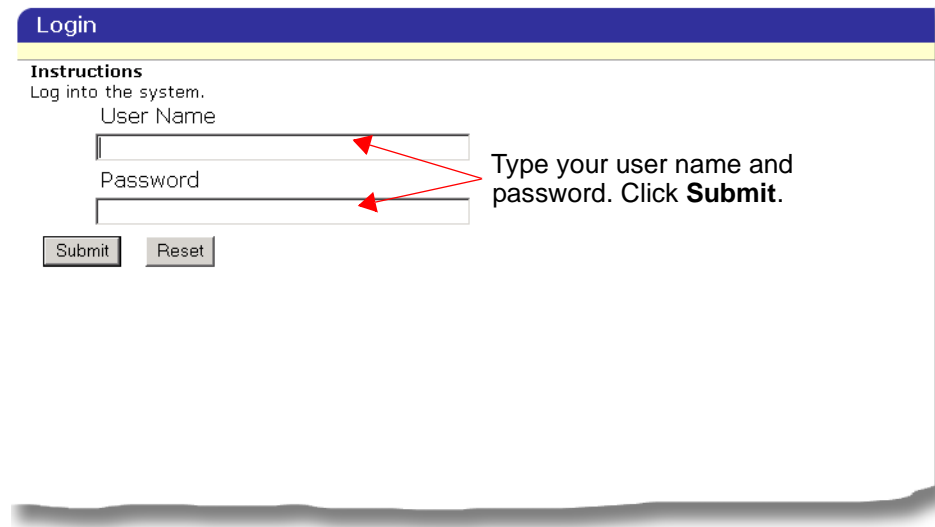
3. Enter a user name and password and click **Log In**. For more information about Login window fields, refer to [Table 3 on page 13](#).

**Table 3.** Login window fields

Field Name	REQ	Description
User Name	✓	Enter a valid user's name. The first time you log in you must log in with the name indicated by the System Administrator. Before you log in, an operator account must be created. Refer to <a href="#">Adding Operators on page 60</a> .
Password	✓	Enter a valid password. If you do not enter a password, an error message is displayed.

## Logging In Using the Web Application

The Facility Commander uses a Web browser application to configure network parameters for client-to-server communications and media devices such as cameras and DVRs, add new or import existing operators from a Picture Perfect system, and more.



The screenshot shows a web browser interface for logging in. It features a blue header bar with the word "Login" in white. Below the header, there is a section titled "Instructions" with the text "Log into the system." followed by "User Name" and "Password" labels. There are two input fields for these labels. To the right of the input fields, there is a text box that says "Type your user name and password. Click **Submit**." with two red arrows pointing to the input fields. At the bottom left, there are two buttons: "Submit" and "Reset".

**Figure 6.** Browser Interface — Login page

Table 3 on page 13 lists and describes the login fields. Refer to [Using the Web Browser Application on page 14](#) for more information about using the Web interface to configure Facility Commander.

## Using the Web Browser Application

The Facility Commander Web browser interface displays two types of pages — a list page and a configuration page. Refer to the following sections for a description of each:

- [List Page](#)
- [Configuration Page on page 19](#)
- [Client Application Title Bars on page 21](#)
- [Customizing the Multi Viewer on page 25](#)

Common elements on both pages include: page name, system messages, navigation pane, context, page displays options, and online help.

## List Page

When you select any item from the Browser Menu, the list page displays. The list page in [Figure 7](#) shows all the defined records and is sorted in alphabetical order. The list page allows you to view, copy, or delete records.

The screenshot shows the 'Access Points' list page. The top bar displays 'Current user: Default System Account | Version 2.2.0.108254 tc03 | 2009-02-06 10:15:24 | Logout'. The left sidebar contains a 'Browser Menu' with categories like Environment, Device Management, Operator Administration, System Administration, and System Diagnostics. The main content area has a 'Page Name' 'Access Points', 'Page Display Options' including a search bar and pagination controls, and a table of records. Red arrows point to the following elements:

- Information Bar**: Points to the top status bar.
- Page Name**: Points to the 'Access Points' header.
- Page Display Options**: Points to the search and pagination controls.
- Search**: Points to the search input field.
- Online Help**: Points to the 'Help' link in the top right.
- Icons**: Points to the document and copy icons in the table header.
- Links**: Points to the 'Tag Name', 'Description', 'Reference ID', and 'External System' columns.
- Browser Menu**: Points to the left sidebar menu.

Tag Name	Description	Reference ID	External System
AP 169-1-0 DOOR 1	AP 169-1-0 DOOR 1		PPSim

**Figure 7.** Browser Interface — List Page

[Table 4](#) on [page 16](#) lists and describes the elements of the List Web page.

**Table 4.** Web interface elements and descriptions

Element	Description
<b>Information Bar</b>	<ul style="list-style-type: none"> <li>Displays the operator's name that is currently logged in, server time, and the Facility Commander version number. Click <b>Logout</b> to exit from the system.</li> <li>Click the Administration Guide link to display this book. Refer to <a href="#">Using This Document on page xi</a> for more information.</li> <li>Click the Help link to display the Facility Commander online help system.</li> </ul>
<b>Page Name</b>	Displays the name of the current page.
<b>Messages</b>	Displays system messages to confirm successful entries or identifies errors in the configuration.
<b>Page Display Options</b>	<p>Displays the page number and the number of items listed on the page.</p> <ul style="list-style-type: none"> <li>Use the <b>Previous</b> and <b>Next</b> arrows to move between the pages when there are multiple pages.</li> <li>Or, type the page number in the text box and click <b>Enter</b> to display a specific page.</li> <li>Use the <b>Items per Page</b> text box to indicate how many items you would like to view on one page.</li> </ul>
<b>Search</b>	<p>Enter text in the <b>Search</b> field and click <b>Go</b>. Using this sample text "Boca" as our search text, use one of the text formats listed below:</p> <ul style="list-style-type: none"> <li>Beginning match: BOCA* returns all records that begin with Boca.</li> <li>End match: *BOCA returns all records that end in Boca.</li> <li>Any match: *BOCA* returns all records that contain the string BOCA anywhere in the field.</li> <li>Exact match: BOCA returns any record that is an exact match.</li> </ul>
<b>Browser Menu</b>	Select any entry in the navigation pane to display the appropriate Browser page. Refer to <a href="#">Browser Menu on page 18</a> for more information.
<b>Links</b>	<p>Use to access other functions, such as editing item records or logging out of the system.</p> <p>If an operator does not have permission to edit the record, the link will be disabled.</p> <ul style="list-style-type: none"> <li>Click tag name or description to make changes to an existing record. The configuration page displays, which allows you to make changes.</li> </ul>

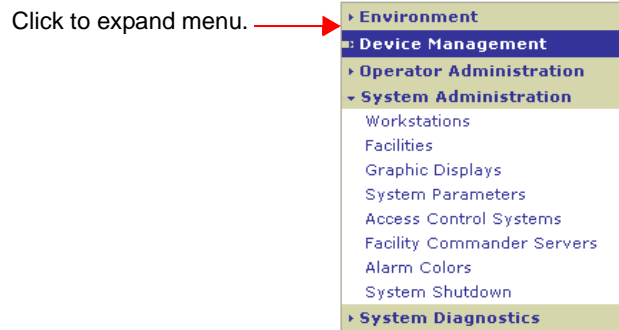


**Table 4.** Web interface elements and descriptions (Continued)

Element	Description
<b>Icons</b>	<p>Click the appropriate icon to copy, or delete a record. If an operator does not have permission to edit the record, the link will be disabled. The icons are:</p> <ul style="list-style-type: none"><li>• Click <b>Copy</b> to make a duplicate of the existing record. The configuration page displays, which allows you to change the information in the existing record. This is useful when you need to create many records with similar information.</li><li>• Click <b>Delete</b> to remove the record.</li></ul>

## Browser Menu

Use the Facility Commander Browser menu shown in [Figure 8](#) to select configuration and list pages.



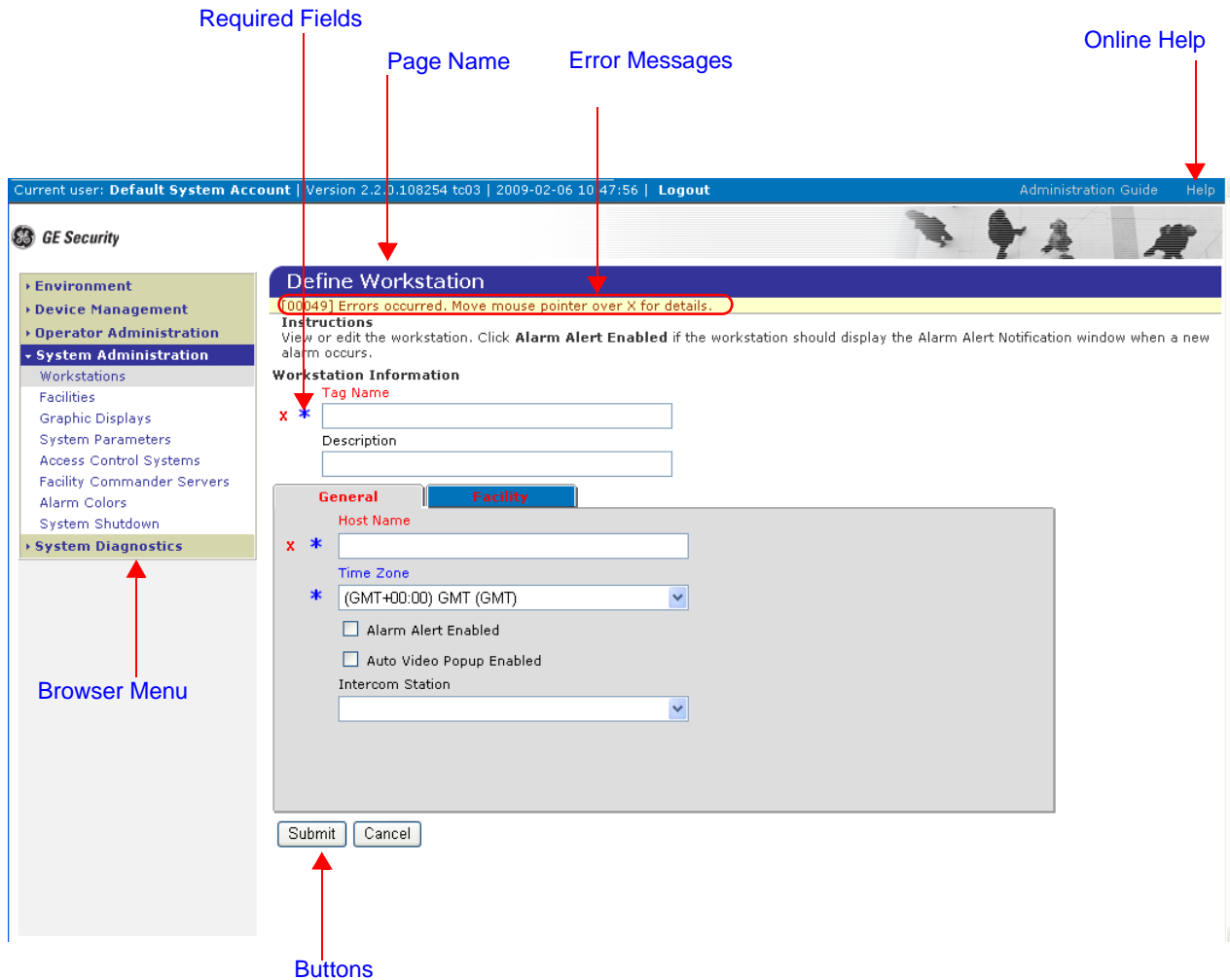
**Figure 8.** Browser menu

Select a menu name, like System Administration, and the menu expands to reveal the browser pages. The menu is divided by tasks and function, such as:

- **Environment** to access the Window Filter and set operator preferences.
- **Device Management** to configure devices, create alarm instructions, event action mappings, and more.
- **Operator Administration** to add operator records, configure permissions, and contexts.
- **System Administration** to configure Facility Commander and Picture Perfect servers, workstations, system parameters, and more.
- **System Diagnostics** to view diagnostics used for troubleshooting.

## Configuration Page

The configuration page as shown in [Figure 9](#) allows you to enter new configuration information or edit existing records in the database. The configuration page includes text boxes, drop-down lists, check boxes, and buttons.



**Figure 9.** Browser Interface — Configuration Page

[Table 5](#) lists and describes the elements of the configuration Web page.

**Table 5.** Web interface elements and descriptions

Element	Description
<b>Required Fields</b>	A blue asterisk (*) displays next to fields that require a data entry. If you do not enter the correct data in a required field, an error message displays. The field name title with the error changes to red, and a red “X” displays next to the field. Correct the entry and click <b>Submit</b> .

**Table 5.** Web interface elements and descriptions

Element	Description
<b>Page Name</b>	Displays the name of the current page.
<b>Messages</b>	A message displays to confirm data was saved successfully for the newly created records. Information displays in black text, such as "Login Successful."
<b>Error Messages</b>	A message displays to notify the user that more information is needed to save the record. <ul style="list-style-type: none"><li>• An error message displays in red text with a number preceding the message to identify the error. Refer to <a href="#">Appendix C on page 409</a>.</li></ul>
<b>Browser Menu</b>	Select any entry in the navigation pane to display the appropriate Browser page. Refer to <a href="#">Browser Menu on page 18</a> for more information.
<b>Buttons</b>	Click the appropriate button to submit, reset, or cancel a record. The buttons include: <ul style="list-style-type: none"><li>• Click <b>Add</b> to display a blank configuration page where you enter information. Required fields are indicated by an asterisk (*).</li><li>• Click <b>Import</b> to import records from the Picture Perfect system.</li><li>• Click <b>Synchronization</b> to synchronize device information between the selected Picture Perfect system and Facility Commander.</li></ul>

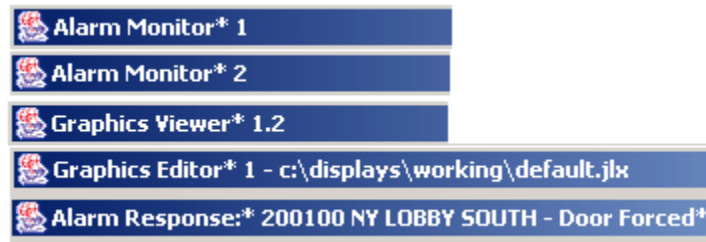
## Managing Multiple Windows

This feature allows you to open multiple client applications and arrange the windows according to your needs. You can monitor alarm activities from different locations and view video from camera positions located anywhere at the same time.

When you first open multiple window instances of the same application, the windows display in a cascade fashion. However, once you move the windows to the position and adjust the window size, the window always opens to the same position and size allowing you to create your own personal workspace.

## Client Application Title Bars

The Facility Commander client applications indicate a window number and other information in the title bar, such as a customized window title, path name, or access point and alarm type.



**Figure 10.** Title bars with window numbers, and other information

Figure 10 shows different title bars from several client applications windows. The information shown on the title bar depends on the application, such as:

- The Alarm Monitor and Event Monitor display a window number and, if configured to do so, a window title. Each time you open another Alarm Monitor or Event Monitor, another window number displays indicating the window sequence, such as 1, 2, 3, and so on. The custom window title displays only on the window where it was created.
- The Graphics Viewer displays the window number, file name, and a custom window title, if configured to do so.
- If you open the Graphics Viewer from an icon on the Alarm Monitor, the Graphics Viewer displays two window numbers, such as 1.1, 1.2, and 2.1, and so on. The first number matches the Alarm Monitor window and the second number indicates the window sequence.
- The Video Console displays the window number and custom window title, if configured to do so. An operator can open four different Video Consoles, position them, and create custom titles for each window. The next time these four Video Consoles are launched, they will return to the same position and display the custom title.
- The Graphics Editor displays the path name of the open file and window number using format 1, 2, and 3. The path name follows the window number.
- The Alarm Response window displays the access point (or device) tag name and the alarm type. An operator may have more than one alarm response window open at the same time.

## Customizing Window Name and Contents

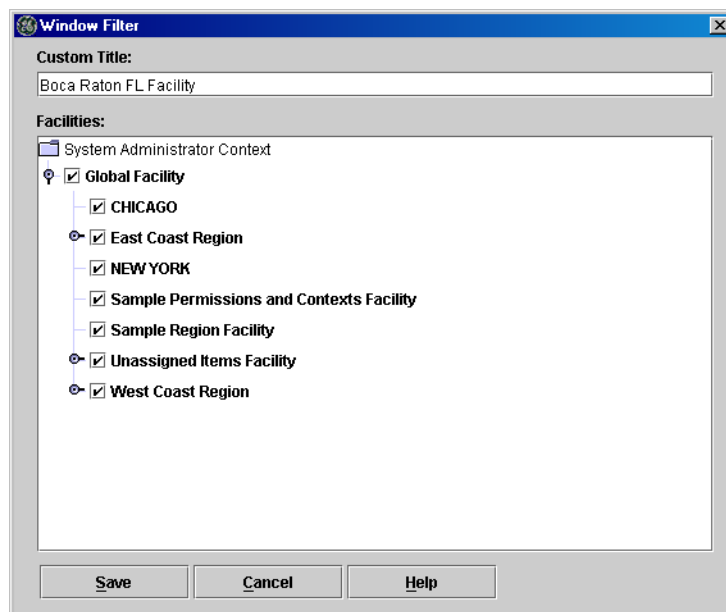
Use the **Window Filter** shown in [Figure 11](#) to modify the current display of items displayed on the Alarm Monitor, Event Monitor, Video Console, Multi Viewer, and the Graphics Viewer.

This feature is used to limit the number of items that display in the navigation pane; allowing an operator to view specific records, such as those from New York and not from Boston or Chicago.

When an operator does not have permission to modify the items in the **Change Window Filter**, the items are disabled. The operator is able to view the items displayed in the window, but not able to make any selections.

► **To filter items from view in the navigation pane, follow these steps:**

1. From the **View** menu, select **Window Filter**. The Window Filter window in [Figure 11](#) displays.



**Figure 11.** Window Filter window

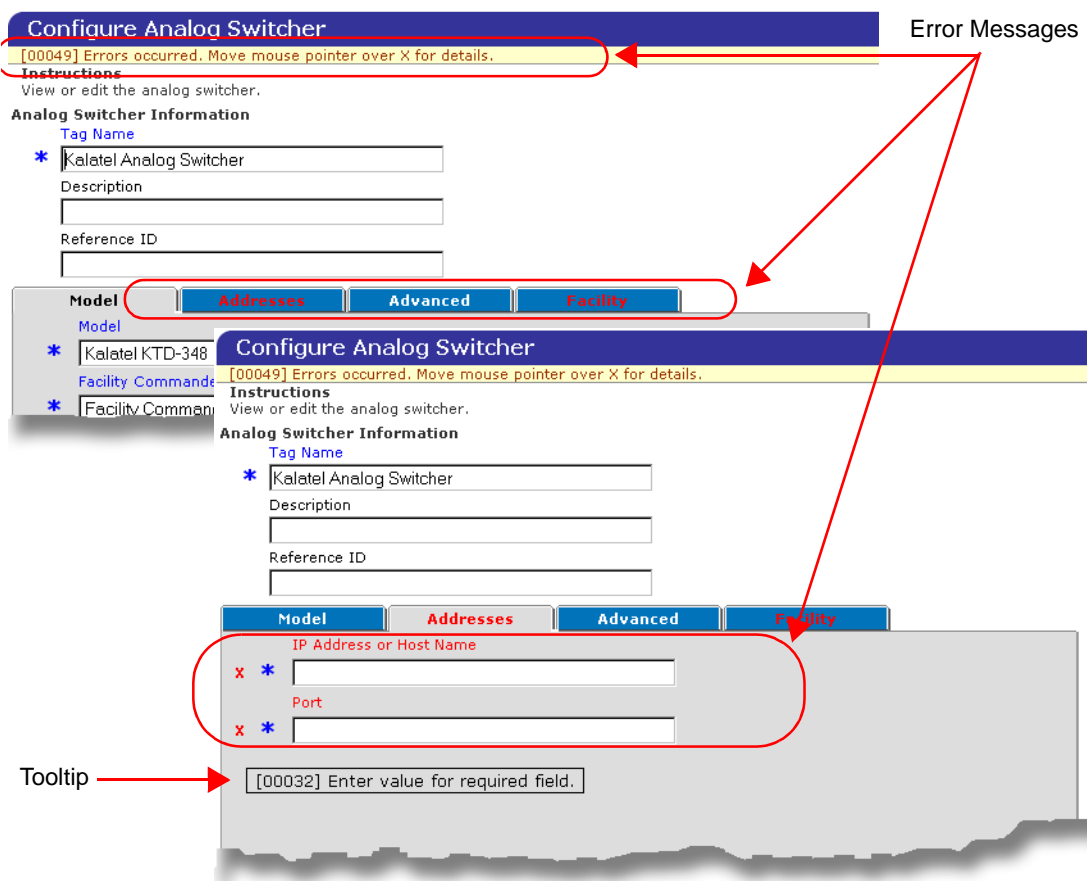
2. Use the **Custom Title** field to identify a title to display on the Video Console title bar. Maximum number of characters is 256.
3. Select the check boxes to indicate the items you want to display in the navigation pane of the client application. A check mark indicates the item is selected.
  - Clear the check boxes to remove the items from view.
4. Click **Save**. The client application displays a window filter icon in the status bar indicating the list of items has changed.

## Error Messages

Facility Commander displays error messages when the information being entered is incorrect or an option selected by an operator is not a valid action. The Facility Commander configuration pages shown in [Figure 12](#) display the error message number, tabbed page, and fields in an error condition.

In the example below there are multiple errors, such as:

- [00049] Errors Occurred. Move mouse pointer over X's for details.
- The text on the Addresses and Facility tabs turns red to identify the tabbed pages with errors.
- A red asterisk displays next to the field name to identify the location of the error. The error could be caused by missing or invalid information.
- A tooltip displays the specific error message for the field in error condition.



**Figure 12.** Configuration pages with error messages

Refer to [Appendix C on page 409](#) for a complete list of error messages.

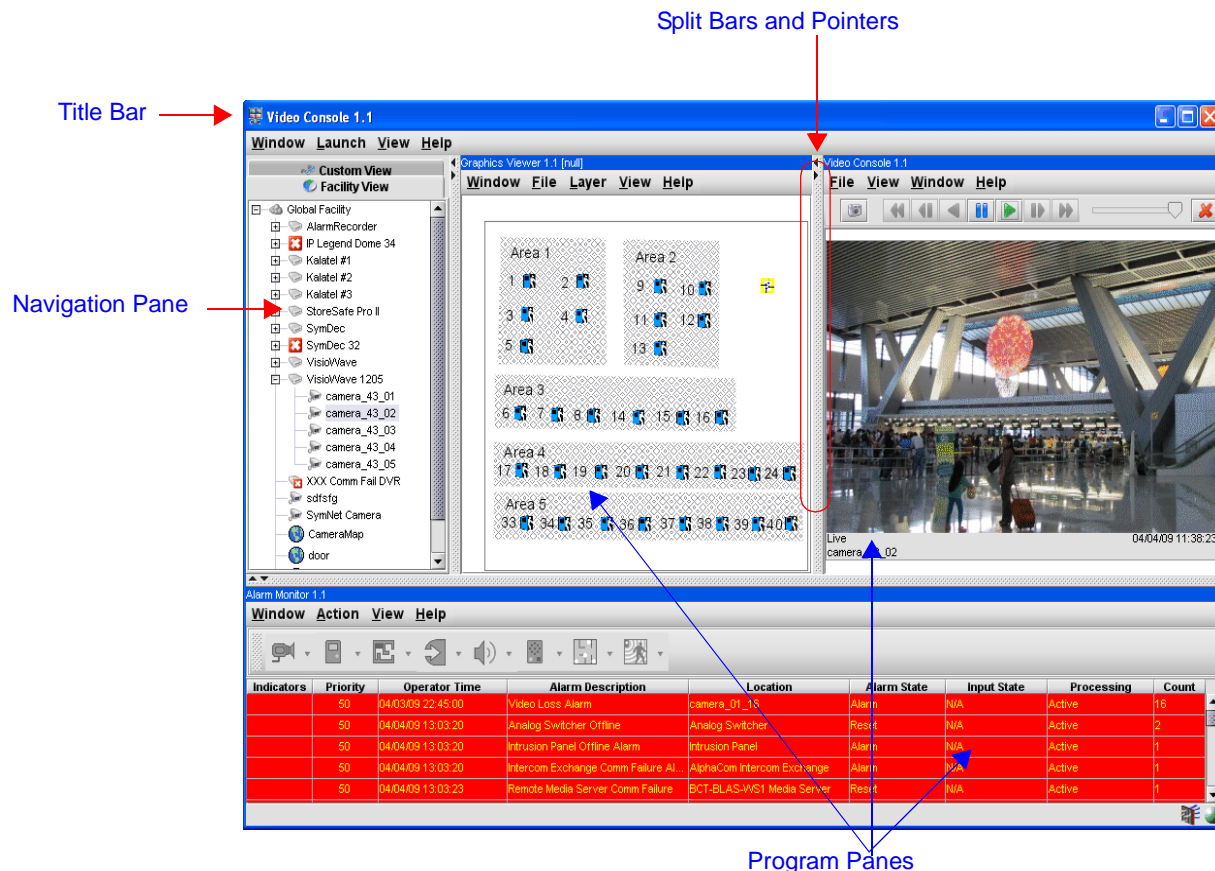
## Navigating the Multi Viewer

The Multi Viewer window in [Figure 13](#) is comprised of three separate viewing areas or panes. Each pane represents separate viewing areas, which allow multiple programs, such as the Video Console, the Graphics Viewer, Event Monitor, and the Alarm Monitor to display within a single window.

Refer to [Customizing the Multi Viewer on page 25](#) for information about changing the programs that display within the Multi Viewer.

➤ **To display the Multi Viewer, follow these steps:**

1. Select **Facility Commander Launcher**.
2. Select **Launch** and then **Multi Viewer**, or select the Multi Viewer icon from the Viewers toolbar. The Multi Viewer window as shown in [Figure 13](#) displays.



**Figure 13.** Multi Viewer window

[Table 6](#) lists and describes the elements found in the Multi Viewer window



**Table 6.** Multi Viewer elements and descriptions

Element	Description
<b>Title Bar</b>	Displays the title Multi Viewer and the window instance number, since you may open more than one occurrence of the Multi Viewer. Refer to <a href="#">Managing Multiple Windows on page 20</a> for more information.
<b>Program Menu Bar</b>	The menu bar displays the menu names specific to the active pane. Some menus contain similar commands such as <b>Open</b> , <b>Exit</b> , and <b>Help</b> . Each program menu bar is different for each program. For example, the Alarm Monitor menu allows you to select columns, customize the toolbar, and display the various commands required for alarms.
<b>Navigation Pane</b>	The navigation pane provides a hierarchal tree structure view of the links and group members. When you are using a client application, the navigation pane displays the facilities and items you have permission to access. Double-click on any item in the navigation pane to select the item.
<b>Program Title Bar</b>	Displays the client application name, such as Alarm Monitor with the window instance number. Refer to <a href="#">Client Application Title Bars on page 21</a> for more information.
<b>Program Panes</b>	Each pane represents separate viewing areas, which allow multiple programs such as the Video Console, the Graphics Viewer, and the Alarm Monitor to display within a single window. Columns within the pane can be resized by dragging either side of the column to its new position.
<b>Split Bars and Pointers</b>	Each pane is divided by a split bar with split pointers, which can be used to change the size of the window. Panes can be resized by moving the location of the splitter bars displayed between the panes or using the split pointers. Click the split pointer to move the window left or right of its current position.

## Customizing the Multi Viewer

Facility Commander allows you to customize the Multi Viewer window by selecting which client application displays. The default applications are the Graphics Viewer, Video Console, and the Alarm Monitor. The Event Monitor can be displayed as well. Use any combination of these applications, or select three of the same application.

- To close a window, use the Window menu and select **Exit**.
- To open a window, right-click in the empty pane. Select the application name from the menu. Or, select **Launch** from the Multi Viewer window and choose the application.



## Chapter 3. Configuring the System

This chapter describes how to configure the Facility Commander components, such as Facility Commander servers, and Picture Perfect systems, and more. A checklist is provided to guide system administrators in setting up Facility Commander.



---

### **In this chapter:**

- [Checklist on page 28](#)
- [Facility Commander Servers on page 31](#)
- [Access Control Systems on page 38](#)
- [Workstations on page 45](#)
- [System Parameters on page 50](#)
- [System Parameters on page 50](#)
- [System Shutdown on page 53](#)

## Checklist

After the product installation is complete, there are additional steps to complete before you begin using Facility Commander. Some of the steps are optional and can be configured later.

To configure the system, follow these steps:

**Table 7.** Checklist

Step	REQ	HTML	Action
1.	✓	Login	Log in to Facility Commander. Use the user name <i>admin</i> and the password <i>admin</i> .
2.	✓	Server	Configure the Facility Commander server. Refer to <a href="#">Facility Commander Servers on page 31</a> .
3.		Server	Define the e-mail settings, which includes the Simple Mail Transfer Protocol (SMTP) settings used for e-mail alerts. If you do not know the SMTP settings, contact the IT department for this information.
4.	✓	Access Control Systems	Configure the Picture Perfect system in the network. Refer to <a href="#">Access Control Systems on page 38</a> .
5.	✓		Reboot the Facility Commander server.
6.	✓	System Parameters	Review the system parameters and make changes, if necessary. Refer to <a href="#">System Parameters on page 50</a> .
7.	✓	Operators	Import the Picture Perfect system administrator operator records and assign the records to Global Facility. You will import other Picture Perfect operator records later in the process. Refer to <a href="#">Importing Operators on page 65</a> .
8.	✓	Operators	Assign System Administrator Context to the system administrator operator records. Refer to <a href="#">Adding Operators on page 60</a> .
9.	✓	Login	Log out of Facility Commander and log in as the newly imported system administrator.
10.	✓	Operators	Change the “admin” operator password. Refer to <a href="#">Adding Operators on page 60</a> .
11.	✓	Facilities	Import the Picture Perfect facilities and assign the records to Global Facilities. Refer to <a href="#">Importing Facilities on page 68</a> .
12.		Facilities	Create Facility Commander facilities and define their relationship to the Picture Perfect facilities.
13.	✓	System Permissions	Define the system permissions, such as viewing the Alarm Monitor. Refer to <a href="#">System Permissions on page 108</a> .

**Table 7.** Checklist (Continued)

Step	REQ	HTML	Action
14.	✓	Facility Permissions	Define the facility permissions, such as locking or unlocking doors, control cameras, and acknowledge alarms. Refer to <a href="#">Facility Permissions on page 102</a> .
15.	✓	Contexts	Define the contexts, which defines the items an operator can view and what actions they can take. Refer to <a href="#">Contexts on page 113</a> .
16.	✓	Operators	Import all other Picture Perfect operators and assign the records to Global Facility. Refer to <a href="#">Importing Operators on page 65</a> .
17.	✓	Operators	Assign the appropriate context to each operator. Refer to <a href="#">Adding Operators on page 60</a> .
18.	✓	Access Points	Import the access points and set the time zone. The access points are automatically assigned to the correct facility. Refer to <a href="#">Importing Access Points on page 75</a> .
19.	✓	Digital Inputs	Import the digital inputs and set the time zone. The digital inputs are automatically assigned to the correct facility. Refer to <a href="#">Importing Digital Inputs on page 81</a> .
20.	✓	Logical Inputs	Import the logical inputs and set the time zone. The logical inputs are automatically assigned to the correct facility. Refer to <a href="#">Importing Logical Inputs on page 87</a> .
21.	✓	Digital Outputs	Import the digital outputs and set the time zone. The digital outputs are automatically assigned to the correct facility. Refer to <a href="#">Importing Digital Outputs on page 92</a> .
22.	✓	Alarm Instructions	Create alarm instructions for Facility Commander-only alarms. Refer to <a href="#">Creating Alarm Instructions on page 199</a> .
23.	✓	Alarm Profiles	Create alarm profiles for Facility Commander-only alarms. Refer to <a href="#">Creating Alarm Profiles on page 201</a> .
24.	✓	Alarm Colors	Review the default alarm colors and make changes, as needed. Refer to <a href="#">Setting Alarm Colors on page 197</a> .
25.	✓	Digital Video Recorders	Configure the Digital Video Recorders (DVRs). Refer to <a href="#">Configuring Digital Video Recorders on page 124</a> .
26.	✓	Cameras	Configure the cameras. Refer to <a href="#">Configuring Cameras on page 132</a> .
27.	✓	Cameras	Configure the camera preset positions. <a href="#">Configuring Camera Preset Positions on page 138</a> .

Table 7. Checklist (Continued)

Step	REQ	HTML	Action
28.	✓	Digital Video Recorders	Link cameras to DVRs. Refer to <a href="#">Linking Cameras to DVRs on page 141</a> .
29.	✓	CCTV Monitors	Configure the CCTV monitors. Refer to <a href="#">Configuring CCTV Monitors on page 150</a> .
30.	✓	Analog Video Switchers	Configure the analog video switchers. Refer to <a href="#">Configuring Analog Video Switchers on page 143</a> .
31.	✓	Inputs and Outputs	Configure the inputs and outputs to use CCTV Monitors. <a href="#">Associating Analog Video Switcher Devices on page 153</a> .
32.	✓	Intercom Exchanges	Configure the intercom exchange. Refer to <a href="#">Adding an Intercom Exchange on page 234</a> .
33.	✓	Intercom Stations	Configure the intercom stations. Refer to <a href="#">Adding Intercom Stations on page 241</a> .
34.	✓	Intrusion Panels	Configure the intrusion panels. Refer to <a href="#">Configuring Intrusion Panels on page 254</a> .
35.	✓	Intrusion Areas	Configure the intrusion areas. Refer to <a href="#">Configuring Intrusion Keypads on page 266</a> .
36.	✓	Intrusion Inputs	Configure the intrusion inputs. Refer to <a href="#">Configuring Intrusion Inputs on page 276</a> .
37.	✓	Intrusion Outputs	Configure the intrusion outputs. Refer to <a href="#">Configuring Intrusion Outputs on page 281</a> .
38.	✓	Intrusion DGPs	Configure the intrusion DGPs. Refer to <a href="#">Configuring Intrusion Inputs on page 276</a> .
39.	✓	Intrusion Keypads	Configure the intrusion keypads. Refer to <a href="#">on page 284</a> .
40.	✓	Graphic Displays	Configure graphic displays to change the file name to a tag name. Refer to <a href="#">Editing Graphic Display Records on page 330</a> .
41.	✓	Event Action Mapping	Configure Event Action Mappings. Refer to <a href="#">Viewing Event Action Mappings on page 181</a> .
42.	✓	Workstations	Configure the workstations and open the <b>Facility Commander Launcher</b> on each workstation to verify the settings. Browser-only workstations are not configured. Refer to <a href="#">Logging In from a Workstation on page 12</a> .

## Facility Commander Servers

The Servers page displays a list of the defined servers, which can include an Application server and Media servers.

Use the SMTP settings when you plan on sending alarm alerts by e-mail to people in your network configuration. Contact your Information Technology (IT) department for the correct SMTP address.

### Viewing Facility Commander Servers

Use the Servers page to view, add, edit, copy, or delete a Facility Commander server record. You may need to edit this information if you make changes in the network configuration or if you want to change any of the other settings.

► **To view Facility Commander server records, follow these steps:**

1. Select **System Administration**.
2. Select **Facility Commander Servers**. The Facility Commander Servers page as shown in [Figure 14](#) displays.



**Facility Commander Servers**

**Instructions**  
View, edit, add or delete Facility Commander servers.

Search:  Go

Add Server

◀ Page 1 of 1 ▶ Go to  Go Items per Page 15 ▼

	Tag Name	Description	Reference ID	IP Address or Hostname
 	Facility Commander Server			3.18.148.62

Link to edit server information.

**Figure 14.** Facility Commander Servers page

## Adding a Facility Commander Server

- To add a Facility Commander server to the system, follow these steps:

1. Select **System Administration**, and then **Facility Commander Server**. The Facility Commander Servers page displays.
2. Click **Add Server**. The Configure Facility Commander Server page as shown in [Figure 15](#) displays.

**Figure 15.** Configure Facility Commander Server page

3. Enter the information described in [Table 8](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 8.** Configure Facility Commander Server fields and description

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.



## Address Tab

The screenshot shows the 'Addresses' tab selected in the configuration interface. The 'Host Name' field contains '3.33.133.63', the 'Port' field contains '8085', and the 'Time Zone' dropdown is set to '(GMT+00:00) GMT (GMT)'. A 'Media Server Only' checkbox is at the bottom and is not checked. Asterisks (\*) next to the Host Name, Port, and Time Zone labels indicate these are required fields.

**Figure 16.** Configure Facility Commander Server — Address tab

5. Select the **Address** tab as shown in [Figure 16](#) and enter the information described in [Table 9](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 9.** Configure Facility Commander server fields and description

Field Name	REQ	Description
Host Name	✓	Enter the host name or IP address of the Facility Commander server. The host name is case-sensitive.
Port	✓	Identify the TCP/IP port on which this server system communicates with the other systems in the network. <b>Facility Commander 2.1 server:</b> The default port for the Application server and Media server is 8085. <b>Facility Commander 2.2 server:</b> The Application server port is 8085, and the Media server port is 8083. <b>Note:</b> Because the default value populated in this field is 8083 (Media server), it must be changed to 8085 if you are configuring an Application server.
Time Zone	✓	Use the drop-down list to select the time zone for this server. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.
Media Server Only		Select this check box only if this server is a Media server. The default value is the check box is not selected.

## E-mail Server Tab

The screenshot shows the 'E-mail Server' configuration tab. It contains the following fields:

- ☐ SMTP Enabled
- SMTP IP Address or Hostname: [Text Input]
- SMTP Port: [Text Input with value 25]
- SMTP User Name: [Text Input]
- Password: [Text Input with masked characters]
- Confirm Password: [Text Input with masked characters]

**Figure 17.** Configure Facility Commander Server — E-mail Server tab

6. Select the **E-mail Server** tab as shown in [Figure 17](#) and enter the information described in [Table 10](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 10.** Configure Facility Commander Server fields and description

Field Name	REQ	Description
<b>SMTP Enabled</b>		Select the check box to enable the Simple Mail Transfer Protocol (SMTP) settings to send e-mail messages. The check box is clear by default.
<b>SMTP IP Address or Host Name</b>		Enter the host name or IP address of the SMTP server. Contact the IT department for this information, if necessary. The host name is case-sensitive.
<b>SMTP Port</b>		Required, if the SMTP Enabled check box is cleared. The default value is 25.
<b>SMTP User Name</b>		Enter a valid user name. Contact the IT department for this information.
<b>Password</b>		Enter the password. Contact the IT department for this information.
<b>Confirm Password</b>		Enter the password again.

## Advanced Tab

The screenshot shows the 'Advanced' tab of the Facility Commander Server configuration. It contains two required fields, each marked with an asterisk (\*):

- Minimum Thread Pool Size:** The input field contains the value '80'.
- Maximum Thread Pool Size:** The input field contains the value '100'.

The tabs at the top of the window are 'Addresses', 'E-mail Server', 'Advanced' (which is highlighted with a red border), 'Alarms', and 'Facility'.

**Figure 18.** Configure Facility Commander Server — Advanced tab

7. Select the **Advanced** tab as shown in [Figure 18](#) and enter the information described in [Table 11](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 11.** Configure Facility Commander Server fields and description

Field Name	REQ	Description
Minimum Thread Pool Size	✓	These values are used to control the number of concurrent activities. Enter the minimum value. The default value is 80.
Maximum Thread Pool Size	✓	These values are used to control the number of concurrent activities. Enter the maximum value. The default value is 100. As the application server grows, the thread pool size will dynamically grow.

## Alarms Tab

**Figure 19.** Configure Facility Commander Server — Alarms tab

8. Select the **Alarms** tab as shown in [Figure 19](#) and enter the information described in [Table 12](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 12.** Configure Facility Commander Server fields and descriptions

Field Name	REQ	Description
Remote Media Server Comm Failure		Use the drop-down list to select the alarm that will activate when the system is unable to communicate with the Media server. The items that appear in this list are defined in Alarm Profiles. Refer to <a href="#">Creating Alarm Profiles on page 201</a> for more information.

## Facilities Tab

The screenshot shows a configuration window with five tabs: Address, E-mail Server, Advanced, Alarms, and Facility. The Facility tab is selected and highlighted with a red circle. Below the tabs, there are two sections: 'Assigned to' and 'Available'. The 'Assigned to' section has a text box containing 'NEW YORK'. The 'Available' section has a list box containing the following items: BOCA RATON, CHICAGO, DALLAS, East Coast Region, Global Facility, LOS ANGELES, NEW YORK (highlighted in blue), PP GLOBAL, Sample Permissions and Contexts Facility, and Sample Region Facility.

**Figure 20.** Configure Facility Commander Server — Facilities tab

9. Select the **Facilities** tab as shown in [Figure 20](#) and enter the information described in [Table 13](#). A check mark indicates a required field.

**Table 13.** Configure Facility Commander Server fields and descriptions

Field Name	REQ	Description
Assigned to		Displays the facility or facilities for this server. Items can belong to more than one facility.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <p>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</p> <ul style="list-style-type: none"><li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li><li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li></ul>

## Access Control Systems

Facility Commander communicates with Picture Perfect access control systems.

The Access Control Systems list page displays the systems that communicate with Facility Commander. Each record includes a tag name and description.

Facility Commander supports these Picture Perfect 1.7 (or later) configurations:



- **Standalone** system is the typical configuration with one Picture Perfect server that manages client systems and microcontrollers.
- **Redundant** system configuration operates with two servers; one server acts as the primary and one server acts as a standby server.
- **Enterprise** system consists of a network host and multiple subhosts. Only subhosts can be configured to communicate with Facility Commander.

### Viewing Access Control Systems

Use the Access Control Systems list page to view, add, edit, copy, or delete a Picture Perfect server record.

► **To view the access control servers, follow these steps:**

1. Select **System Administration**.
2. Select **Access Control Systems**. The Access Control Systems page as shown in [Figure 21](#) displays.

	Tag Name	Description	Reference ID	Facility Commander Server
	pictureofjamie			Facility Commander Server
	PP_NY	Picture Perfect New York		Facility Commander Server

**Figure 21.** Access Control Systems page

## Adding an Access Control System

- To add a Picture Perfect system, follow these steps:
1. Select **System Administration**, and then **Access Control Systems**. The Access Control Systems list page displays
  2. Click **Add Access Control System**. The Configure Access Control System page as shown in [Figure 22](#) displays.

**Figure 22.** Configure Access Control Systems page

3. Enter the information described in [Table 14](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 14.** Configure Access Control Systems fields and description

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blueprint or wiring diagram. Use 1-20 characters.

## Address Tab

The screenshot shows the 'Address' tab of the Facility Commander configuration interface. The tab is highlighted with a red box. Below the tab are five fields, each with a blue asterisk indicating it is required:

- IP Address or Host Name:** A text input field containing '3.33.133.63'.
- Access Control System Port:** A text input field containing '8088'.
- Time Zone:** A drop-down menu showing '(GMT+00:00) GMT (GMT)'.
- Facility Commander Server:** A drop-down menu showing 'Facility Commander Server'.
- Enabled:** A checked checkbox.

**Figure 23.** Configure Access Control System — Address tab

5. Select the **Address** tab as shown in [Figure 23](#) and enter the information described in [Table 15](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 15.** Configure Access Control System fields and description

Field Name	REQ	Description
Host Name	✓	Enter the host name of the server. The host name is case-sensitive. Refer to <a href="#">Verifying Computer Host Name on page 384</a> if you do not know the system host name.
Access Control System Port	✓	Identify the TCP/IP port on which the access control (Picture Perfect) system communicates with Facility Commander. The default value is 8088.
Time Zone	✓	Use the drop-down list to select the time zone for this access control server. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.
Facility Commander Server	✓	Use the drop-down list to identify the server to communicate with the access control system.
Enabled		The check box to enable the access control system server is selected as the default value. If you do not want the access control system to communicate with Facility Commander, clear the check box to disable the server.



## External System Tab

The screenshot shows the 'External System' configuration tab. It includes a tabbed interface with 'Address', 'External System' (selected), 'Advanced', 'Alarms', and 'Facility'. The 'External System' tab contains the following fields:

- Model:** A drop-down menu with 'Picture Perfect' selected. A blue asterisk indicates it is a required field.
- User Name:** A text input field containing 'dudley.lennon'. A blue asterisk indicates it is a required field.
- Password:** A text input field with masked characters (asterisks).
- Confirm Password:** A text input field with masked characters (asterisks).

**Figure 24.** Configure Access Control System — External System tab

6. Select the **External System** tab as shown in [Figure 24](#) and enter the information described in [Table 16](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 16.** Configure Access Control System fields and description

Field Name	REQ	Description
Model	✓	Use the drop-down list to select which access control system is being used with Facility Commander.
User Name	✓	Enter the Picture Perfect operator name used by Facility Commander to connect to the access control system.
Password		Enter the operator's password.
Confirm Password		Re-enter the password.

## Advanced Tab

The screenshot shows a configuration window with five tabs: Address, External System, Advanced, Alarms, and Facility. The 'Advanced' tab is selected and highlighted with a red border. Inside the 'Advanced' tab, there are three configuration items:

- Ping Interval (seconds):** A text input field containing the number '5'. A blue asterisk (\*) is positioned to the left of the field, indicating it is a required field.
- Backup IP Address or Host Name:** An empty text input field.
- Enable Encryption With Access Control System:** A checkbox that is currently unchecked.

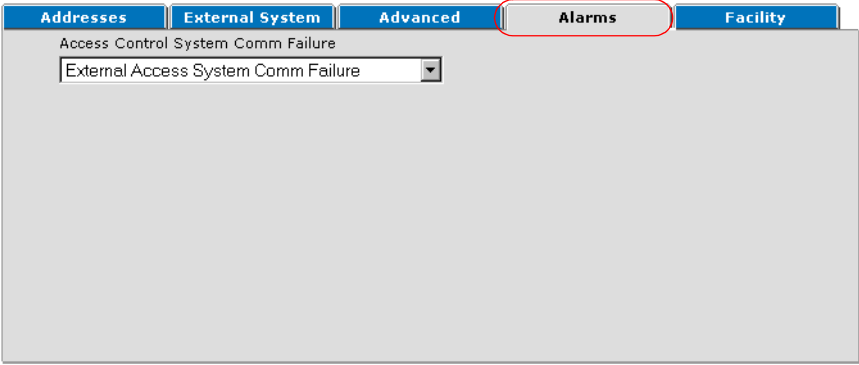
**Figure 25.** Configure Access Control System — Advanced tab

7. Select the **Advanced** tab as shown in [Figure 25](#) and enter the information described in [Table 17](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 17.** Configure Access Control System fields and description

Field Name	REQ	Description
<b>Ping Interval (seconds)</b>	✓	This is the number of seconds, or ping interval, the Facility Commander server will ping the access control system. The default setting is five seconds.
<b>Backup IP Address or Host Name</b>		If this is a redundant Picture Perfect system, enter the IP address or host name of the backup machine. The host name is case-sensitive.
<b>Enable Encryption to With Access Control System</b>		Select this check box to encrypt communication between the access control system and Facility Commander.

# Alarms Tab



**Figure 26.** Configure Access Control System — Alarms tab

8. Select the **Alarm** tab as shown in [Figure 26](#) and enter the information described in [Table 18](#). Continue to enter information on the tabbed pages.

**Table 18.** Configure access control System fields and description

Field Name	REQ	Description
Access System Comm Failure		Use the drop-down list to select the alarm that will activate when Facility Commander is unable to communicate with the access control system. The items that appear in this list are defined in Alarm Profiles. Refer to <a href="#">Creating Alarm Profiles on page 201</a> for more information.

## Facility Tab

The screenshot shows a web interface with five tabs: Address, External System, Advanced, Alarms, and Facility. The Facility tab is selected and highlighted with a red circle. Below the tabs, there are two sections: 'Assigned to' and 'Available'. The 'Assigned to' section has a text box containing 'NEW YORK'. The 'Available' section has a list box containing the following items: BOCA RATON, CHICAGO, DALLAS, East Coast Region, Global Facility, LOS ANGELES, NEW YORK (highlighted in blue), PP GLOBAL, Sample Permissions and Contexts Facility, and Sample Region Facility.

**Figure 27.** Configure Access Control — Facility Tab

9. Select the **Facility** tab as shown in [Figure 32](#) and enter the information described in [Table 19](#).

**Table 19.** Configure Access Control fields and descriptions

Field Name	REQ	Description
<b>Assigned to</b>		Displays the facility or facilities for this workstation. Items can belong to more than one facility. This is a read-only field and cannot be edited.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Workstations

Use the Workstations page to identify the computer systems in your network that can run the client applications, such as the Alarm Monitor. An operator will not be able to access any of the client applications if the workstation is not defined.

### Configuring the Alarm Alert Window

Use Workstations to enable the Alarm Alert window on a particular workstation. The Alarm Alert window in [Figure 28](#) displays on the workstation when an alarm event is generated.



**Figure 28.** Alarm Alert window

The Alarm Alert window shows the operator the number of active, unacknowledged, and highest priority alarms. Refer to [Alarm Alert on page 207](#) for more information.

### Launching the Video Console Automatically

In addition, you can configure Facility Commander workstation to automatically launch a Video Console when an alarm event occurs with associated video. Each time an alarm event occurs within the specified priority range, the Video Console launches and displays both live video and the recorded video clip of the event.

### Intercom Stations

Use Workstations to associate an intercom master station with a workstation. (The intercom device should be physically located next to the workstation.) When an operator logs onto the system using the specified workstation, they are able to connect to another intercom station from the Alarm Monitor or Graphics Viewer.

If the workstation is not configured, operators are not able to connect to any intercom stations using Facility Commander; the connection must be dialed manually.

## Viewing Defined Workstations

Use the Workstations list page to view, add, edit, copy, or delete a workstation record. Also use to edit the workstation record if you want to enable the Alarm Alert window.

► **To view workstation records, follow these steps:**

1. Select **System Administration**.
2. Select **Workstations**. The Workstations page as shown in [Figure 29](#) displays.

**Workstations**

**Instructions**  
View, edit, add or delete workstations.

Search:

◀ Page 1 of 1 ▶ Go to   Items per Page 15 ▼

	Tag Name	Description	Hostname	Alarm Alert Enabled	Auto Video Popup Enabled
	<a href="#">workstation 100</a>		bct-jlennon	Yes	No
	<a href="#">workstation 101</a>		bctmaltabet1	No	Yes
	<a href="#">workstation 102</a>		bct-jdomino	No	Yes
	<a href="#">workstation 103</a>		bctjamie-server	No	Yes
	<a href="#">workstation 104</a>		bct-jlennon	No	Yes
	<a href="#">workstation 200</a>		bctjlennon1	No	Yes

**Figure 29.** Workstations page

## Adding a Workstation

- To add a workstation, follow these steps:
1. Select **System Administration**, and then **Workstations**. The Workstations page displays.
  2. Click **Add Workstation**. The Define Workstation page as shown in [Figure 30](#) displays.

Define Workstation

**Instructions**  
View or edit the workstation. Click **Alarm Alert Enabled** if the workstation should display the Alarm Alert Notification window when a new alarm occurs.

**Workstation Information**  

Tag Name

\* workstation 100

Description

General

Facility

Hostname

\* bct-jlennon

Time Zone

\* (GMT-05:00) America/New\_York (EST)

☒ Alarm Alert Enabled
☒ Auto Video Popup Enabled

Intercom Station

NY Intercom Bldg 1\_Master

Submit

Cancel

**Figure 30.** Define Workstation page

3. Enter the information described in [Table 20](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 20.** Define Workstation fields and description

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.

## General Tab

**Figure 31.** Workstations — General tab

5. Select the **General** tab as shown in [Figure 31](#) and enter the information described in [Table 21](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 21.** Define Workstations fields and descriptions

Field Name	REQ	Description
Host Name	✓	Enter the workstation host name. The host name is case-sensitive. <b>Note:</b> The host name <i>must</i> be entered <i>exactly</i> as the "hostname" command returns it.
Time Zone	✓	Use the drop-down list to select the time zone for this server. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.
Alarm Alert Enabled		<ul style="list-style-type: none"> <li>• Select this check box to enable the Alarm Alert window to display on this workstation when an alarm occurs.</li> <li>• Clear the check box if you do not want the Alarm Alert window to display.</li> </ul>
Auto Video Popup Enabled		<ul style="list-style-type: none"> <li>• Select this check box to enable the Video Console to automatically display on this workstation when an alarm occurs.</li> <li>• Clear the check box if you do not want the Video Console to launch automatically.</li> </ul>
Intercom Station		Use the drop-down list to select the intercom station associated with this workstation.



## Facilities Tab

The screenshot shows a software interface with two tabs: 'General' and 'Facility'. The 'Facility' tab is selected and highlighted with a red rectangular box. Below the tabs, there are two main sections. The first section, labeled 'Assigned to', contains a text box with the value 'NEW YORK'. The second section, labeled 'Available', contains a list box with the following items: BOCA RATON, CHICAGO, DALLAS, East Coast Region, Global Facility, LOS ANGELES, NEW YORK (which is highlighted with a blue background), PP GLOBAL, Sample Permissions and Contexts Facility, and Sample Region Facility. The list box has a vertical scrollbar on its right side.

**Figure 32.** Workstations — Facility tab

6. Select the **Facility** tab as shown in [Figure 32](#) and enter the information described in [Table 22](#).

**Table 22.** Define Workstations fields and descriptions

Field Name	REQ	Description
Assigned to	✓	Displays the facility or facilities for this workstation. Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All of the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## System Parameters

The Configure System Parameters page displays the system locale, operator idle timeout parameter, alarm priority range to launch a Video Console, alarm priority range to require an alarm response, select video preplay time, and an option to select encryption with Facility Commander client applications.

The operator idle timeout represents the length of time that a workstation is idle before Facility Commander forces a log off.

### Launch Video Console by Alarm Priority

Facility Commander automatically launches a Video Console when an alarm event occurs with associated video, when configured to do so. Each time an alarm event occurs within the specified priority range, the Video Console launches and displays both live video and the recorded video clip of the event.

Any time an alarm event occurs within a specified priority range, the Video Console will launch displaying live and recorded video for the alarm event. If a range is not specified, the Video Console will not launch automatically.

### Require an Alarm Response

The Alarm Monitor window allows operators to respond to incoming alarms by using the Alarm Response window. Using the Alarm Response window, an operator can acknowledge, remove, or purge an alarm from the Alarm Monitor.

Any time an alarm event occurs within a specified priority range, an operator response will be required. If a priority range is not specified, alarms can be acknowledged without entering a response in the Alarm Response window.

### Configure Video Pre-Play Time

The Video Pre-Play Time feature allows you to see activities that occurred immediately before the alarm event. You can specify the number of seconds to start playing a video clip before the actual clip time. The range is from 0 to 60 seconds.

*The “number of seconds” is subtracted from the actual video start time, and playback occurs the “number of seconds” earlier than the actual alarm event.*

For example, an event action mapping definition for a forced door alarm includes video tagging. The Video Pre-Play time is set for 15 seconds. If the alarm event occurs at 10:21:30 AM, you can view the recorded video starting at 10:21:15 AM, fifteen seconds before the alarm event occurred.

## Configuring System Parameters

➤ **To make changes, follow these steps:**

1. Select **System Administration**, and then **System Parameters**.  
The Configure System Parameters page shown in [Figure 33](#) displays.

**Figure 33.** Configure System Parameters page

2. Enter the information described in [Table 23](#) to make changes. A check mark indicates a required field. Continue to enter information on the tabbed pages.
3. Click **Submit** to save the record.

**Table 23.** Configure System Parameters fields and description

Field Name	REQ	Description
<b>System Default Locale</b>	✓	Click on the drop-down list to select the language for the local system when operator locale information is not available.
<b>Operator Idle Timeout (minutes)</b>	✓	Enter the number of minutes for a session to remain idle. When the session times out, the operator will be asked to log in again. This applies to the browser and client applications. Maximum amount of time is 480 minutes.
<b>Auto Alarm Video Popup Priority Range</b>		Enter one or more priority ranges from 1-to-500. Leave this field blank to disable this option. Examples are: 1-10;300;400-500 or 1-500. Refer to <a href="#">Launching the Video Console Automatically on page 45</a> for more information.

**Table 23.** Configure System Parameters fields and description (Continued)

Field Name	REQ	Description
<b>Alarm Response Required Priority Range</b>		Enter one or more priority ranges from 1-to-500. Leave this field blank to disable this option. Examples are: <b>1-10;300;400-500 or 1-500.</b> Any time an alarm event occurs within a specified priority range, an operator response is required. Refer to <a href="#">Require an Alarm Response on page 50</a> for more information.
<b>Video PrePlay Time (seconds)</b>	✓	Enter the number of seconds to start playing a video clip before the actual clip time. Refer to <a href="#">Configure Video Pre-Play Time on page 50</a> for more information.
<b>Enable Encryption With Clients</b>		Select this check box to encrypt communication between Facility Commander and the client applications.

## System Shutdown

Use System Shutdown to initiate a shutdown of the system. All active client workstations are notified of the pending shutdown with a pop-up window. Operators using a Browser page are notified of the shutdown when the operator takes an action that causes the page to change, such as clicking **Submit** or requesting another page.

### Shutdown Notification to Client Applications

When a shutdown request is issued, all client workstations are immediately notified. A window with a progress bar displays on each workstation, with this message: **System shutdown is in progress. Application will be terminated.** When the time expires, all client workstations are immediately logged off.

### Shutdown Notification to Browser Configuration Clients

The browser workstations behave differently because the browser pages do not refresh dynamically. The page does not refresh until the operator selects another page or clicks **Submit** on a page.

When the operator takes either of these actions, the message bar displays the message: **System shutdown in progress.** When the time expires, and the operator again selects another page, the Login page is displayed with this message: **System has been shutdown.**

After a shutdown, Facility Commander must be rebooted. The Facility Commander system is automatically started as part of the reboot process.

## Shutting Down the System

- To begin a system shutdown, follow these steps:
  1. Select **System Administration**, and then **System Shutdown**. The Shutdown System page as shown in [Figure 34](#) displays.

**Shutdown System**

**Instructions**  
Specify the number of minutes delay before system shutdown and then click **Shutdown**.

Shutdown Delay Time (minutes)

\*

Initiate System Shutdown Procedure

**Shutdown** Cancel

**Figure 34.** Shutdown System page

2. Enter the number of minutes to delay before the system performs the shutdown. The default setting is five minutes.
3. Click **Shutdown**.



## Chapter 4. Importing Records

This chapter describes the how Facility Commander uses existing Picture Perfect records. Imported devices can be assigned a time zone and used on graphic displays to issue commands, such as locking and unlocking doors.



---

### **In this chapter:**

[Overview on page 56](#)

[Operator Records on page 58](#)

[Facilities on page 67](#)

[Window Filter on page 73](#)

[Access Points on page 74](#)

[Digital Inputs and Outputs on page 80](#)

## Overview

Importing Picture Perfect records allows the system administrator to identify which records to integrate with Facility Commander. Before records are added to the Facility Commander database, follow these steps:

- 
- ✓ Create an operator account for the Facility Commander administrator and remove the default operator account. Refer to [Adding Operators on page 60](#) for instructions.
- 
- ✓ Import facilities from Picture Perfect. When you import facilities before importing any other records, future imported records are assigned to the correct facility.
- 

To prevent creating duplicate records, there are two instances when you cannot import an existing record, which are:

- When the record is added manually to Facility Commander using the Web browser interface.
- When the record has already been imported into Facility Commander, the same record cannot be imported a second time.

After a record is deleted from the Facility Commander database, the record is immediately available to import again.

## Tag Names, Descriptions, and Record IDs

Facility Commander uses tag names, descriptions, and reference IDs to identify items in the database.

- **Tag names** are short text labels used to identify items in the database. The names must be unique and will be used system-wide to identify this item. Use standard ASCII characters to ensure the tag name is viewable in a Web browser, regardless of the language fonts installed on Facility Commander.
- **Descriptions** are longer text labels used to describe the records in more detail.
- **Reference IDs** are used to associate a device to a blue print or wiring diagram. Different items in the system can have the same reference ID.

## Time Zones

When importing records from a Picture Perfect system, you can assign each one to a time zone representing its location. Operators viewing alarm activity in multiple locations can see alarm activity in the configured time zone.

The Alarm Monitor and Event Monitor can be configured to display up to four time zone columns, which are:

- **GMT** indicates Greenwich Mean Time.



- **Operator** indicates the location of the operator and the default setting.
- **Server** indicates location of the server.
- **Device** indicates location of the device associated with the event.

The format is month, day, year, hour, minute, and seconds (mm/dd/yy hh:mm:ss). For example: 12/10/02 16:28:04. The date format may change depending on the operator's location.

## Synchronize Records

Sometimes an operator must change the record description of a door, input, input group, or output. Facility Commander provides the ability to synchronize descriptions so that the operator does not have to re-enter the new description in Facility Commander. For any device page, click **Synchronize** results in displaying a list of devices whose descriptions are different from those of existing imported records in Facility Commander.

If an operator changes the facility of a record, the facility must be changed manually on Facility Commander. Because facilities in Facility Commander can have more complex relationships, it is not possible for the system to make the necessary changes automatically.

Facility Commander synchronizes the device information between the selected Picture Perfect system and Facility Commander. For more information, refer to [Synchronization on page 196](#).

## Terminology

[Table 24](#) lists and describes the Picture Perfect item names, the corresponding Facility Commander names, and description.

### Picture Perfect Terms

**Table 24.** Picture Perfect and Facility Commander terms

Picture Perfect	Description	Facility Commander
<b>Doors</b>	Door + Door Input Group for Door Forced, Door Held, and Badge Alarms. Prepend AP to the Picture Perfect description.	<b>Access Points</b>
<b>Input</b>	Input (Physical Inputs that have a one-to-one relationship with their Input Group.) Prepend DI to the Picture Perfect description.	<b>Digital Input</b>
<b>Input Group</b>	Multiple DIs tied to a single Input Group, or Logical (software generated) Input Group, or Communications Failure, such as Micro Comm Fail or Reader Comm Fail. Prepend LI to the Picture Perfect description.	<b>Logical Input</b>
<b>Output</b>	Output (physical) Prepend DO to the Picture Perfect description.	<b>Digital Output</b>

## Operator Records

Facility Commander recognizes two types of operator records — external operators and local operators.

- External operators defined in the Picture Perfect system are imported into Facility Commander.
- Local operators are defined only in the Facility Commander system and not in the Picture Perfect system.

To log in to Facility Commander, operators must be defined in Facility Commander as well. Operators can be added manually or imported from the Picture Perfect system. Refer to [Importing Operators on page 65](#) for instructions.

Facility Commander provides a system administrator account called “admin.” Change the password for this account to prevent unauthorized persons from accessing the system. In the event the Picture Perfect system is offline, this account will allow access to Facility Commander.

The default system account identifies a local operator only when there are no other operators defined in the system. The default account allows you to add local operators or import external operators and begin to configure other parts of the system.

## Operator Passwords

Operator passwords are authenticated and stored on the system where they are created.

- Local operator passwords are stored and authenticated on Facility Commander;
- External operator passwords are stored and authenticated on the Picture Perfect system.

## Operator Preferences

A system administrator can identify operator preferences, such as setting the language for displays when an operator logs in and the number of items to display on the browser list page.

Refer to [Changing Operator Preferences on page 66](#) for more information.

## Viewing Facility Commander Operators

Use the Operators page to view, import, copy, add, and delete records.

► **To view Facility Commander operators, follow these steps:**

1. Select **Operator Administration**.
2. Select **Operators**. The Operators page as shown in [Figure 35](#) displays.

Operators

Instructions

Import, view, edit, add or delete operators.

Search:

Add Operator

◀ Page 1 of 1 ▶

Go to

Items per Page

pictureofjamie ▼

	Full Name	User Name	Context	External System	Preferences
	Default System Account	admin	System Administrator Context		Preferences
	Denise Dahl	DDahl	Regional Administrator Context		Preferences
	Dudley Lennon	dudley	System Administrator Context	pictureofjamie	Preferences
	Frank Zheng	FZheng	Guard Supervisor Context		Preferences
	Pierre Lefebure	PLefebure	Intermediate Guard Context		Preferences
	Vincent Raaijmakers	VRaaijmakers	Regional Administrator Context		Preferences
	Xiahoe Chu	XChu	Intermediate Guard Context		Preferences

**Figure 35.** Operators page

## Adding Operators

► To add a Facility Commander operator to the system, follow these steps:

1. Select **Operator Administration**, and then **Operators**. The Operators list page displays.
2. Click **Add Operator**. The Configure Operator page as shown in [Figure 36](#) displays.

**Figure 36.** Configure Operator page

3. Enter the information described in [Table 25](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 25.** Configure Operator fields and descriptions

Field Name	REQ	Description
User Name	✓	Enter the operator's name using the appropriate naming convention. This may be the first initial and last name. For example: fsmith Use 1-to-50 characters. Spaces are not valid.
Full Name	✓	Enter the first name and last name of the person who is assigned to the user name. For example: Fred Smith Use 1-to-50 characters. Spaces are valid.

## General Tab

The screenshot shows the 'Configure Operator' form with the 'General' tab selected. The form includes the following fields:

- Password:** A text input field.
- Confirm Password:** A text input field.
- Context:** A dropdown menu with a blue asterisk indicating it is a required field. The selected value is 'Entry Level Guard Context'.

**Figure 37.** Configure Operator — General tab

5. Select the **General** tab as shown in [Figure 37](#) and enter the information described in [Table 26](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 26.** Configure Operator fields and descriptions

Field Name	REQ	Description
<b>Password</b>		<p>The Password field is encrypted and displays asterisks.</p> <ul style="list-style-type: none"> <li>• If you have selected the <b>External System</b> check box (on <b>External System</b> tab), do not enter a password. The Picture Perfect system will authenticate the operator's account using its own password information.</li> <li>• If this user does not have an existing account on the Picture Perfect system, enter a password to access Facility Commander, which authenticates the operator's account using this password information.</li> </ul>
<b>Confirm Password</b>		<p>The new password must be entered again exactly as it was entered in the Password field.</p> <p>The Confirm Password field is encrypted and is displayed as asterisks.</p>
<b>Context</b>	✓	<p>Use the drop-down list to select the appropriate context for this operator.</p> <p>Refer to <a href="#">Contexts on page 113</a> for more information.</p>

## External System Tab

The image shows a software interface with three tabs: 'General', 'External System', and 'Facility'. The 'External System' tab is selected and highlighted with a red rectangle. Below the tabs, there is a checkbox labeled 'External System' which is currently unchecked. The rest of the tab area is a large, empty light gray rectangle.

**Figure 38.** Configure Operator — External System tab

6. Select the **External System** tab as shown in [Figure 38](#) and enter the information described in [Table 27](#).

**Table 27.** Configure Operator fields and descriptions

Field Name	REQ	Description
<b>External System</b>		Select this check box if this operator has an account on the Picture Perfect system. <ul style="list-style-type: none"><li>- When the check box is selected, the operator has access to external Picture Perfect systems.</li><li>- When the check box is not selected, the operator does not have access to external Picture Perfect systems.</li></ul>

## Facility Tab

The screenshot shows a software interface with three tabs: 'General', 'External System', and 'Facility'. The 'Facility' tab is selected and highlighted with a red circle. Below the tabs, there is a section labeled 'Assigned to' with an empty text box. Below that is a section labeled 'Available' with a list of facility names. A blue asterisk is positioned to the left of the 'Global Facility' entry in the list.

**Figure 39.** Configure Operator — Facility tab

7. Select the **Facility** tab as shown in [Figure 39](#) and enter the information described in [Table 28](#).

**Table 28.** Configure Operator fields and descriptions

Field Name	REQ	Description
<b>Assigned To</b>		Identifies the facility where the operator is assigned. Items can belong to more than one facility. This is a read-only field and cannot be edited.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Removing Default Account

*Do not remove the default system account before creating a Facility Commander operator record for the system administrator.*

- **To remove the default operator account from the system, follow these steps:**
  1. Select **Operator Administration**.
  2. Select **Operators**. The Operators list page as shown in [Figure 35](#) displays.
  3. Click the **Delete** icon next to the Default System Account item. The Confirm Deletion window with the operator's full name displays.
  4. Click **Yes** to delete the record. The default account is removed from the system.



## Importing Operators

Importing operators allows the system administrator to identify which operators can log in to Facility Commander.

➤ **To import existing operator records, follow these steps:**

1. Select **Operator Administration**, and then select **Operators**. The Operators list page displays.
2. Use the **Server** drop-down list to select the Picture Perfect server with the records you want to import to Facility Commander.
3. Click **Import**. The Import page as shown in [Figure 40](#) displays.

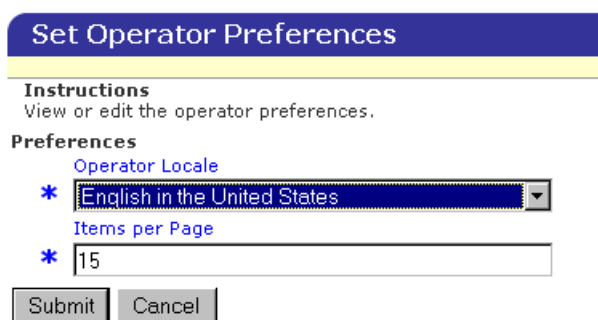
**Figure 40.** Import page

4. Use the Facility drop-down list to select a facility for the imported operators. Refer to [Facilities on page 67](#) for more information.
5. Select the operator records you want to import into Facility Commander. You can select one, several, or all the operators appearing in the list.
  - To import several operators, select the first operator and press the **Ctrl** key while selecting the other operators. The selected operator names are highlighted.
  - To import all the operators, select the first operator in the list, press the **Shift** key and select the last operator in the list. All the operator names are highlighted.
6. Click **Import**. The list page displays the operator information from the imported records.

## Changing Operator Preferences

Use the Set Operator Preferences page to set the language for displays and change the number of items that display on a Facility Commander list page.

1. Select **Environment**, and then **Preferences**. The Set Operator Preferences page displays.



**Set Operator Preferences**

**Instructions**  
View or edit the operator preferences.

**Preferences**

Operator Locale  
\* English in the United States

Items per Page  
\* 15

Submit Cancel

**Figure 41.** Set Operator Preferences

2. Use the **Operator Locale** drop-down list to select the language for the workstation.
3. Enter the number of items to display at one time on the Facility Commander list pages in the **Items Per Page** field. This becomes the operator's default setting. The number of items can be changed anytime on the list page.
4. Click **Submit** to save the record.

## Facilities

The Facility Commander facility feature is similar to Picture Perfect, but offers even more flexibility. Facilities are not limited to physical items or locations, but now include logical groupings based on operational strategy.

The facilities feature partitions the Facility Commander database into logical segments, or groupings. As a result of partitioning the database, operators assigned to a specific facility might be only permitted to view and control the items associated with only that facility, and not others.

When creating facilities in Facility Commander, consider:

- A facility can be a member of only one other facility at a given time, which means a facility can only have one parent.
- All other items can be a member of any number of facilities at any given time, which means they can have more than one parent facility.

Items include all the objects that someone can view, control, or modify, such as access points, DVRs, or alarm colors, and the Facility Commander system itself.

Facility Commander provides pre-defined and sample facility definitions and context to use when creating new facilities. The definitions include:

- **Global Facility** is the top level facility and contains all the other facilities and their associated items.
- **Sample Profiles and Context Facility** is where sample contexts, system permissions, and facility permissions are located. Use these to create context and permissions tailored to meet your organization's needs.
- **Sample Region Facility** is only referenced by the sample contexts.

Refer to the following sections for more information:

- [Viewing Facilities on page 68](#)
- [Importing Facilities on page 68](#)
- [Creating a Facility on page 70](#)

## Viewing Facilities

Use the Facilities page to view, import, add, edit, copy, or delete facility records.

► **To view the Facilities list page, follow these steps:**

1. Select **System Administration**.
2. Select **Facilities**. The Facilities page as shown in [Figure 42](#) displays.

Tag Name	Description
BOCA RATON	BOCA RATON
East Coast Region	Includes Boca Raton and New York
Global Facility	Contains all other facilities and their members
NEW YORK	NEW YORK
PP GLOBAL	PP GLOBAL
Sample Permissions and Contexts Facility	Contains sample permissions and contexts
Sample Region Facility	Sample region
West Coast Region	West Coast Region

**Figure 42.** Facilities page

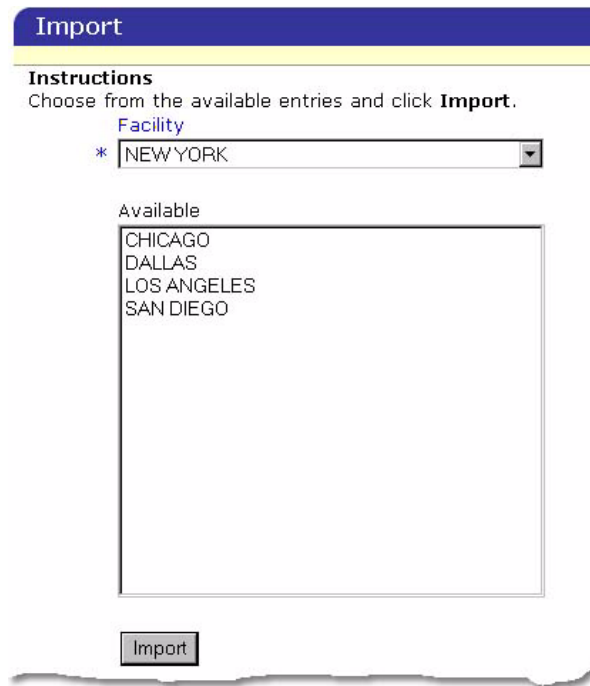
## Importing Facilities

Select the access control facilities that you want to import. The Picture Perfect Global Facility is renamed PPGLOBAL in Facility Commander. The Global Facility in Facility Commander contains all other facilities.

► **To import facilities, follow these steps:**

1. Select **System Administration**, and then select **Facilities**. The Facilities list page displays.
2. Use the **Server** drop-down list to select the Picture Perfect server with the facilities records you want to import to Facility Commander.

3. Click **Import**. The Import page as shown in [Figure 43](#) displays.



**Import**

**Instructions**  
Choose from the available entries and click **Import**.

Facility  
\* NEW YORK

Available  
CHICAGO  
DALLAS  
LOS ANGELES  
SAN DIEGO

Import

**Figure 43.** Import page

4. Select the destination facility where the imported facilities will be assigned. You can select one, several, or all the facilities in the list.
  - To import several facilities, select the first facility and press the **Ctrl** key while selecting the other facilities. The selected facilities are highlighted.
  - To import all the facilities, select the first facility in the list, press the **Shift** key and select the last facility in the list. All the facilities are highlighted.
5. Click **Import**. The list page displays the imported facilities from the Picture Perfect server.

## Creating a Facility

- To add items or operators to a facility, follow these steps:
1. Select **System Administration**, and then select **Facilities**. The Facilities list page displays.
  2. Click **Add Facility**. The Configure Facility page as shown in [Figure 44](#) displays.

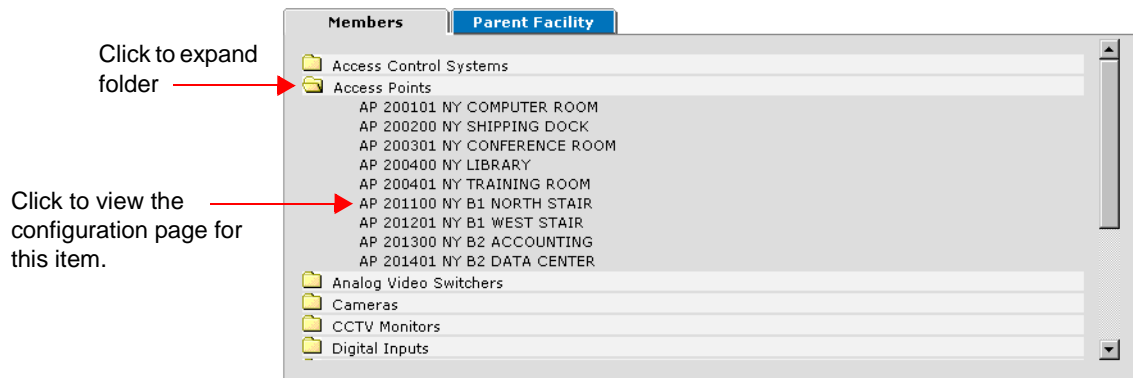
**Figure 44.** Configure Facility — Add New Facility

3. Enter the information described in [Table 29](#). A check mark indicates a required field.
  - If this is a new record, this message displays: **This facility has no members**. Continue to enter information on the tabbed pages.
  - If this is not a new record, the Members tab as shown in [Figure 45 on page 71](#) displays the items assigned to the facility
4. Click **Submit** to save the record.

**Table 29.** Configure Facility fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description.

## Members Tab



**Figure 45.** Configure Facility — Members tab

5. Select the **Member** tab as shown in [Figure 45](#). The Members tab lists all the items assigned to this facility.
  - Expand a folder to display the associated items, listed by their tag name.
  - Select an item to view the configuration page. Use the browser's back arrow to return to this page.

## Parent Facility Tab

The screenshot shows a software interface with two tabs: 'Members' and 'Parent Facility'. The 'Parent Facility' tab is active. It contains two main sections. The first section, 'Assigned to', has a text input field that is currently blank. The second section, 'Available', is marked with a blue asterisk and contains a list of facility names: BOCA RATON, East Coast Region, Global Facility, NEW YORK, PP GLOBAL, Sample Permissions and Contexts Facility, Sample Region Facility, test3, and West Coast Region.

**Figure 46.** Configure Facilities — Parent Facility tab

6. Select the **Parent Facility** tab as shown in [Figure 46](#) and enter the information described in [Table 30](#). A check mark indicates a required field.

**Table 30.** Configure Facility fields and descriptions

Field Name	REQ	Description
Assigned to		The field is blank when a new facility is being added and has not yet been assigned.
Available	✓	Displays a list of facilities. Select a parent facility where this facility should be assigned.



## Window Filter

Use the Window Filter page in [Figure 47](#) to limit the number of items in the client application navigation pane or drop-down lists. This is helpful when you are working in a large organization and you want to isolate one facility to perform troubleshooting activities.

**Window Filter**

**Instructions**  
Select the facilities that are to be active in the window filter.

**Facilities**

- ☒ Global Facility
- ☒ East Coast Region
- ☒ NEW YORK
  - ☒ Sample Permissions and Contexts Facility
  - ☒ Sample Region Facility
- ☒ Unassigned Items Facility
- ☒ West Coast Region

**Figure 47.** Window Filter page

## Changing Contents of View

Limit your view of items in Facility Commander by selecting only the facilities you want to view and filtering the remainder from view.

- **To change the items in your view, follow these steps:**
1. Select **Environment**, and then **Window Filter**. The **Window Filter** page as shown in [Figure 47](#) displays.
  2. Select the check boxes to indicate the facilities whose items you want to view. The default setting is all check boxes are selected. A check mark indicates the facility is selected and operators are able to view data from the facility.
    - Clear the check boxes to remove the facility from your view. No check mark indicates operators will not be able to view data from the facility.
  3. Click **Submit** to save the record.

## Access Points

Facility Commander imports door and reader records from existing Picture Perfect systems and creates access point records. In Facility Commander, an access point is made up of:

- Reader
- Door Contact
- Request to Exit (REX)
- Strike

Use the Picture Perfect system to configure the devices used by an access point. Use Facility Commander to configure the access points properties not defined in the Picture Perfect systems, such as associated site maps and time zones.

Refer to the following sections for more information:

- [Importing Access Points on page 75](#)
- [Editing Access Points on page 76](#)

## Viewing Imported Access Points

Use the **Access Points** page to view, import, copy, delete, and synchronize records from Picture Perfect.

► **To view access points, follow these steps:**

1. Select **Device Management**.
2. Select **Access Points**. The Access Points list page as shown in [Figure 48](#) displays.

Access Points

Instructions

Import, synchronize, view, edit or delete access points.

Search:  Go

pictureofjamie










Import

Synchronize

◀ Page 1 of 1 ▶

Go to  Go

Items per Page

	Tag Name	Description	Reference ID	External System
	AP 200101 NY COMPUTER ROOM	AP 200101 NY COMPUTER ROOM		pictureofjamie
	AP 200200 NY SHIPPING DOCK	AP 200200 NY SHIPPING DOCK		pictureofjamie
	AP 200301 NY CONFERENCE ROOM	AP 200301 NY CONFERENCE ROOM		pictureofjamie
	AP 200400 NY LIBRARY	AP 200400 NY LIBRARY		pictureofjamie
	AP 200401 NY TRAINING ROOM	AP 200401 NY TRAINING ROOM		pictureofjamie
	AP 201100 NY B1 NORTH STAIR	AP 201100 NY B1 NORTH STAIR		pictureofjamie
	AP 201201 NY B1 WEST STAIR	AP 201201 NY B1 WEST STAIR		pictureofjamie
	AP 201300 NY B2 ACCOUNTING	AP 201300 NY B2 ACCOUNTING		pictureofjamie
	AP 201401 NY B2 DATA CENTER	AP 201401 NY B2 DATA CENTER		pictureofjamie

**Figure 48.** Access Points page

## Importing Access Points

- To import access points, follow these steps:
1. Select **Device Management**.
  2. Select **Access Points**. The Access Points list page as shown in [Figure 48 on page 74](#) displays.
  3. Use the **Server** drop-down list to select the Picture Perfect server with the records you want to import.
  4. Click **Import**. The Import page as shown in [Figure 49](#) displays.

**Import**

**Instructions**  
Choose from the available entries and click **Import**.

Time Zone  
(GMT-05:00) EST (EST)

Available

- AP 100100 BOCA LOBBY EAST
- AP 100101 BOCA COMPUTER ROOM
- AP 100200 BOCA SHIPPING DOCK
- AP 100201 BOCA CAFETERIA
- AP 100300 BOCA LOBBY WEST
- AP 100301 BOCA CONFERENCE ROOM
- AP 100400 BOCA LIBRARY
- AP 100401 BOCA TRAINING ROOM
- AP 101100 BOCA B1 NORTH STAIR
- AP 101101 BOCA B1 SOUTH STAIR
- AP 101200 BOCA B1 EAST STAIR
- AP 101201 BOCA B1 WEST STAIR
- AP 101300 BOCA B2 ACCOUNTING
- AP 101301 BOCA B2 ACCTS PAYABLE
- AP 101400 BOCA B2 ACCTS RECV
- AP 101401 BOCA B2 DATA CENTER

**Import**

**Figure 49.** Import page

5. Use the **Time Zone** drop-down list to select the time zone where this access point is located.
6. Select the access points you want to import. Use the **Shift** key to select all the records or the **Ctrl** key to make multiple selections from the list.
7. Click **Import**. The Access Points list page displays the imported items from Picture Perfect.

## Editing Access Points

- To make changes to an access point, follow these steps:
1. Select **Device Management**, and then **Access Points**. The Access Points list page displays.
  2. Locate the access point you want to edit and select the link. The Configure Access Point page as shown in [Figure 50](#) displays.

	Tag Name	Description	Reference ID	External System
	AP 200100 NY LOBBY EAST	AP 200100 NY LOBBY EAST		pictureofjamie
	AP 200101 NY COMPUTER ROOM	AP 200101 NY COMPUTER ROOM		pictureofjamie
	AP 200200 NY SHIPPING DOCK	AP 200200 NY SHIPPING DOCK		pictureofjamie
	AP 200301 NY CONFERENCE ROOM	AP 200301 NY CONFERENCE ROOM		pictureofjamie
	AP 200400 NY LIBRARY	AP 200400 NY LIBRARY		pictureofjamie
	AP 200401 NY TRAINING ROOM	AP 200401 NY TRAINING ROOM		pictureofjamie
	AP 201100 NY B1 NORTH STAIR	AP 201100 NY B1 NORTH STAIR		pictureofjamie
	AP 201201 NY B1 WEST STAIR	AP 201201 NY B1 WEST STAIR		pictureofjamie
	AP 201300 NY B2 ACCOUNTING	AP 201300 NY B2 ACCOUNTING		pictureofjamie
	AP 201401 NY B2 DATA CENTER	AP 201401 NY B2 DATA CENTER		pictureofjamie

**Figure 50.** Configure Access Point page

3. Enter the information described in [Table 31](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

4. Click **Submit** to save the record.

[Table 31](#) lists and describes the fields on the Configure Access Point page.

**Table 31.** Configure Access Points fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

**Figure 51.** Configure Access Point — General tab

5. Select the **General** tab as shown in [Figure 51](#) and enter the information described in [Table 32](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 32.** Configure Access Points fields and descriptions

Field Name	REQ	Description
Graphic Display		Use the drop-down list box to select the graphic display to show when an alarm is generated for this access point. When a site plan is selected, a globe icon displays on the Alarm Monitor and Event Monitor when an alarm event occurs indicating a site plan is available.
Time Zone	✓	Use the drop-down list to select the time zone for this access point. This time zone displays on the Alarm Monitor or Event Monitor. The default time zone setting is GMT.

## Facility Tab

The screenshot shows a web interface for configuring an access point. At the top, there are two tabs: 'General' and 'Facility'. The 'Facility' tab is selected and highlighted with a red rectangle. Below the tabs, there are two main sections. The first section is labeled 'Assigned to' and contains a text input field with the value 'NEW YORK'. The second section is labeled 'Available' and contains a list of facilities. The list items are: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEW YORK' (which is highlighted in blue), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. To the left of the 'Available' list, there is a blue asterisk icon. At the bottom of the 'Available' list, there is a note: 'Hold the **Ctrl** key down for multiple selection.'

**Figure 52.** Configure Access Point — Facility tab

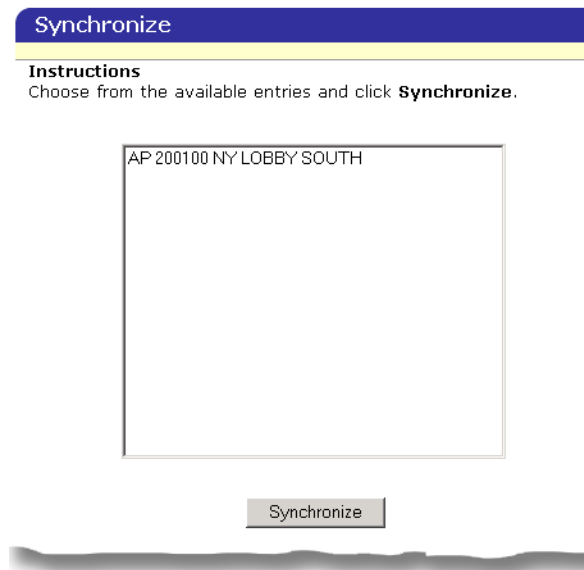
6. Select the Facility tab as shown in [Figure 52](#) and enter the information described in [Table 33](#).

**Table 33.** Configure Access Points fields and descriptions

Field Name	REQ	Description
<b>Assigned to</b>		Displays the facility or facilities for this access point. Items can belong to more than one facility. This is a read-only field and cannot be edited.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Synchronizing Access Points

- To synchronize access points, follow these steps:
1. Select **Device Management**, and then **Access Points**. The Access Points list page displays.
  2. Click **Synchronize** and the Synchronize page in [Figure 53](#) displays.



**Synchronize**

**Instructions**  
Choose from the available entries and click **Synchronize**.

AP 200100 NY LOBBY SOUTH

Synchronize

**Figure 53.** Synchronize page

3. Select the records that have changed on the Picture Perfect system that should be synchronized with Facility Commander.
4. Click **Synchronize**.

## Digital Inputs and Outputs

An input, also called a digital input (DI) or alarm input, is a physical sensing device used to monitor an electronic contact connected to a micro controller. There are three basic types of digital inputs:

- Door sensors, which monitor the door state
- Exit requests, which provide access to leave without presenting a badge
- Devices, which monitor items such as heat and moisture

An output, also called a digital output (DO), is a physical device that controls door hardware or annunciates an alarm. Outputs can also be used to turn lights, heaters, or air conditioners on and off using a schedule.

Use the Picture Perfect system to configure Inputs, Outputs, Input Groups, and Output Groups. Refer to the *Picture Perfect Administration Guide* for more information.

Refer to the following sections for more information:

- [Importing Digital Inputs on page 81.](#)
- [Importing Logical Inputs on page 87.](#)
- [Importing Digital Outputs on page 92.](#)

### Viewing Digital Inputs

Use the **Digital Inputs** page to view, import, copy, delete, and synchronize records from Picture Perfect.

➤ **To view digital inputs, follow these steps:**

1. Select **Device Management**.
2. Select **Digital Inputs**. The Digital Inputs page as shown in [Figure 54](#) displays.

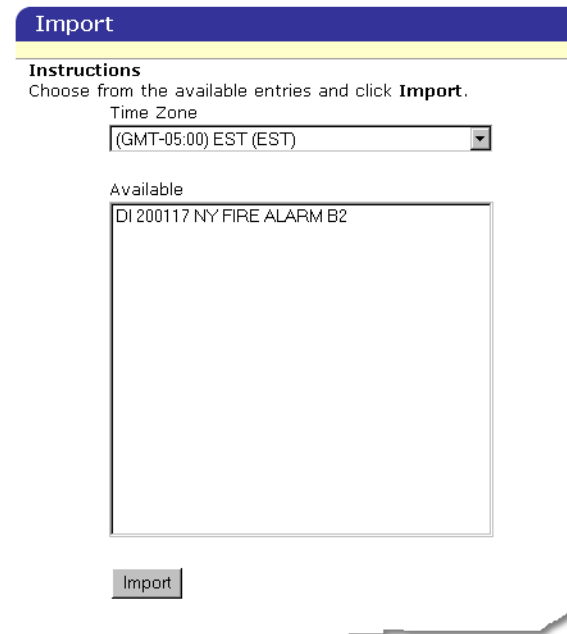
	Tag Name	Description	Reference ID	External System
	DI 200116 NY FIRE ALARM 1	DI 200116 NY FIRE ALARM 1		pictureofjamie
	DI 200117 NY FIRE ALARM B2	DI 200117 NY FIRE ALARM B2		pictureofjamie

**Figure 54.** Digital Inputs page



## Importing Digital Inputs

- To import digital inputs, follow these steps:
1. Select **Device Management**, and then **Digital Inputs**. The Digital Inputs page displays.
  2. Use the **Server** drop-down list to select the Picture Perfect server with the records you want to import.
  3. Click **Import**. The Import page as shown in [Figure 55](#) displays.



The screenshot shows the 'Import' page of a software application. At the top is a blue header bar with the word 'Import' in white. Below this is a yellow bar. The main content area has a title 'Instructions' followed by the text 'Choose from the available entries and click **Import**.' Below the instructions is a 'Time Zone' section with a drop-down menu currently showing '(GMT-05:00) EST (EST)'. Underneath is an 'Available' section with a list box containing the text 'DI 200117 NY FIRE ALARM B2'. At the bottom of the form is a button labeled 'Import'.

**Figure 55.** Import page

4. Use the **Time Zone** drop-down list to select the time zone where this device is located.
5. Select the digital inputs you want to import. Use the **Shift** key to select all the records or the **Ctrl** key to make multiple selections from the list.
6. Click **Import**. The Digital Inputs list page displays with the imported items from Picture Perfect.

## Editing Digital Inputs

Edit each digital input to change a time zone or to specify which graphic display shows in the Graphics Viewer when an alarm event occurs.

► **To make changes to a digital input, follow these steps:**

1. Select **Device Management**, and then **Digital Inputs**. The Digital Inputs list page displays.
2. Locate the digital input you want to edit and select the link. The Configure Digital Input page as shown in [Figure 56](#) displays.

**Figure 56.** Configure Digital Input page

3. Enter the information described in [Table 34](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 34.** Configure Digital Input fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

**Figure 57.** Configure Digital Input — General tab

5. Select the General tab as shown in [Figure 57](#) and enter the information described in [Table 35](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 35.** Configure Digital Input fields and descriptions

Field Name	REQ	Description
Graphic Display		Use the drop-down list box to select the site plan to display when an alarm is generated for this digital input.  When a site plan is selected, a globe icon displays on the Alarm Monitor and Event Monitor when an alarm event occurs indicating a site plan is available.
Time Zone	✓	Use the drop-down list to select the time zone for this device. This time zone displays on the Alarm Monitor or Event Monitor. The default time zone setting is GMT.

## Facility Tab

The screenshot shows a web interface for configuring digital input. At the top, there are two tabs: 'General' and 'Facility'. The 'Facility' tab is selected and highlighted with a red circle. Below the tabs, there are two main sections. The first section is labeled 'Assigned to' and contains a text box with the value 'NEW YORK'. The second section is labeled 'Available' and contains a list box with the following items: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEW YORK' (which is highlighted in blue), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. A small blue asterisk is visible to the left of the 'Available' list box.

**Figure 58.** Configure Digital Input — Facility tab

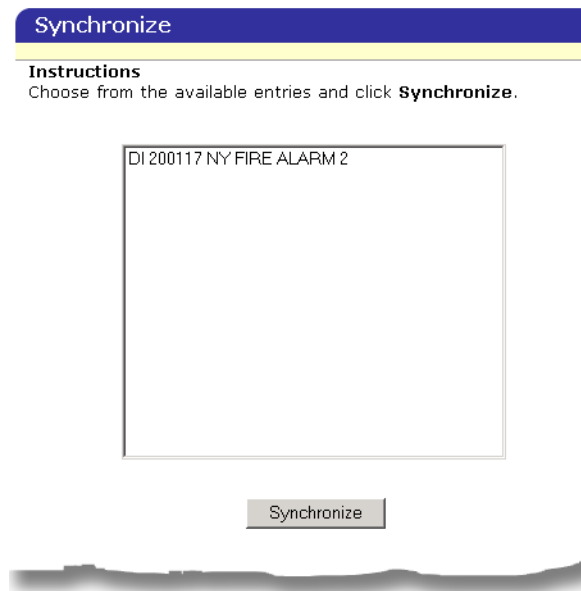
6. Select the Facility tab as shown in [Figure 58](#) and enter the information described in [Table 36](#).

**Table 36.** Configure Digital Input fields and descriptions

Field Name	REQ	Description
Assigned to		Displays the facility or facilities for this digital input. Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Synchronizing Digital Inputs

- **To synchronize digital inputs, follow these steps:**
  1. Select **Device Management**, and then **Digital Inputs**. The Digital Input list page displays.
  2. Click **Synchronize** and the Synchronize page in [Figure 53](#) displays.



**Figure 59.** Synchronize page

3. Select the records that have changed on the Picture Perfect system that should be synchronized with Facility Commander.
4. Click **Synchronize**.

## Viewing Logical Inputs

Use the Logical Inputs page to view, import, copy, delete, and synchronize logical input records from Picture Perfect.

► **To view logical inputs, follow these steps:**

1. Select **Device Management**.
2. Select **Logical Inputs**. The Logical Inputs page as shown in [Figure 60](#) displays. The Input record imported from the Picture Perfect system displays in the **Tag Name** field, with LI prepended to the name.

Logical Inputs

Request was successful.

Instructions

Import, synchronize, view, edit or delete logical inputs.

Search:

pictureofjamie

◀ Page 1 of 1 ▶

Go to

Items per Page

30

	Tag Name	Description	External System
	LI 100100 BOCA LOBBY EAST	LI 100100 BOCA LOBBY EAST	pictureofjamie
	LI 200100 NY LOBBY EAST	LI 200100 NY LOBBY EAST	pictureofjamie
	LI 200101 NY COMPUTER ROOM	LI 200101 NY COMPUTER ROOM	pictureofjamie
	LI 200200 NY SHIPPING DOCK	LI 200200 NY SHIPPING DOCK	pictureofjamie
	LI 200300 NY LOBBY WEST	LI 200300 NY LOBBY WEST	pictureofjamie
	LI 200301 NY CONFERENCE ROOM	LI 200301 NY CONFERENCE ROOM	pictureofjamie
	LI 200400 NY LIBRARY	LI 200400 NY LIBRARY	pictureofjamie
	LI 200401 NY TRAINING ROOM	LI 200401 NY TRAINING ROOM	pictureofjamie

**Figure 60.** Logical Inputs page

## Importing Logical Inputs

► To import logical inputs, follow these steps:

1. Select **Device Management**, and then **Logical Inputs**. The Logical Inputs list page displays.
2. Use the **Server** drop-down list to select the Picture Perfect server with the records you want to input.
3. Click **Import**. The Import page as shown in [Figure 61](#) displays.

**Import**

**Instructions**  
Choose from the available entries and click **Import**.

Time Zone  
(GMT-05:00) EST (EST)

Available

- LI 100101 BOCA COMPUTER ROOM
- LI 100200 BOCA SHIPPING DOCK
- LI 100201 BOCA CAFETERIA
- LI 100300 BOCA LOBBY WEST
- LI 100301 BOCA CONFERENCE ROOM
- LI 100400 BOCA LIBRARY
- LI 100401 BOCA TRAINING ROOM
- LI 101100 BOCA B1 NORTH STAIR
- LI 101101 BOCA B1 SOUTH STAIR
- LI 101200 BOCA B1 EAST STAIR
- LI 101201 BOCA B1 WEST STAIR
- LI 101300 BOCA B2 ACCOUNTING
- LI 101301 BOCA B2 ACCTS PAYABLE
- LI 101400 BOCA B2 ACCTS RECV
- LI 101401 BOCA B2 DATA CENTER
- LI 200116 NY FIRE ALARM

**Import**

**Figure 61.** Import page

4. Use the **Time Zone** drop-down list to select the time zone where this device is located.
5. Select the logical inputs you want to import. Use the **Shift** key to select all the records or the **Ctrl** key to make multiple selections from the list.
6. Click **Import**. The Logical Input list page displays with the imported items from Picture Perfect.

## Editing Logical Input Records

- To make changes to a logical input, follow these steps:
  1. Select **Device Management**, and then **Logical Inputs**. The Logical Inputs list page displays.
  2. Locate the logical input you want to edit and select the link. The Configure Logical Input list page in [Figure 62](#) displays.

**Figure 62.** Configure Logical Input

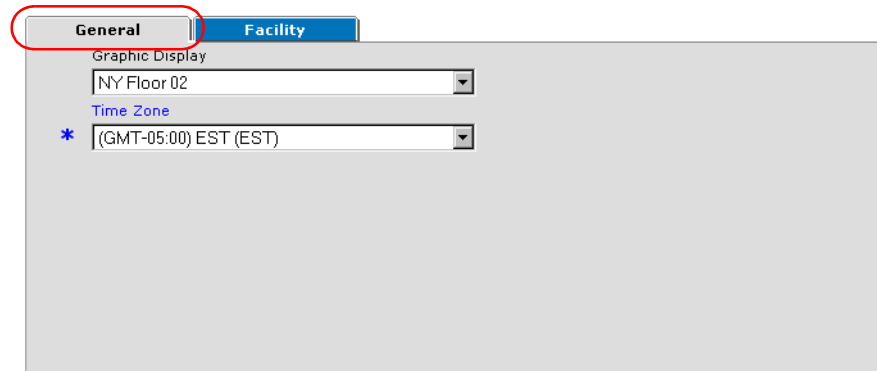
3. Enter the information described in [Table 37](#). A check mark indicates a required field. Continue to enter information on the tabbed pages. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 37.** Configure Logical Input fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.



## General Tab



**Figure 63.** Configure Logical Input — General tab

5. Select the General tab as shown in [Figure 63](#) and enter the information described in [Table 38](#). A check mark indicates a required field.

**Table 38.** Configure Logical Input fields and descriptions

Field Name	REQ	Description
Display Map		Use the drop-down list box to select the site plan to display when an alarm is generated for this logical input. When a site plan is selected, a globe icon displays on the Alarm Monitor and Event Monitor when an alarm event occurs indicating a site plan is available.
Time Zone	✓	Use the drop-down list to select the time zone for this device. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.

## Facility Tab

The screenshot shows a software interface with two tabs: 'General' and 'Facility'. The 'General' tab is active. Under the 'Assigned to' label, there is a text box containing 'NEW YORK'. Below this, under the 'Available' label, is a list box containing the following items: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEW YORK' (which is highlighted with a blue background), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. A red circle is drawn around the 'Assigned to' text box.

**Figure 64.** Configure Logical Input — Facility tab

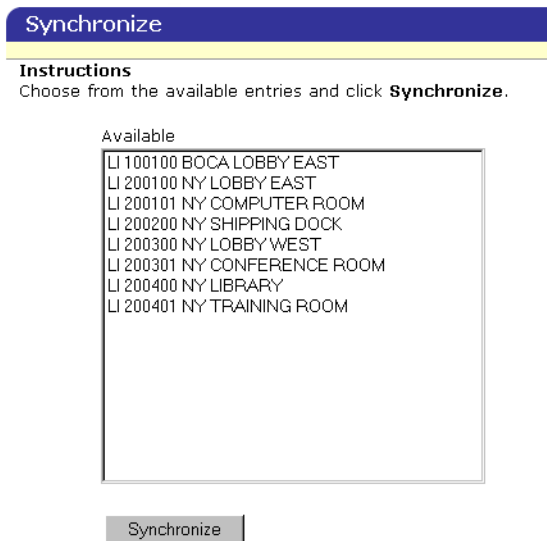
6. Select the Facility tab as shown in [Figure 64](#) and enter the information described in [Table 39](#).

**Table 39.** Configure Logical Input fields and descriptions

Field Name	REQ	Description
Assigned to		Displays the facility or facilities for this logical input. Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Synchronizing Logical Inputs

- To synchronize logical inputs, follow these steps:
1. Select **Device Management**, and then **Logical Inputs**. The Logical Inputs list page displays.
  2. Click **Synchronize** and the Synchronize page in [Figure 65](#) displays.



**Synchronize**

**Instructions**  
Choose from the available entries and click **Synchronize**.

Available

- LI 100100 BOCA LOBBY EAST
- LI 200100 NY LOBBY EAST
- LI 200101 NY COMPUTER ROOM
- LI 200200 NY SHIPPING DOCK
- LI 200300 NY LOBBY WEST
- LI 200301 NY CONFERENCE ROOM
- LI 200400 NY LIBRARY
- LI 200401 NY TRAINING ROOM

**Synchronize**

**Figure 65.** Synchronize page

3. Select the records that have changed on the Picture Perfect system that should be synchronized with Facility Commander.
4. Click **Synchronize**.

## Viewing Digital Outputs

Use the Digital Outputs page to view, import, edit, copy, delete, or synchronize digital output records from Picture Perfect.

► **To view digital outputs, follow these steps:**

1. Select **Device Management**.
2. Select **Logical Inputs**. The Logical Inputs page as shown in [Figure 60](#) displays. The Output record imported from the Picture Perfect system displays in the **Tag Name** field, with DO prepended to the name.

Tag Name	Description	Reference ID	External System
DO 200116 NY FIRE SOUNDER	DO 200116 NY FIRE SOUNDER		pictureofjamie

Figure 66. Digital Output page

## Importing Digital Outputs

► **To import digital outputs, follow these steps:**

1. Select **Device Management**, and then **Digital Outputs**. The Digital Outputs page displays.
2. Use the **Server** drop-down list to select the Picture Perfect server with the records you want to input.

3. Click **Import**. The Import page as shown [Figure 67](#) displays.

**Import**

**Instructions**  
Choose from the available entries and click **Import**.

Time Zone  
(GMT-05:00) EST (EST)

Available  
DO 200116 NY FIRE SOUNDER

Import

**Figure 67.** Import page

4. Use the **Time Zone** drop-down list to select the time zone where this device is located.
5. Select the digital outputs you want to import. Use the **Shift** key to select all the records or the **Ctrl** key to make multiple selections from the list.
6. Click **Import**. The Digital Output list page displays the imported items from the Picture Perfect server.

## Editing Digital Outputs

Edit each digital output to assign a time zone or to specify which site plan displays in the Graphics Viewer when an alarm event occurs.

► **To make changes to a digital output, follow these steps:**

1. Select **Device Management**, and then **Digital Outputs**. The Digital Outputs list page displays.
2. Locate the digital output you want to edit and select the link. The Digital Outputs page in [Figure 68](#) displays.

**Figure 68.** Configure Digital Output

3. Enter the information described [Table 40 on page 94](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 40.** Configure Digital Output fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

**Figure 69.** Configure Digital Output — General tab

5. Select the General tab as shown in [Figure 69](#) and enter the information described in [Table 41](#). A check mark indicates a required field.

**Table 41.** Configure Digital Output fields and descriptions

Field Name	REQ	Description
Graphic Display		Use the drop-down list box to select the site plan to display when an alarm is generated for this access point. When a site plan is selected, a globe icon displays on the Alarm Monitor when an alarm event occurs indicating a site plan is available.
Time Zone	✓	Use the drop-down list to select the time zone for this device. This time zone displays on the Alarm Monitor or Event Monitor. The default time zone setting is GMT.

## Facility Tab

The screenshot shows a web interface with two tabs: 'General' and 'Facility'. The 'Facility' tab is selected and highlighted with a red circle. Below the tabs, there are two sections: 'Assigned to' and 'Available'. The 'Assigned to' section has a text input field containing 'NEWYORK'. The 'Available' section has a list box containing the following items: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEWYORK' (which is highlighted in blue), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. A blue asterisk is visible to the left of the 'PP GLOBAL' item.

**Figure 70.** Configure Digital Output — Facility tab

6. Select the Facility tab as shown in [Figure 70](#) and enter the information described in [Table 42](#).

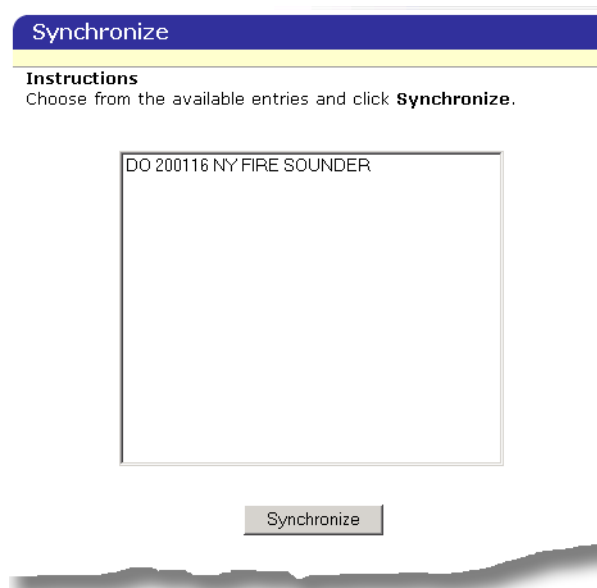
**Table 42.** Configure Digital Output fields and descriptions

Field Name	REQ	Description
<b>Assigned to</b>		Displays the facility or facilities for this digital output. Items can belong to more than one facility. This is a read-only field and cannot be edited.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>



## Synchronizing Digital Outputs

- To synchronize access points, follow these steps:
1. Select **Device Management**, and then **Digital Outputs**. The Digital Outputs list page displays.
  2. Click **Synchronize** and the Synchronize page in [Figure 71](#) displays.



The screenshot shows a web interface for the 'Synchronize' page. At the top is a blue header bar with the word 'Synchronize' in white. Below this is a yellow bar with the heading 'Instructions' in bold. The instructions text reads: 'Choose from the available entries and click **Synchronize**.' Below the instructions is a large, empty rectangular box with a thin black border. At the bottom center of the page is a grey button with the text 'Synchronize' in black.

**Figure 71.** Synchronize page

3. Select the records that have changed on the Picture Perfect system that should be synchronized with Facility Commander.
4. Click **Synchronize**.



# Chapter 5. Assigning Permissions and Context

This chapter describes how facilities, permissions, and context are assigned to operators and used to control access to features and visibility to items in the database.



---

**In this chapter:**

[Overview on page 100](#)

[Checklist on page 101](#)

[Facility Permissions on page 102](#)

[System Permissions on page 108](#)

[Contexts on page 113](#)

[Examples on page 118](#)

## Overview

Facilities, permissions, and context are used to control access to features and visibility to items in the database, such as the ability to view and edit device records or issue commands to lock and unlock access points.

### Facilities + Permissions = Context

**Figure 72.** Context definition

In the equation above, facilities determine which items an operator can see, permissions determine what actions an operator can take; and together make up the operator's context.

## Facilities

*Facilities determine which items an operator can view or access.*

The facilities feature partitions the Facility Commander database into logical segments, or grouping of items. Items include all the objects that an operator can view, control, or modify, such as access points, DVRs, and cameras.

An item can belong to more than one facility. Each facility can be a member of one other facility. Refer to [Facility Permissions on page 102](#) for more information.

## Permissions

*Permissions define what actions an operator may perform with specific items.*

Permissions can be described in terms of the operator's role, such as system administrator, guard supervisor, guards. Permission can also be described in terms of the actions that can be performed, such as viewing and updating records.

In planning the system, carefully determine the permissions that each person will require to support the tasks associated with their job responsibilities. Permissions clearly define the limits of who can view or modify information in the database.

There are two types of permissions which will be described later — system and facility.

## Context

*Context defines which items an operator can view and what actions they can take.*

Context consists of a single System Permission and one or more Facility and Facility Permission pairs. A context is created for each *type* of operator, such as entry level guard or supervisor. Refer to [Contexts on page 113](#) for information about configuring contexts.

## Pre-Defined Permissions and Context

Facility Commander provides pre-defined permissions and contexts that can be assigned to operators. These pre-defined permissions can be copied to create new permissions, but they cannot be deleted. The Delete icon is dimmed.

## Examples

Refer to the [Examples on page 118](#) to see how a typical system can be configured. Facility Commander provides sample facility, permission, and context definitions.

## Checklist

This checklist is provided to describe to the system administrator all the tasks needed to implement the facilities, permissions, and context features. The tasks begin with importing Picture Perfect facilities and end with assigning context to an operator.

- 
- ✓ Begin by importing existing Picture Perfect facilities. Imported facilities are automatically be assigned to the same facility as in Picture Perfect. Refer to [Importing Facilities on page 68](#) for more information.
- 
- ✓ Review the imported facilities and examine their relationship. Decide if the existing facility structure is suitable, or if new facilities are needed.
    - If you want to maintain the same facility structure as defined in Picture Perfect, assign the imported facilities to the Global Facility.
    - If not, create new facilities and move the imported facilities as needed.Refer to [Creating a Facility on page 70](#) for more information.
- 
- ✓ Review the facility level permissions and create new permissions, if necessary. Facility level permissions are used to grant permission to lock and unlock access points, view video, purge alarms, and more. Refer to [Adding Facility Permissions on page 104](#) for more information.
- 
- ✓ Review the system level permissions and create new permissions, if necessary. System level permissions are used to grant permission to use the client applications, such as the Alarm Monitor, create event action mappings, or shut down the system.  
Refer to [Adding System Permissions on page 110](#) for more information.
- 
- ✓ Review the context definitions and create new contexts, if necessary. The context determines which items an operator can view and what actions they may take. To define a context, select the appropriate system permission and then select the appropriate permissions for each facility.  
Refer to [Adding Context Definitions on page 114](#) for more information.
- 
- ✓ Assign a context to each operator. Context determines which items the operator can see and what actions they can take.  
Refer to [Adding Operators on page 60](#) for more information.
-

## Facility Permissions

Use Facility Permissions to grant or deny permissions to monitor and control items, such as, locking or unlocking door access points or control PTZ cameras, view live or recorded video, acknowledge alarms, and more.

A system administrator may need permissions to create or modify items such as door access points, while another operator may need only view permissions for applications such as the Alarm Monitor.

Facility Commander provides pre-defined Facility Permissions that can be modified, which include:

- **All Facility Permissions**  
Grants all permissions, including view, update, create, and delete items. This also grants permission for all actions, such as locking and unlocking doors, controlling cameras and acknowledging an alarms.
- **Update Configuration Facility Permissions**  
Grants all permissions, but not for actions like acknowledging alarms.
- **View Configuration Facility Permissions**  
Grants permissions to view all items, but not modify.
- **No Configuration Facility Permissions**  
Grants no permissions.

There are also three pre-defined guard-level permissions, which are:

- **Guard Supervisor System Permissions** grants permission to purge alarms from the Alarm Monitor in addition to the same permissions as the guard levels.
- **Intermediate Guard Permissions**
- **Entry Level Guard Permissions**

## Using Pre-Defined Facility Permissions

Use the pre-defined permissions to create new permissions. The sample permission files can be copied, but not deleted as they are permanent Facility Commander records.

- **To use one of the pre-defined facility permissions, follow these steps:**
  1. Click the **Copy** icon next to the pre-defined facility permission that you want to use. The Configure Facility Permission page as shown in [Figure 74 on page 104](#) displays.
  2. Enter the information required to modify a facility permission record.
    - Change the tag name and description.
    - Review the tabbed pages and make the appropriate modifications.
  3. Click **Submit** to save the record.

## Viewing Facility Permissions

Use the Facility Permissions page to view, add, edit, copy, or delete facility permission records. Refer to the following sections:

- [Using Pre-Defined Facility Permissions.](#)
- [Adding Facility Permissions on page 104.](#)

► **To view facility permissions, follow these steps:**

1. Select **Operator Administration**.
2. Select **Facility Permissions**. The Facility Permission page as shown in [Figure 73](#) displays.

**Facility Permissions**

**Instructions**  
View, edit, add or delete facility permissions.

Search:

◀ Page: 1 of 1 ▶ Go to:   Items per Page 15 ▼

Click to add a facility permission →

	Tag Name	Description
	All Facility Permissions	Grants ALL facility level permissions
	Entry Level Guard Facility Perms	Grants limited monitoring and command facility level permissions for guards
	Guard Supervisor Facility Perms	Grants supervisory monitoring and command facility level permissions for guards
	Intermediate Guard Facility Perms	Grants intermediate monitoring and command facility level permissions for guards
	No Facility Permissions	Grants NO facility level permissions
	Update Configuration Facility Perms	Grants configuration update facility level permissions
	View Configuration Facility Perms	Grants configuration view-only facility level permissions

Click to copy a facility permission →

**Figure 73.** Facility Permissions page

## Adding Facility Permissions

- To add or edit a facility permission, follow these steps:
1. Select **Operator Administration**, and then **Facility Permissions**. The Facility Permissions page displays.
  2. Click **Add Facility Permission** to display the Configure Facility Permissions page as shown in [Figure 74](#).

**Figure 74.** Configure Facility Permissions page

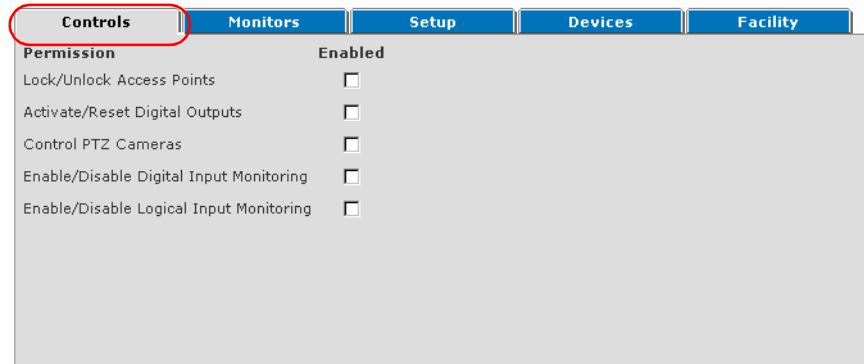
3. Enter the information described in [Table 43](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 43.** Configure Facility Permissions — Control tab

Field Name	REQ	Description
Tag Name	✓	Enter a name to identify this record. Use 2-36 characters.
Description		Enter a description for this record. Use 1-100 characters.



## Control Tab

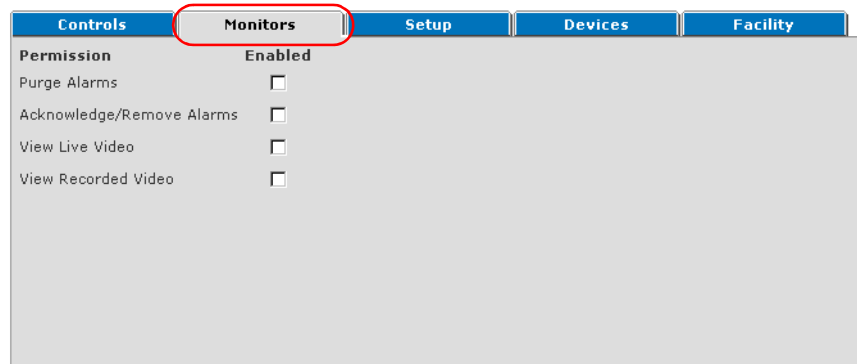


Controls	Monitors	Setup	Devices	Facility
<b>Permission</b>	<b>Enabled</b>			
Lock/Unlock Access Points	<input type="checkbox"/>			
Activate/Reset Digital Outputs	<input type="checkbox"/>			
Control PTZ Cameras	<input type="checkbox"/>			
Enable/Disable Digital Input Monitoring	<input type="checkbox"/>			
Enable/Disable Logical Input Monitoring	<input type="checkbox"/>			

**Figure 75.** Facility Permissions — Controls tab

5. Select the **Control** tab shown in [Figure 75](#) to choose one or more check boxes granting permissions. A check mark indicates the permission is enabled.
  - Enabling the Control PTZ Cameras permission also grants View Live Video permissions to be enabled. If the View Live Video permission is not enabled, the Control PTZ Cameras permission is also not enabled.

## Monitors Tab



Controls	Monitors	Setup	Devices	Facility
<b>Permission</b>	<b>Enabled</b>			
Purge Alarms	<input type="checkbox"/>			
Acknowledge/Remove Alarms	<input type="checkbox"/>			
View Live Video	<input type="checkbox"/>			
View Recorded Video	<input type="checkbox"/>			

**Figure 76.** Facility Permissions — Monitors tab

6. Select the **Monitors** tab shown in [Figure 76](#) to choose one or more check boxes granting permissions. A check mark indicates the permission is enabled.
  - Enabling the View Live Video permission also grants Control PTZ Cameras permission to be enabled. If the View Live Video permission is not enabled, the View Live Video permission is also not enabled.

## Setup Tab

Controls	Monitors	Setup	Devices	Facility	
Permission	None	View	Update	Create	Delete
Operators	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contexts	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Permissions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Facility Permissions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Facilities	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Facility Commander Servers	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Workstations	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Access Control Systems	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Figure 77.** Facility Permissions — Setup tab

7. Select the **Setup** tab shown in [Figure 77](#). For each permission, such as Workstations, select the appropriate permission level. All permissions preceding the selected button are granted.
  - If **Create** is selected, an operator has permission to view and update workstation records.
  - If **View** is selected, an operator can only view workstation records and cannot modify or delete them.
8. Review permission and select the appropriate permissions level.

## Devices Tab

Controls	Monitors	Setup	Devices	Facility	
Permission	None	View	Update	Create	Delete
Access Points	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital Inputs	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logical Inputs	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital Outputs	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital Video Recorders	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cameras	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intercom Exchanges	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intercom Stations	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Analog Video Switchers	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CCTV Monitors	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intrusion Panels	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intrusion Areas	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Figure 78.** Facility Permissions — Devices tab

9. Select the **Devices** tab shown in [Figure 78](#). For each permission, such as Camera Permission, select the appropriate permission level. Permission is granted to all the actions preceding the selected option.
  - If **Create** is selected, an operator has permission to view and update the camera device records.
  - If **View** is selected, an operator can only view camera records and cannot modify or delete them.
10. Review each item and select the appropriate permissions. When you select one of these option buttons, permission is granted to all of the actions preceding the selected option button.

## System Permissions

Use System Permissions to grant or deny access to system applications, such as the Alarm Monitor or Event Monitor, or other items that are not assigned to facilities. Examples of items that are not in facilities include: alarm colors, alarm instructions, and alarm profiles.

### Using Pre-defined System Permissions

Facility Commander provides pre-defined System Permissions that can be modified, which include:

- **All System Permissions**  
Grants all permissions, including view, update, create, and delete for system level items. This also grants permission to use applications, such as the Alarm Monitor or permission to configure event action mapping definitions.
- **No System Permissions**  
Grants no permissions.

There are three pre-defined guard level permissions, which are:

- **Guard Supervisor System Permission**
- **Intermediate Guard Permissions**
- **Entry Level Guard Permissions**

The pre-defined permissions can be copied to create new permissions, but not deleted as they are permanent Facility Commander records.

➤ **To use one of the pre-defined facility permissions, follow these steps:**

1. Click the **Copy** icon next to the pre-defined system permission that you want to use and the Configure System Permissions page as shown in [Figure 80](#) displays.
2. Enter the information required to modify a facility permission record.
  - Change the tag name and description.
  - Review the tabbed pages and make the appropriate modifications.
3. Click **Submit** to save the record.

## Viewing System Permission

Use the System Permission page view, add, edit, copy, or delete system permission records. Refer to the following:

- [Using Pre-defined System Permissions.](#)
- [Adding System Permissions on page 110.](#)

► **To view system permissions, follow these steps:**

1. Select **Operator Administration**.
2. Select **System Permissions**. The System Permission page as shown in [Figure 80](#) displays.

**System Permissions**

**Instructions**  
View, edit, add or delete system permissions.

Search:  Go

Click to add a system permission profile. → [Add System Permission](#)

Page: 1 of 1 Go to:  Go Items per Page 15

	Tag Name	Description
	All System Permissions	Grants ALL system level permissions
	Entry Level Guard System Perms	Grants limited monitoring and command system level permissions for guards
	Guard Supervisor System Perms	Grants supervisory monitoring and command system level permissions for guards
	Intermediate Guard System Perms	Grants intermediate monitoring and command system level permissions for guards
	No System Permissions	Grants NO system level permissions

Click to copy a system permission profile. →

**Figure 79.** System Permissions

## Adding System Permissions

► To add or edit a system permission, follow these steps:

1. Select **Operator Administration**, and then **System Permissions**. The System Permissions page displays.
2. Click **Add System Permission**. The Configure System Permissions page as shown in [Figure 80](#) displays.

**Figure 80.** Configure System Permissions page

3. Enter the information described in [Table 44](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 44.** Configure System Permissions fields and description

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.

## Applications Tab

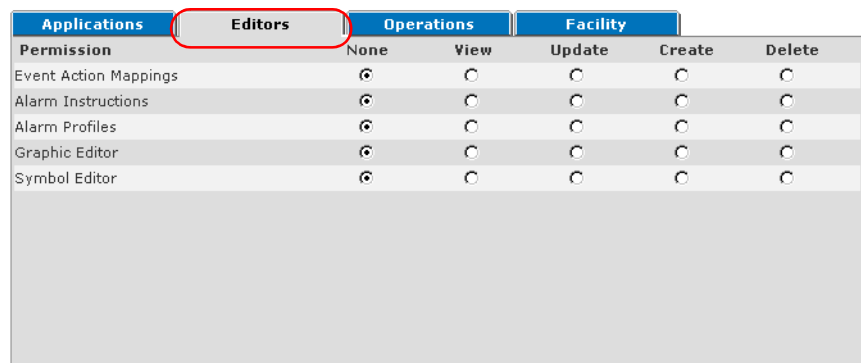


Permission	Enabled
Alarm Monitor	<input type="checkbox"/>
Event Monitor	<input type="checkbox"/>
Video Viewer	<input type="checkbox"/>
Graphic Viewer	<input type="checkbox"/>

**Figure 81.** Configure System Permissions page — Applications tab

5. Select the **Applications** tab shown in [Figure 81](#) to choose one or more check boxes granting permissions. A check mark indicates the permission is enabled.

## Editors Tab

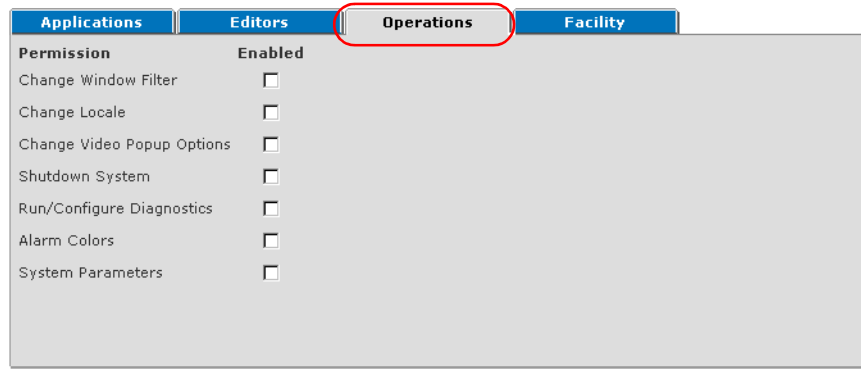


Permission	None	View	Update	Create	Delete
Event Action Mappings	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alarm Instructions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alarm Profiles	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Graphic Editor	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Symbol Editor	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Figure 82.** Configure System Permissions page — Editors tab

6. Select the **Editors** tab shown in [Figure 82](#). For each permission, such as the Event Action Mapping Permission, select the permission level. All permissions preceding the selected button are granted.
  - If **Create** is selected, an operator has permission to create, view and update Event Action Mappings.
  - If **View** is selected, an operator can only view the Event Action Mapping records, and cannot modify or delete them.
7. Review each permission and select the appropriate permission level.

## Operations Tab



Applications	Editors	Operations	Facility
<b>Permission</b>			
<b>Enabled</b>			
Change Window Filter			
<input type="checkbox"/>			
Change Locale			
<input type="checkbox"/>			
Change Video Popup Options			
<input type="checkbox"/>			
Shutdown System			
<input type="checkbox"/>			
Run/Configure Diagnostics			
<input type="checkbox"/>			
Alarm Colors			
<input type="checkbox"/>			
System Parameters			
<input type="checkbox"/>			

**Figure 83.** Configure System Permissions page — Operations tab

8. Select the **Operations** tab as shown in [Figure 83](#) to choose one or more check boxes granting permissions. A check mark indicates the permission is enabled.



## Contexts

Contexts are comprised of system permissions and facility permissions; and assigned to each operator.

Facility Commander provides pre-defined Contexts that can be modified to meet your organization's needs, which include:

- **System Administrator Context**  
Grants control over the entire system. It grants all permissions to all action, items, and facilities.
- **Regional Administrator Context**  
Grants control over a limited portion of the system. It grants all system level permissions to all actions and items, but not all facilities.

The Context definitions also include three guard-level permissions that range from supervisory monitoring and command capabilities to a more limited definition suitable for a beginner operator guard. These include:

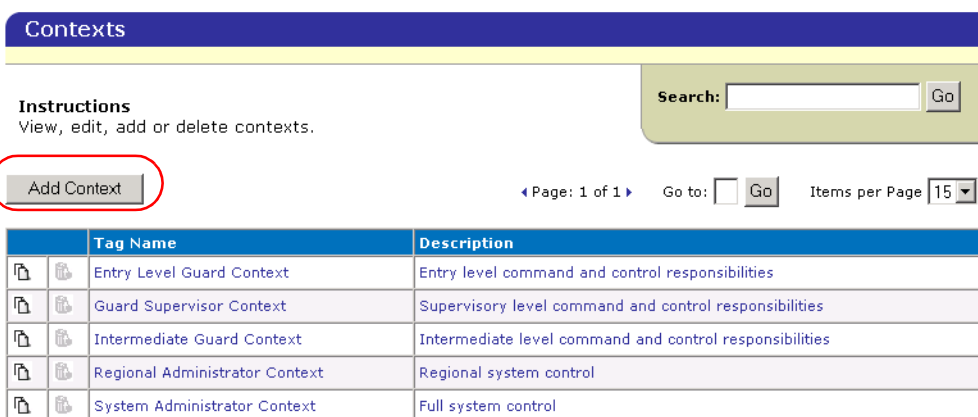
- **Guard Supervisor Context**
- **Intermediate Guard Context**
- **Entry Level Context**






## Viewing Context Definitions

Use the Context page to view, add, edit, copy, or delete context records.

► **To view the context definitions, follow these steps:**

1. Select **Operator Administration**
2. Select **Contexts**. The Contexts page as shown in [Figure 84](#) displays.

Click to add context → 

	Tag Name	Description
	Entry Level Guard Context	Entry level command and control responsibilities
	Guard Supervisor Context	Supervisory level command and control responsibilities
	Intermediate Guard Context	Intermediate level command and control responsibilities
	Regional Administrator Context	Regional system control
	System Administrator Context	Full system control

**Figure 84.** Contexts page

## Adding Context Definitions

► To add the context definitions, follow these steps:

1. Click **Add Context**. The Define Context page as shown in [Figure 85](#) displays.

**Figure 85.** Define Context page

2. Enter the information described in [Table 45](#) to define a new context definition. Continue to enter information on the tabbed pages.
3. Click **Submit** to save the record.

[Table 45 on page 114](#) lists and describes the elements on the Define Context page.

**Table 45.** Define Context fields and elements

Element	REQ	Description
Tag Name	✓	Enter a name to identify this record. Use 2-36 characters.
Description		Enter a description for this record. The description must be 1-100 characters.
System Profile	✓	Select the system permission definition.

**Table 45.** Define Context fields and elements (Continued)

Element	REQ	Description
<b>Global Facility</b>		<p>Use the Global Facility drop-down list to select the appropriate permission level for this context. It cannot be deleted.</p> <ul style="list-style-type: none"> <li>To grant full access to a system administrator, select <b>All Facility Permissions</b>. Other contexts should limit access to this facility.</li> <li>To grant partial access to a regional system administrator, select <b>No Facility Permissions</b> at the Global Facility and select <b>All Facility Permissions</b> at the Regional Facility.</li> </ul>
<b>Unassigned Items Facility</b>		<p>This facility contains all newly created, facility-based items. When the new facility is assigned to its correct facility, it is automatically removed from the Unassigned Items Facility.</p>

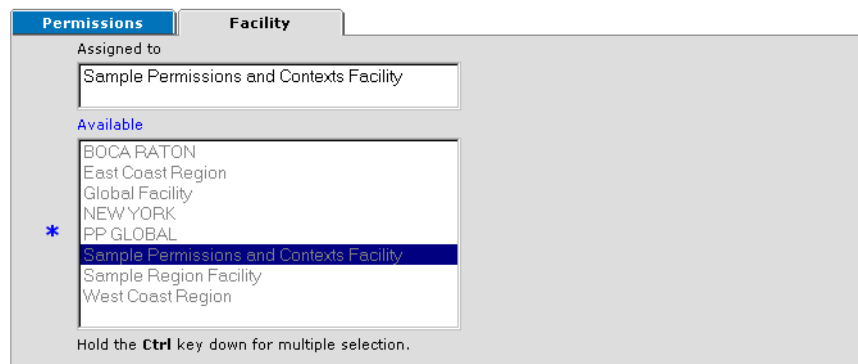
## Permissions Tab

Facilities	Facility Permissions
Global Facility	
East Coast Region	
NEW YORK	
Sample Permissions and Contexts Facility	
Sample Region Facility	Entry Level Guard Facility Perms
Unassigned Items Facility	
West Coast Region	

**Figure 86.** Define Context — Permissions tab

- Select the **Permission** tab shown in [Figure 86](#) to choose one or more permissions to associate with this context definition. Refer to [Adding Facility Permissions on page 104](#) for more information. Continue to enter information on the next tabbed page.

## Facility Tab



The screenshot shows a web interface with two tabs: 'Permissions' and 'Facility'. The 'Facility' tab is active. Under the 'Assigned to' label, a text box contains 'Sample Permissions and Contexts Facility'. Below this, under the 'Available' label, is a list box containing the following items: BOCA RATON, East Coast Region, Global Facility, NEW YORK, PP GLOBAL, Sample Permissions and Contexts Facility (highlighted in blue), Sample Region Facility, and West Coast Region. A blue asterisk is positioned to the left of the 'Available' header. At the bottom of the interface, a note states: 'Hold the **Ctrl** key down for multiple selection.'

**Figure 87.** Define Context — Facility tab

5. Select the **Facility** tab as shown in [Figure 87](#) and enter the information described in [Table 46](#).

**Table 46.** Define Context fields and descriptions

Field Name	REQ	Description
Assigned to		Displays the facility or facilities for this context definition. Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Pre-defined Contexts

Facility Commander provides five pre-defined contexts. [Table 47](#) shows the Facility Permissions and System Permissions associated with each context.

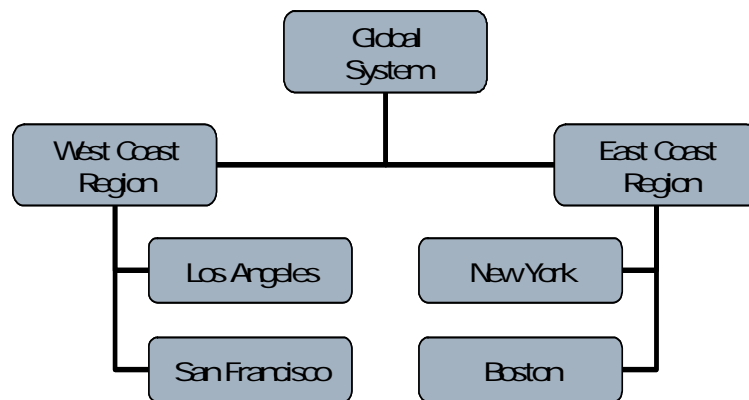
**Table 47.** Pre-defined Contexts

Contexts	System Permissions	Facility Permissions
<b>System Administrator</b>	All System Permissions	All Facility Permissions for Global Facility
	Other Pre-defined System Permissions	Other Pre-defined Facility Permissions
	No System Permissions	No Facility Permissions
		View Configuration Facility Permissions
		Update Configuration Facility Permissions
<b>Regional Administrator</b>	All System Permissions	All Facility Permissions for Sample Region Facility, Sample Permissions and Context.
<b>Guard Supervisor</b>	Guard Supervisor System Permissions	Guard Supervisor Facility Permissions
<b>Intermediate Guard</b>	Intermediate Guard System Permissions	Guard Supervisor Facility Permissions
<b>Entry Level Guard</b>	Entry Level Guard System Permissions	Entry Level Guard Facility Permissions

## Examples

Facility Commander provides the flexibility to build relationships by creating parent facilities and sub-facilities. *Each facility can be a member of one other facility. An item can belong to more than one facility.*

In the illustration in [Figure 88](#), facilities in different geographic locations are used to show the relationship between facilities. These facilities will be used later to build contexts.



**Figure 88.** Two regional facilities and four imported facilities.

The imported Picture Perfect facilities are:

- Los Angeles representing a corporate office
- San Francisco representing a sales office
- New York representing a corporate office
- Boston representing a data center

To further organize the facilities, two additional facilities are created — West Coast Region and East Coast Region. These regional facilities are used to group the individual area facilities, which includes New York, Boston, Los Angeles, and San Francisco. By creating the regional levels, a hierarchy is established. Permissions do not have to be explicitly defined at the individual area level, but rather can be inherited from their regional facility.

By granting access to the each regional administrator, the administrator has access to everything below in the hierarchy. The permissions are inherited from the facility above, unless explicitly specified.

In this example:

- The system administrator is assigned the System Administrator Context and therefore given full access to all items in the system.

- A regional system administrator is assigned the Regional Administrator Context and therefore given access to items in their regional facility. This administrator would not have access to items in another regional facility, unless permission is specifically granted.
- Operators assigned to a lower level facility, such as New York, might be granted permissions to view and control the items associated with the New York facility, but not others.

To accomplish this, the context definitions would look like this:

<b>System Administrator</b>	
Context	System Administrator
System Permissions	All System Permissions
Facility Permissions	All Facility Permissions for Global Facility

<b>East Coast Regional Administrator</b>	
Context	East Coast Regional Administrator
System Permissions	All System Permissions
Facility Permissions	All Facility Permissions for East Coast Facility

Because the East Coast Facility is the parent facility of New York and Boston, the regional administrator will automatically be given full access to New York and Boston items.

<b>West Coast Regional Administrator</b>	
Context	West Coast Regional Administrator
System Permissions	All System Permissions
Facility Permissions	All Facility Permissions for West Coast Facility

Because the West Coast Facility is the parent facility of Los Angeles and San Francisco, the regional administrator will automatically be given full access to Los Angeles and San Francisco items.





## Chapter 6. Configuring Video Devices

This chapter describes how to configure video devices, cameras, and camera preset positions, CCTV monitors, and switchers. Troubleshooting steps are provided for extra assistance, if there is any difficulty.

Readers should use the vendor's documentation for instructions on how to use their products. For information about device drivers refer to the vendor's Release Notes.



---

### **In this chapter:**

[Overview on page 122](#)

[Configuring Digital Video Recorders on page 124](#)

[Configuring Cameras on page 132](#)

[Configuring Cameras on page 132](#)

[Configuring IP Cameras on page 137](#)

[Configuring Camera Preset Positions on page 138](#)

[Linking Cameras to DVRs on page 141](#)

[Configuring Analog Video Switchers on page 143](#)

[Configuring CCTV Monitors on page 150](#)

[Associating Analog Video Switcher Devices on page 153](#)

## Overview

The digital video features in Facility Commander allow operators to view live and recorded video; select and control different cameras; direct cameras to a preset position; and mark a video clip to playback later.

Refer to the following checklist for the configuration order to add media devices to Facility Commander:

- 
- ✓ Configure the Digital Video Recorders (DVRs). Refer to [Configuring Digital Video Recorders on page 124](#).
  - ✓ Configure the cameras. Refer to [Configuring Cameras on page 132](#) for more information.
  - ✓ Identify the preset camera positions. Refer to [Configuring Camera Preset Positions on page 138](#) for more information.
  - ✓ Link the cameras to the Digital Video Recorders (DVRs). Refer to [Linking Cameras to DVRs on page 141](#) for more information.
  - ✓ Assign the equipment to the appropriate facility. Refer to [Facilities on page 67](#) for more information.
-

## Define digital video recorders

Facility Commander supports the following digital video multiplexer/ recorders:

**Table 48.** Supported Video Devices

Provider	Model Description	Version
GE	GE DVMRe - 4 CD GE DVMRe - 10 CD GE DVMRe - 16 CD	Requires duplex PPC firmware Version 3.18 or later and MUX firmware Version 3.24 or later.
	GE DVMRe CT / StoreSafe Pro - 4 GE DVMRe CT / StoreSafe Pro - 10 GE DVMRe CT / StoreSafe Pro - 16	Requires triplex firmware Version 5.x or later. CT, StoreSafe, and StoreSafe Pro series recorders are part of the family of wavejet compression-based technology products.
	GE DVMRe CT II / StoreSafe Pro II - 4 GE DVMRe CT II / StoreSafe Pro II - 10 GE DVMRe CT II / StoreSafe Pro II - 16	CT II and StoreSafe Pro II series recorders are part of the family of wavejet compression-based technology products.
	GE Discovery 300 GE Discovery 2400	VOS Version 3.x These recorders are part of the family of VisioWave video products.
	GE Discovery 105E GE Discovery 1205 GE Discovery 2405 GE Discovery 2415 GE Evolution 2800 GE Evolution 2809 GE Evolution 3005 GE ECVRS	VOS Version 4.x These recorders are part of the family of VisioWave video products.
	SymDec 16 SymSafe SymSafe Pro SymNet 1 Legend IP	1.47k 1.28i 1.28i 2.00i 3.6 These recorders are part of the family of SymSuite video products.
Integral Technologies	DVXi DVXe DS Xpress	3.1 4.0, 4.1 2.1
American Dynamics	Intellex DVMS8000	3.1
Nice	Pro Harmony	8.0
Digital Watchdog	DWPro 9016	2.3
Pelco	DX8000	1.0
Panasonic	HD500A	2.5

**Note:** Increasing the processor speed and memory on the server and/or client workstations may be required for optimizing performance in your specific application.

## Video Devices

The video equipment and supporting software applications must be installed according to the manufacturer's directions. The Facility Commander supports GE Security and other vendor products including NTSC and PAL video formats. Refer to the product documentation provided by the manufacturer for instructions to install and use their products.

You can add an unlimited number of DVRs, which allows you to add more DVRs and cameras as your business needs grow. The number of cameras you can use will depend on the DVR type and model used in your environment.

All the cameras in Facility Commander must be licensed; the number of licenses is determined by the number of cameras in the whole deployment and not per DVR device.

## Configuring Digital Video Recorders

A Digital Video Recorder (DVR) is a device which is capable of recording video from multiple cameras simultaneously and storing it on the DVR's internal hard disk. The DVR provides access to stored video and live camera images using a standard ethernet connection.

Digital recording can improve playback quality over time-lapse VCRs and eliminates the need to change tapes.

Refer to the following sections:

- [Adding DVRs on page 126](#)
- [Linking Cameras to DVRs on page 141](#)

## Viewing DVRs

Use the Digital Video Recorders page to view, add, edit, copy, or delete DVR records.

► **To view DVRs, follow these steps:**

1. Select **Device Management**.
2. Select **Digital Video Recorders**. The Digital Video Recorders page as shown in [Figure 89](#) displays.



**Digital Video Recorders**

**Instructions**  
View, edit, add or delete digital video recorders.

Search:  Go

Add DVR

◀ Page 1 of 1 ▶ Go to  Go Items per Page 10 ▼

	Tag Name	Description	Reference ID	IP Address or Hostname	Online	Link Cameras
 	NY B1 DVR			3.18.148.51	Yes	<a href="#">Link Cameras</a>

Use to link camera with DVR

**Figure 89.** Digital Video Recorders page

## Adding DVRs

► To add a DVR device, follow these steps:

1. Select **Device Management**, and then **Digital Video Recorders**. The Digital Video Recorders page displays.
2. Click **Add DVR** and the Configure Digital Video Recorder page as shown in [Figure 90](#) displays.

**Configure Digital Video Recorder**

**Instructions**  
View or edit the digital video recorder.

**Digital Video Recorder Information**

**Tag Name**

\*

Description

Reference ID

**Model** | **Addresses** | **Advanced** | **Alarms** | **Facility**

☒ Online

**Model**

\*

**Number of Inputs**

\*

**Time Zone**

\*

**Facility Commander Server**

\*

**Archive Device**

**Video Clip Search Timeout (seconds)**

\*

**Figure 90.** Configure Digital Video Recorder page

3. Enter the information described in [Table 49](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 49.** Configure DVR fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## Model Tab

The screenshot shows the 'Model' tab of a configuration window. The 'Model' tab is highlighted with a red circle. The configuration fields are as follows:

- Online:** A checked checkbox.
- Model:** A dropdown menu showing 'Kalatel DVMRe-16CT'.
- Number of Inputs:** A text input field containing '16'.
- Time Zone:** A dropdown menu showing '(GMT-05:00) America/New\_York (EST)'.
- Facility Commander Server:** A dropdown menu showing 'Media Server'.
- Archive Device:** An empty dropdown menu.
- Video Clip Search Timeout (seconds):** A text input field containing '30'.

**Figure 91.** Configure DVR — Model tab

5. Select the **Model** tab shown in [Figure 91](#) and enter the information described in [Table 50](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 50.** Configure DVR fields and descriptions

Field Name	REQ	Description
Online		Default setting is online. A check mark indicates the DVR is online. Clear the check box to take the DVR offline. The DVR must be offline to use another application, such as WaveReader.
Model	✓	Use the drop-down list to select the DVR model name.
Number of Inputs	✓	Enter the number of available inputs on the DVR. This number is different depending on the DVR model. For all Sym devices, this number must be 20. Configure the first IP camera on Input 17.
Time Zone	✓	Use the drop-down list to select the time zone where this device is located. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.
Facility Commander Server	✓	Use the drop-down list to select the Media server that controls communication with this DVR.
Archive Device		When configuring an IP camera, use the drop-down list to select the device to which this camera sends archived video.
Video Clip Search Timeout (seconds)	✓	Enter the number of seconds to poll the DVR to find a video clip to play.

## Addresses Tab

**Figure 92.** Configure DVR — Addresses tab

6. Select the **Addresses** tab shown in [Figure 92](#) and enter the information described in [Table 51](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 51.** DVR fields and descriptions

Field Name	REQ	Description
<b>IP Address or Host Name</b>	✓	Enter the DVR IP address or host name. The host name is case-sensitive.
<b>Port</b>	✓	Enter the port number.  <b>Note:</b> If the Media server is installed on a Windows operating system and the firewall is ON, all ports that are configured in the Digital Video Recorders page, Addresses tab, need to be added to the firewall exceptions list.
<b>RS-485 Address</b>		Enter the RS-485 address. For IP cameras, enter 1 for the RS-485 address. This is configured on the DVR and used for PTZ addressing.
<b>Auxiliary Address</b>		If you are using a converter, enter the address.
<b>Auxiliary Port</b>		If you are using a converter, enter the port number.



## Advanced Tab

The screenshot shows the 'Advanced' tab of the 'Configure DVR' interface. The tab is highlighted with a red box. The form contains the following fields:

- User Name:
- Password:
- Confirm Password:
- Status Polling Interval (seconds):  (marked with a blue asterisk)
- Command Retry Interval (seconds):  (marked with a blue asterisk)

**Figure 93.** Configure DVR — Advanced tab

7. Select the **Advanced** tab shown in [Figure 93](#) and enter the information described in [Table 52](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 52.** DVR fields and descriptions

Field Name	REQ	Description
User Name		Enter a valid user name.
Password		Enter the password to access the DVR. This password is set on the DVR.
Confirm Password		Enter the password again for confirmation.
Status Polling Interval (seconds)	✓	Enter the number of seconds to wait before Facility Commander polls the DVR device. The default value is five seconds.
Command Retry Interval (seconds)	✓	Enter the number of seconds to wait before trying to reconnect to the Facility Commander server. The default value is 15 seconds.

## Alarms Tab

The screenshot shows the 'Alarms' tab selected in a configuration window. The tab is highlighted with a red border. Below the tab, there are four drop-down menus, each with a label and a downward arrow icon. The labels are: 'DVR Communications Alarm', 'DVR Health Fail Alarm', 'DVR Health Trouble Alarm', and 'Disk Full Alarm'.

**Figure 94.** Configure DVR — Alarms tab

8. Select the **Alarms** tab shown in [Figure 94](#) and enter the information described in [Table 53](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 53.** DVR fields and descriptions

Field Name	REQ	Description
<b>DVR Communications Alarm</b>		Use the drop-down list to select the alarm that will trigger when the system is unable to communicate with the DVR.
<b>DVR Health Fail Alarm</b>		Use the drop-down list to select the DVR Health Fail alarm for this DVR.
<b>DVR Health Trouble Alarm</b>		Use the drop-down list to select the DVR Health Trouble alarm for this DVR.
<b>Disk Full Alarm</b>		Use the drop-down list to select the Disk Full alarm for this DVR.

## Facility Tab

**Figure 95.** Configure DVR — Facility tab

9. Select the **Facility** tab shown in [Figure 95](#) and enter the information described in [Table 54](#). A check mark indicates a required field.

**Table 54.** Configure DVR fields and descriptions

Field Name	REQ	Description
<b>Assigned to</b>		Displays the facility or facilities for this device. Items can belong to more than one facility. This is a read-only field and cannot be edited.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

10. Click **Submit** to save the record. After you add the DVR to the system, you must define the cameras, and return to the DVR page to link the cameras to the DVR.

## Configuring Cameras

Facility Commander supports multiple camera equipment vendors including their devices with pan/tilt/zoom features and preset camera positions.

Refer to the following sections:

- [Adding Cameras on page 133](#)
- [Configuring IP Cameras on page 137](#)
- [Viewing Camera Preset Positions on page 138](#)
- [Adding Camera Preset Positions on page 139](#)
- [Linking Cameras to DVRs on page 141](#)

## Viewing Cameras

Use the Cameras page to view, add, edit, copy, or delete camera records.

► **To view camera records, follow these steps:**

1. Select **Device Management**.
2. Select **Cameras**. The Cameras page as shown in [Figure 96](#) displays.

	Tag Name	Description	Reference ID	DVR	Presets
	NY Cam 100			NY B1 DVR	<a href="#">Presets</a>
	NY Cam 200			NY B1 DVR	<a href="#">Presets</a>
	NY Cam 210			NY B1 DVR	<a href="#">Presets</a>
	NY Cam 300			NY B1 DVR	<a href="#">Presets</a>

**Figure 96.** Cameras page

## Adding Cameras

► To add a camera device, follow these steps:

1. Select **Device Management**, and then **Cameras**. The Cameras page displays.
2. Click **Add Camera**. The Configure Camera page as shown in [Figure 97](#) displays.

**Figure 97.** Configure Camera page

3. Enter the information described in [Table 55](#). A check mark indicates a required field. Continue to add information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 55.** Configure Camera fields and description

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

The screenshot shows a web interface for configuring a camera. At the top, there are three tabs: 'General', 'Alarms', and 'Facility'. The 'General' tab is selected and highlighted with a red circle. Below the tabs, there are four configuration fields:

- Linked to DVR:** A text input field containing 'NY B1 DVR'.
- DVR Camera Input:** A text input field containing '1'.
- PTZ Controller:** A drop-down menu with 'NY B1 DVR' selected.
- Bus Address:** A text input field containing '1'.

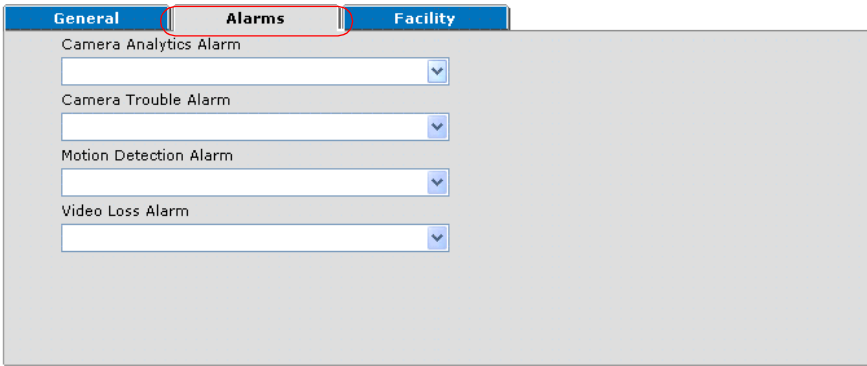
**Figure 98.** Configure Camera — General tab

5. Select the **General** tab shown in [Figure 98](#) and enter the information described in [Table 56](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 56.** Configure Camera fields and descriptions — General tab

Field Name	REQ	Description
<b>Linked to DVR</b>		Identifies the DVR where this camera is linked. Refer to <a href="#">Linking Cameras to DVRs on page 141</a> for more information.
<b>DVR Camera Input</b>		Identifies the DVR input associated with this camera.
<b>PTZ Controller</b>		Use the drop-down list to select the DVR that controls the PTZ device.
<b>Bus Address</b>		Enter the value for the bus address.

## Alarms Tab



The screenshot shows the 'Alarms' tab selected in a configuration window. The tab is highlighted with a red border. Below the tab, there are four dropdown menus, each with a label and a downward arrow icon. The labels are: 'Camera Analytics Alarm', 'Camera Trouble Alarm', 'Motion Detection Alarm', and 'Video Loss Alarm'. The dropdown menus are currently empty, showing only the arrow icon.

**Figure 99.** Configure Camera — Alarms tab

6. Select the **Alarms** tab shown in [Figure 99](#) and enter the information described in [Table 57](#). A check mark indicates a required field.

**Table 57.** Configure Camera fields and descriptions

Field Name	REQ	Description
Camera Analytics Alarm		Select the Camera Analytics alarm for this camera.
Camera Trouble Alarm		Select the Camera Trouble alarm for this camera.
Motion Detection Alarm		Select the Motion Detection alarm for this camera.
Video Loss Alarm		Select the Video Loss alarm for this camera.

## Facility Tab

**Figure 100.** Configure Camera — Facility tab

7. Select the Facilities tab as shown in [Figure 100](#) and enter the information described in [Table 58](#). A check mark indicates a required field.

**Table 58.** Configure Camera fields and descriptions

Field Name	REQ	Description
Assigned to		Displays the name of facility or facilities where this items is currently assigned. Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>



## Configuring IP Cameras

IP cameras differ from analog cameras in that they are associated to hardware by IP address and are not directly connected to a DVR. To configure an IP camera, the DVR must be able to identify the IP address of the IP camera and vice versa.

**Note:** For VisioWave devices, refer to the *"Facility Commander 2.2 with VisioWave Setup Guide."*

► **To add an IP camera, follow these steps:**

1. If you have not already added a DVR, select **Device Management**, and then **Digital Video Recorders**. The Digital Video Recorders page displays. Refer to [Configuring Digital Video Recorders on page 124](#) to add a DVR.
2. Select **Device Management**, and then **Cameras**. The Cameras page displays. Refer to [Configuring Cameras on page 132](#) to add an IP camera.
3. Select **Device Management**, and then **Digital Video Recorders**. The Digital Video Recorders page displays. Find the DVR you want to link this IP camera to, and then select Link Camera. Refer to [Linking Cameras to DVRs on page 141](#) to link the IP camera to this DVR.

► **To associate a DVR to an IP camera, follow these steps:**

1. After you have added a DVR and an IP camera, right-click on that DVR in the navigation pane and select **Browse**. This will take you to the manufacturer's configuration website for this DVR. The login information will differ depending on the manufacturer.
2. Navigate to the page where you will identify the IP camera for this DVR. For Sym devices, this can be configured on the Camera page.
3. Enter the IP address of the IP camera in the Source Address field, and then click Save.

► **To associate an IP camera to a DVR, follow these steps:**

1. In the navigation pane, right-click on the IP camera you want to configure, and then select **Browse**. This will take you to the manufacturer's configuration website for this camera. The login information will differ depending on the manufacturer.
2. Navigate to the page where you will identify the archive device for this IP camera. Streaming video from this IP camera will be sent to the archive device. The name of this page will differ depending on the manufacturer. For Legend IP Dome cameras, this can be configured on the Configure page under Encoder streaming settings.
3. In the Streaming Address field, enter the IP address of the archive device you selected, and then click Save. Refer to the [Model Tab on page 127](#) to identify the archive device.

## Configuring Camera Preset Positions

When a camera has PTZ capabilities, the camera presets are first configured using the digital video vendor's equipment. These preset positions are then defined in Facility Commander, so that an operator can control the camera's location.

### Viewing Camera Preset Positions

Use the Camera Preset page to view, add, edit, copy, or delete camera preset records.

► **To view the camera presets, follow these steps:**

1. Select **Device Management**.
2. Select **Cameras**. The Cameras page displays.
3. Select a camera in the list and click **Presets**, which is a link to Camera Preset list page. The Camera Presets page as shown in [Figure 101](#) displays.

**Camera Presets**

**Instructions**  
View, edit, add or delete camera presets.

Search:

◀ Page 1 of 1 ▶ Go to   Items per Page 10 ▼

	Tag Name	Description	Camera ID	Preset Number
	NY Cam 100 PS 01		NY Cam 100	1
	NY Cam 100 PS 02		NY Cam 100	2
	NY Cam 100 PS 03		NY Cam 100	3
	NY Cam 100 PS 04		NY Cam 100	4

**Figure 101.** Camera Presets page

## Adding Camera Preset Positions

- To configure the camera's preset positions, follow these steps:
1. Select **Device Management**, and then **Cameras**.
  2. Select a camera from the list to view the Configure Camera page.
  3. Select a PTZ Controller and Bus Address, if not already selected. Click Submit to return to the Cameras page. You will now see a selection for Presets in the Presets column for that camera.
  4. Click **Presets**, which is a link to Camera Preset list page. This displays only the presets for the selected camera.
  5. Select **Camera Presets**. The Configure Camera Preset list page as shown in [Figure 101](#) displays.
  6. Select **Add Preset**. The Configure Camera Preset configuration page as shown in [Figure 102](#) displays.

**Configure Camera Preset**

**Instructions**  
View or edit the camera preset.

**Preset Information**

Tag Name  
\* NY Cam 100 PS 01  
Description

**General**

Camera ID  
NY Cam 100  
Preset Number  
\* 1

**Figure 102.** Configure Camera Preset page

7. Enter the information described in [Table 59](#) to identify the camera preset positions.
8. Click **Submit** to save the record.

[Table 59](#) lists and describes the fields on the Configure Camera Preset page.

**Table 59.** Configure Camera Preset fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.

**Table 59.** Configure Camera Preset fields and descriptions

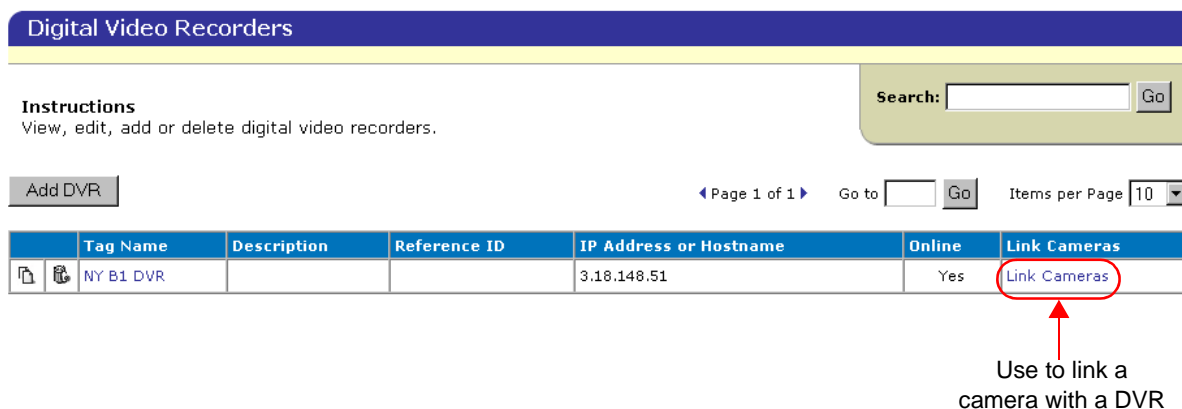
Field Name	REQ	Description
Camera ID		Use the Camera ID drop-down list to select the camera. Refer to <a href="#">Configuring Cameras on page 132</a> for more information about adding a camera.
Preset Number	✓	Enter the number assigned to the preset position.

## Linking Cameras to DVRs

The Link Cameras page is used to link the cameras with DVRs. The number of cameras is determined by the number of inputs, usually 32, and is configured using the Configure Digital Video Recorder page.

► **To link the cameras to the DVR device, follow these steps:**

1. Select **Device Management**.
2. Select **Digital Video Recorders**. The Digital Video Recorders page as shown in [Figure 103](#) displays.



**Figure 103.** Digital Video Recorders page

3. Click **Link Cameras**. The Link Cameras page in [Figure 104](#) on [page 142](#) displays.

**Link Cameras**

**Instructions**  
Link Cameras to DVR. Select the camera that is connected to each input of the DVR.

DVR Camera Input	Linked Camera
Input 1	NY Cam 100
Input 2	NY Cam 200
Input 3	NY Cam 210
Input 4	NY Cam 300
Input 5	
Input 6	
Input 7	
Input 8	
Input 9	
Input 10	
Input 11	
Input 12	
Input 13	
Input 14	
Input 15	

**Figure 104.** Link Cameras page

4. Use the drop-down lists to select the cameras associated with this DVR. If you are linking an IP camera with a SymDec device, you must select Input 17 as the first IP camera input.
5. Click **Submit** when you are finished associating the cameras with DVR device.

## Configuring Analog Video Switchers

The Analog Video Switchers page is used to add a new analog video switcher record, upload a configuration file, and identify the inputs and outputs.

**Note:** Refer to the Installation Manual for specific cabling instructions.

### Viewing Analog Video Switchers

► To view the analog video switcher records, follow these steps:


1. Select **Device Management**.
2. Select **Analog Video Switchers**. The Analog Video Switchers page as shown in [Figure 105](#) displays.

**Analog Video Switchers**

**Instructions**  
View, edit, add or delete analog video switchers.

Search:

◀ Page 1 of 1 ▶ Go to   Items per Page 50 ▼

	Tag Name	Description	Reference ID	Model	IP Address or Host Name	Inputs and Outputs
	Kalatel Switcher KTD-348			Kalatel KTD-348	3.137.171.33	<a href="#">Inputs and Outputs</a>

Inputs and Outputs

**Figure 105.** Analog Video Switchers page

## Adding an Analog Video Switcher

- To add an analog video switcher, follow these steps:
1. Select **Device Management**, and then **Analog Switchers**.
  2. Click **Add Analog Switcher**. The Configure Analog Switcher page as shown in [Figure 106](#) displays.

**Configure Analog Video Switcher**

**Instructions**  
View or edit the analog video switcher.

**Analog Video Switcher Information**

[Tag Name](#)

\*

Description

Reference ID

**Model** | **Addresses** | **Advanced** | **Alarms** | **Facility**

[Model](#)

\*

[Facility Commander Server](#)

\*

[Time Zone](#)

\*

**Figure 106.** Configure Analog Video Switcher page

3. Enter the information described in [Table 60](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 60.** Configure Analog Video Switcher fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate an item to a blue print or wiring diagram. Use 1-20 characters.



Model Tab

The screenshot shows a configuration window with four tabs: Model, Addresses, Advanced, and Facility. The Model tab is active and highlighted with a red circle. Below the tabs, there are three required fields, each marked with a blue asterisk (\*):

- Model:** A drop-down menu showing "Kalatel KTD-348".
- Facility Commander Server:** A drop-down menu showing "Facility Commander Server".
- Time Zone:** A drop-down menu showing "(GMT-05:00) EST (EST)".

Figure 107. Configure Analog Video Switcher — Model tab

5. Select the **Model** tab shown in Figure 107 and enter the information described in Table 61. A check mark indicates a required field. Continue to enter information on the tabbed pages

Table 61. Configure Analog Video Switcher fields and descriptions

Field Name	REQ	Description
Model	✓	Use the drop-down list to select the correct model name.
Facility Commander Server	✓	Use the drop-down list to select the Facility Commander server that controls communication with this analog video switcher.
Time Zone	✓	Use the drop-down list to select the time zone for this analog switcher. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.

## Addresses Tab

The screenshot shows a configuration window with five tabs: Model, Addresses, Advanced, Alarms, and Facility. The 'Addresses' tab is selected and highlighted with a red circle. Below the tabs, there are two input fields. The first field is labeled 'IP Address or Host Name' and has an asterisk (\*) to its left, indicating it is a required field. The second field is labeled 'Port' and also has an asterisk (\*) to its left, indicating it is a required field. Both fields are currently empty.

**Figure 108.** Configure Analog Video Switcher — Addresses tab

6. Select the **Addresses** tab shown in [Figure 108](#) and enter the information described in [Table 62](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 62.** Configure Analog Video Switcher fields and descriptions

Field Name	REQ	Description
IP Address or Host Name	✓	Enter the host name or IP address of the analog video switcher. The host name is case-sensitive.
Port	✓	Identify the TCP/IP port on which the analog video switcher communicates with Facility Commander.

### Advanced Tab

The screenshot shows a configuration window with five tabs: Model, Addresses, Advanced, Alarms, and Facility. The 'Advanced' tab is selected and highlighted with a red circle. Below the tabs, there are two input fields. The first field is labeled 'Status Polling Interval (seconds)' and contains the value '60'. The second field is labeled 'Command Retry Interval (seconds)' and contains the value '30'. Both fields have an asterisk (\*) next to them, indicating they are required fields.

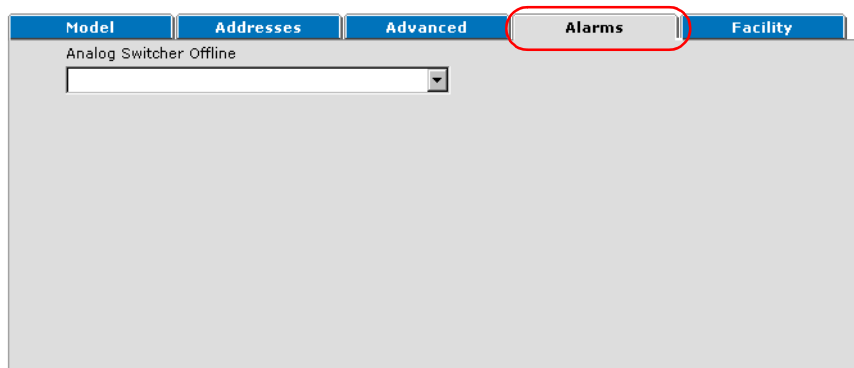
**Figure 109.** Configure Analog Video Switcher — Advanced tab

7. Select the **Advanced** tab shown in [Figure 109](#) and enter the information described in [Table 63](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 63.** Configure Analog Video Switcher fields and descriptions

Field Name	REQ	Description
Status Polling Interval (seconds)	✓	Enter the number of seconds to wait before Facility Commander polls the analog video switcher device. The default value is 60 seconds.
Command Retry Interval (seconds)	✓	Enter the number of seconds to wait before trying to reconnect to the Facility Commander server. The default value is 30 seconds.

## Alarms Tab



The screenshot shows a web-based configuration interface with five tabs: Model, Addresses, Advanced, Alarms, and Facility. The 'Alarms' tab is selected and highlighted with a red rectangular box. Below the tabs, the 'Analog Switcher Offline' section contains a dropdown menu with a downward arrow on the right side.

**Figure 110.** Configure Analog Video Switcher — Alarms tab

8. Select the **Alarms** tab shown in [Figure 109](#) and enter the information described in [Table 64](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 64.** Configure Analog Video Switcher fields and descriptions

Field Name	REQ	Description
Analog Switcher Offline		Use the drop-down list to select the appropriate alarm indicating when the analog switcher is offline.

## Facility Tab

The screenshot shows a configuration window with four tabs: 'Model', 'Addresses', 'Advanced', and 'Facility'. The 'Facility' tab is selected and highlighted with a red rectangle. Below the tabs, there are two main sections. The first section, labeled 'Assigned to', contains a text box with the value 'NEW YORK'. The second section, labeled 'Available', contains a list box with the following items: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEW YORK' (which is highlighted in blue), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. A small blue asterisk is visible to the left of the 'PP GLOBAL' item.

**Figure 111.** Configure Analog Video Switcher — Facility tab

9. Select the Facility tab shown in [Figure 111](#) and enter the information described in [Figure 65](#). A check mark indicates a required field.

**Table 65.** Configure Analog Video Switcher fields and descriptions

Field Name	REQ	Description
Assigned To		Displays the name of the facility where this graphic display is currently assigned. Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"><li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li><li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li><li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key, and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li></ul>

## Configuring CCTV Monitors

CCTV Monitors are used to display video from cameras connected to analog switchers. Use the CCTV Monitors page to view, add, edit, copy, or delete CCTV Monitor records.

Refer to the following sections:

- [Viewing CCTV Monitors](#)
- [Adding CCTV Monitors on page 151](#)

### Viewing CCTV Monitors

► **To view CCTV monitors, follow these steps:**

1. Select **Device Management**.
2. Select **CCTV Monitors**. The CCTV Monitors page as shown in [Figure 112](#) displays.

**CCTV Monitors**

**Instructions**  
View, edit, add or delete CCTV monitors.

Search:

◀ Page 1 of 1 ▶ Go to   Items per Page

	Tag Name	Description	Reference ID
	Lobby 100 Monitor	NY	
	Lot 400 Monitor	NY East Parking Lot	
	West Lobby 200 Monitor	NY West Lobby	

**Figure 112.** CCTV Monitors page

## Adding CCTV Monitors

► To configure CCTV monitors, follow these steps:

1. Select **Device Management** and then select **CCTV Monitors**. The CCTV Monitors page displays.
2. Click **Add CCTV Monitor** and the Configure CCTV Monitor page as shown in [Figure 113](#) displays.

**Figure 113.** Configure CCTV Monitor page

3. Enter the information described in [Table 66](#). A check mark indicates a required field.
4. Click **Submit** to save the record.

**Table 66.** Configure CCTV Monitor fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate an item to a blue print or wiring diagram. Use 1-20 characters.

**Table 66.** Configure CCTV Monitor fields and descriptions (Continued)

Field Name	REQ	Description
<b>Facility</b>		
<b>Assigned To</b>		Displays the name of facility or facilities where this item is currently assigned. Items can belong to more than one facility. This is a read-only field.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <p>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>



## Associating Analog Video Switcher Devices

Use the Analog Video Switcher Inputs and Outputs page to associate the analog video switcher with cameras and monitors. The information can be added manually or by loading a configuration file.

Kalatel provides a utility program to generate an XML file, which contains camera and monitor records.

If the number of inputs or outputs on the screen does not match your device you have to manually edit the switcher definition file. The definition files can be found in the Resources folder. The naming format is <brand>SwitcherCommands.xml.

► **For instructions on how to import this file, follow these steps:**

1. Select **Device Management**.
2. Select **Analog Video Switchers**. The Analog Switchers page shown in [Figure 105](#) displays.
3. Click the appropriate **Inputs & Outputs** link on the list page. The Analog Switcher Inputs and Outputs page shown in [Figure 114](#) displays.

**Analog Switcher Inputs and Outputs**

**Instructions**  
View or edit analog switcher inputs and outputs. Select the camera or CCTV monitor that is connected to each port of the switcher.

[Import Configuration File](#)

**Inputs:** ◀ Page 1 of 1 ▶ Go to  Go

Port	Camera Alias	Camera Title	Camera
0	<input type="text"/>	<input type="text"/>	camera_01_01
1	<input type="text"/>	<input type="text"/>	camera_01_02
2	<input type="text"/>	<input type="text"/>	camera_01_03
3	<input type="text"/>	<input type="text"/>	camera_01_04
4	<input type="text"/>	<input type="text"/>	
5	<input type="text"/>	<input type="text"/>	
6	<input type="text"/>	<input type="text"/>	

**Outputs:** ◀ Page 1 of 1 ▶ Go to  Go

Port	Monitor Alias	Monitor
0	<input type="text"/>	Monitor 1
1	<input type="text"/>	Monitor 2
2	<input type="text"/>	
3	<input type="text"/>	

[Submit](#) [Cancel](#)

**Figure 114.** Analog Video Switcher Inputs and Outputs page

4. Click **Import Configuration File**. The Inputs and Outputs File Import page shown in [Figure 115](#) displays.

**Inputs and Outputs File Import**

**Instructions**  
Select a file to import.

**Configuration File**

☒ Create cameras and monitors

**Figure 115.** Inputs and Outputs File Import page

5. Enter the directory path in the Configuration File field or use the **Browse** button to navigate to the directory folder where the file is stored. Select the file and click **OK**.
6. Select the **Create cameras and monitors** check box, which is the default setting.
7. Click **Submit** to generate the camera and monitor records and enter the records in the database. The Analog Switcher Inputs and Outputs page displays to allow the operator to make additional changes.
  - If any changes are made, click **Submit** again to save the edited records. Click **Cancel** to end the task and delete the camera and monitor records. If another page is accessed, these records remain in the database and will need to be removed manually.

Table 67 lists and describes the elements and descriptions.

**Table 67.** Analog Video Switcher Inputs and Outputs elements and descriptions

Field Name	REQ	Description
<b>Inputs</b>		
<b>Port</b>		Identifies the port number. The number of ports is dependent on the switcher model.
<b>Camera Alias</b>		Identifies the camera alias. This is assigned automatically by the configuration file.
<b>Camera Title</b>		Displays a camera title. This is assigned automatically by the configuration file.
<b>Camera</b>		Use the drop-down list to select to select the camera, if you want to change the camera assignment.
<b>Outputs</b>		
<b>Port</b>		Identifies the monitor port number.
<b>Monitor Alias</b>		Identifies the monitor alias.
<b>Monitor</b>		Use the drop-down list to select the monitor to associate with the camera.

## Troubleshooting Steps

This section describes procedures to troubleshoot Facility Commander if you are experiencing problems with video. If these steps do not resolve the problem, contact Customer Support for assistance.

### Configuration

**Table 68.** Configuration Troubleshooting Tips

Step	Action:						
1.	<ul style="list-style-type: none"> <li>Verify the client computer “hosts” file contains an entry for the Facility Commander host name and the Remote Media server host name, if applicable. If you are using DNS for all machines, this does not apply.</li> <li>Use the <code>hostname</code> command (Windows, Linux, and AIX).</li> </ul>						
2.	Verify the DVR is plugged in and is recording.						
3.	<ul style="list-style-type: none"> <li>Verify the Facility Commander license file includes video and camera capabilities. If you are unsure, contact Customer Support to review the license.</li> </ul>						
4.	Review the DVR page to check the following items:						
	<table> <tr> <td><b>Model Tab</b></td><td>Verify the correct model has been chosen, such as the Kalatel DVMRe-16CT. Confirm this DVR is associated with the correct server.</td></tr> <tr> <td><b>Address Tab</b></td><td>Verify the correct IP Address, Port, and RS-485 Address have been entered. (Also, verify this information on the DVR itself.)</td></tr> <tr> <td><b>Password Tab</b></td><td>If an Ethernet password was defined in the DVR, the same password must be entered on the Password tab.</td></tr> </table>	<b>Model Tab</b>	Verify the correct model has been chosen, such as the Kalatel DVMRe-16CT. Confirm this DVR is associated with the correct server.	<b>Address Tab</b>	Verify the correct IP Address, Port, and RS-485 Address have been entered. (Also, verify this information on the DVR itself.)	<b>Password Tab</b>	If an Ethernet password was defined in the DVR, the same password must be entered on the Password tab.
<b>Model Tab</b>	Verify the correct model has been chosen, such as the Kalatel DVMRe-16CT. Confirm this DVR is associated with the correct server.						
<b>Address Tab</b>	Verify the correct IP Address, Port, and RS-485 Address have been entered. (Also, verify this information on the DVR itself.)						
<b>Password Tab</b>	If an Ethernet password was defined in the DVR, the same password must be entered on the Password tab.						
5.	<ul style="list-style-type: none"> <li>DVRs can be connected to the Facility Commander server or to a Remote Media server. If the DVR is connected to a Media server, verify the <b>Media Server Only</b> check box on the Facility Commander page is selected.</li> <li>Verify the Remote Media server is running.</li> </ul>						
6.	Refer to the following sections to continue troubleshooting the problem: <ul style="list-style-type: none"> <li><a href="#">Configuration on page 155</a></li> <li><a href="#">Client Path Settings on page 156</a></li> <li><a href="#">Communication Failure on page 156</a></li> </ul>						

## Client Path Settings

Facility Commander uses Window DLL files, which codes and decodes video streams, to display video.

- On the client computer, the Kalatel DLL file is named:  
`NativeADV601Codec.dll`
- The DLL file resides in:  
`C:\Program Files\FacilityCommanderClient\lib\resources.`

The Client system path must be able to find the DLL file, which is created during the installation process.

➤ **To verify the path, follow these steps:**

1. From the **Start** menu, select **Settings, Control Panel**, and then **System**.
2. Select the **Advanced** tab.
3. Click **Environment Variables**.
4. In the System Variables group, confirm the path statement contains the following entries:  
`C:\Program Files\FacilityCommanderClient`  
`C:\Program Files\FacilityCommanderClient\lib\resources`
5. If these entries do not exist, click **Edit**. The New System Variable window displays.
  - a. Enter the **Variable Name**: Path
  - b. Enter the **Variable Value** identified in Step 4.
  - c. Click **OK**.
6. Click **OK** twice to close the Properties windows.

## Communication Failure

Using the Alarm Monitor, check for a DVRComm Failure Alarm.

➤ **If an alarm exists, follow these steps:**

1. Try to ping the DVR. If the ping command fails, verify the IP address, IP address mask, and gateway settings on the DVR are correct. Refer to the vendor's documentation for instructions.
2. Verify the DVR is plugged in and is recording.
3. Try turning the power to the DVR on and off.
4. If you are using a GE Security DVR, you can use a Web browser to reset it. Right click on the DVR in the navigation pane and select Browse, or follow these steps:
  - a. Use the IP address of the DVR to construct the following URL:  
`http://DVR IP Address/index.ssi`
  - b. Select **Configure**, then **Reboot**.
5. Try to ping the DVR again. If the ping command is successful, use the Alarm Monitor to reset the DVRCommFail Alarm.

## Chapter 7. Using the Video Console

This chapter describes how to use the Video Console to view live and recorded video. This chapter also includes instructions to take snapshots, select cameras, and search for video clips.



---

### **In this chapter:**

[Overview on page 158](#)

[Navigating the Video Console on page 160](#)

[Controlling Cameras on page 163](#)

[Viewing Live Video on page 165](#)

[Viewing Recorded Video on page 165](#)

[Searching for Video on page 167](#)

[Customizing the Video Console on page 175](#)

## Overview

The Video Console allows operators to view live video, select and control any camera, retrieve a marked video clip, or direct cameras to a preset position.

For cameras with PTZ (Pan/Tilt/Zoom) capabilities, you can use the mouse to control movement. This feature is not available if another operator has control of the camera. Refer to [Controlling Cameras on page 163](#) for more information.

When an alarm is generated with an associated video clip, a video icon displays on the Alarm Monitor or Event Monitor, if configured to do so. Click the video icon to launch a Video Console to display the video clip of the alarm event. Refer to [Tagging Video Events for Access Points on page 182](#) for more information.

The Graphics Viewer can be used to launch a Video Console from symbols on graphic displays. Refer to [Issuing Commands on page 340](#) for more information.

## Automatically Launch by Alarm Priority

In addition, you can configure Facility Commander to automatically launch a Video Console when an alarm event occurs with associated video. Each time an alarm event occurs within the specified priority range, the Video Console launches and displays both live video and the recorded video clip of the event.

To configure:

- Use the Configure System Parameters page to identify the priority range, which determines when the Video Console launches automatically. Refer to [System Parameters on page 50](#) for more information.
  - The priority range is from 1-to-500. Every alarm within the specified priority range will cause the Video Console to launch automatically. If a range is not specified, the Video Console will not launch automatically.
- Use Event Action Mapping to associate the alarm event and video tagging instructions, which include camera presets, camera preset with video tagging, and video tagging. Refer to [Tagging Video Events for Access Points on page 182](#) for more information.
- Identify the workstations where you want the Video Console to launch automatically when an alarm event occurs. Refer to [Workstations on page 45](#) for more information.
- Open the Alarm Monitor to display alarm activity. If the Alarm Monitor is not opened, the Video Console does not automatically launch.

If a Video Console is already displaying video from the associated camera, an additional Video Console will not launch. Also, a maximum of four video panes will automatically display within the Video Console.

## Navigating the Multi Viewer

The Multi Viewer allows you to work within each Facility Commander application at once. By default, the Multi Viewer displays the Graphics Viewer, Video Console and Alarm Monitor in the same window. However, you can select any combination of applications to display in each of the Multi Viewer's three panes.

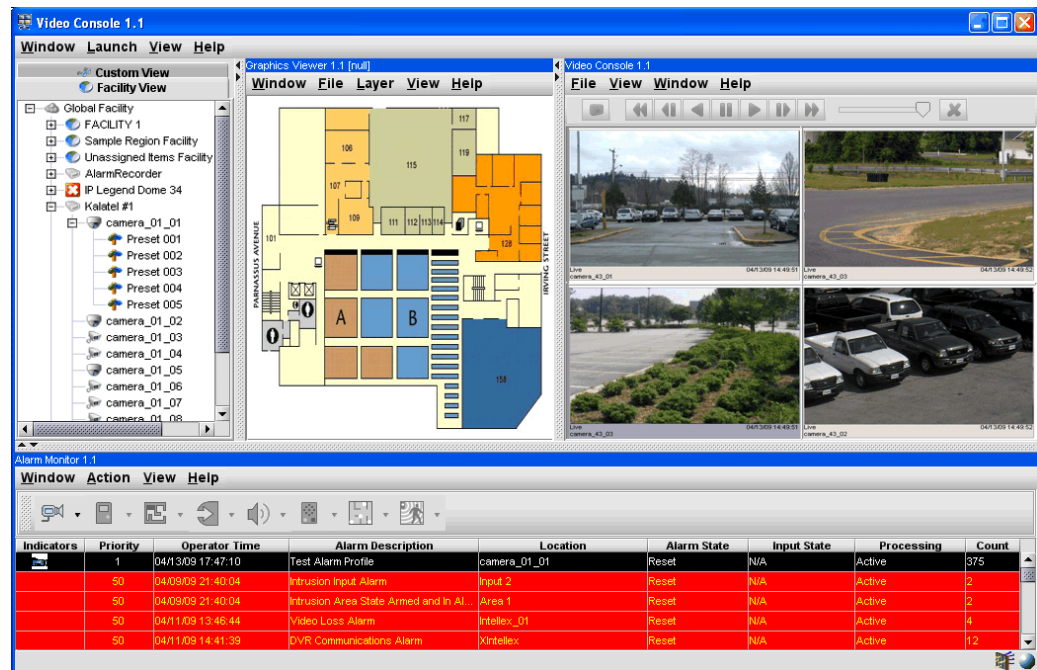


Figure 116. Multi Viewer

### ► To arrange applications in the Multi Viewer:

1. Select a pane in which to view a Facility Commander application.
2. Click File>Exit or Window>Exit, depending on the application, to close the application in that pane.
3. Right-click in the empty pane. Select from any of the four Facility Commander applications (Alarm Monitor, Event Monitor, Video Viewer or Graphics Viewer).
4. The selected application displays in that pane. The name of the application displays a number indicating how many instances of an application is open. For example, if there are two instances of the Graphics Viewer open, the first will display as 1.1 and the second as 1.2.

## Drag and Drop Cameras

Use this feature with cameras connected to DVRs. Operators can select cameras from the navigation pane, or from a map in the Graphics Viewer, and drag the camera to any pane in the Video Console. Live video displays in the selected pane.

## Navigating the Video Console

► To display the Video Console, follow these steps:

1. Open the **Facility Commander Launcher** window.
2. Select **Launch** and **Video Viewer**, or select the Video Viewer icon from the Viewers toolbar. The Video Console window shown in [Figure 117](#) displays.

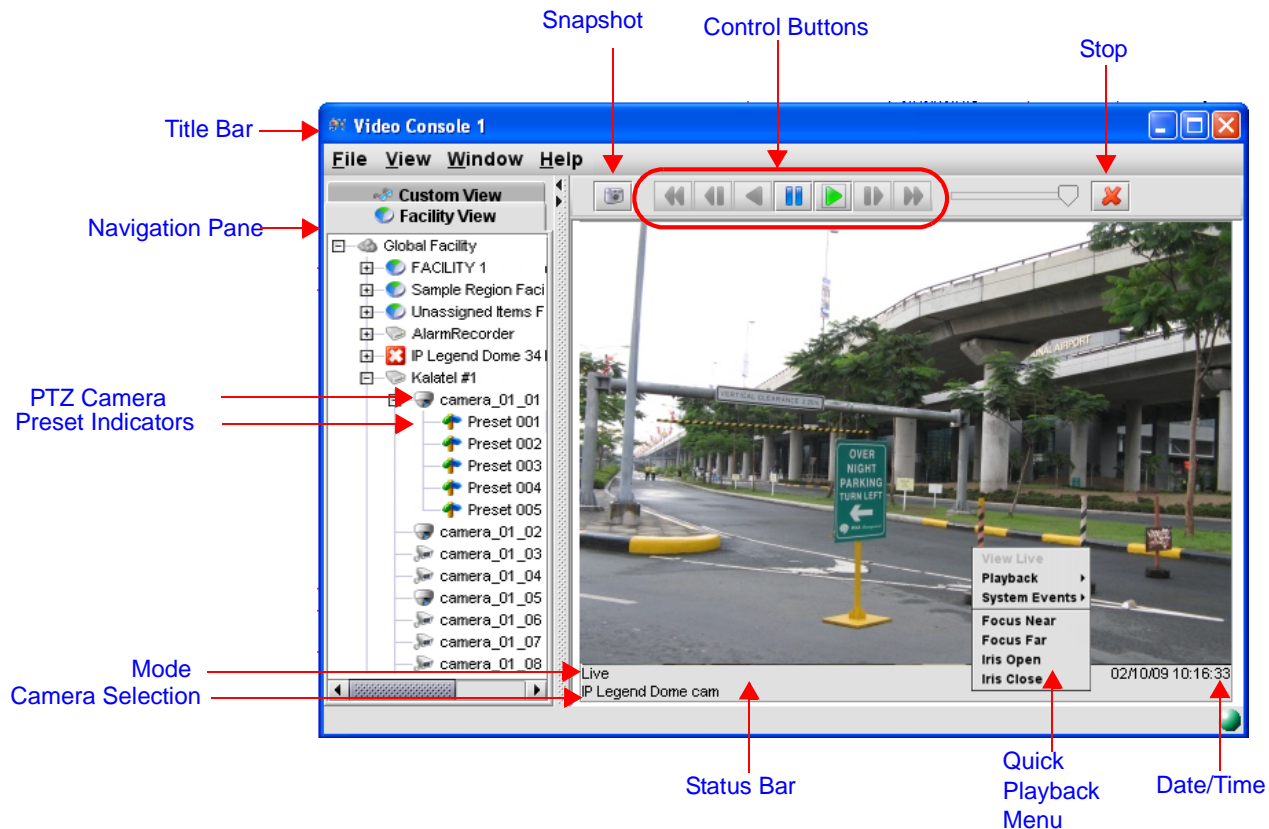


Figure 117. Video Console

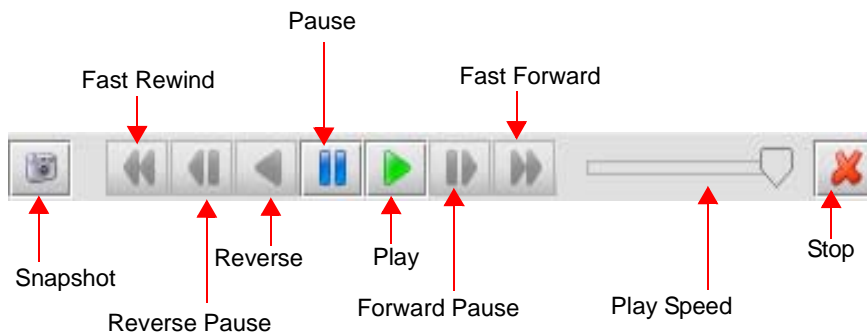
[Table 69](#) lists and describes the elements in the Video Console.

Table 69. Video Console elements and descriptions









Element	Description
Title Bar	Displays Video Console, window instance number, and custom window title. <ul style="list-style-type: none"> <li>Refer to <a href="#">Managing Multiple Windows on page 20</a> for more information about window instance numbers.</li> <li>Refer to <a href="#">Creating Custom Views on page 175</a> for instructions to add window titles.</li> </ul>





**Table 69.** Video Console elements and descriptions (Continued)

Element	Description
<b>Navigation Pane</b>	<p>The Video Console displays the configured DVRs and cameras in a hierarchal structure. Each DVR is identified with the associated cameras and preset conditions. The DVRs are listed in alphabetical order using the Tag Name field.</p> <p>To change camera views, select a different camera in the navigation pane. The Video Console replaces the previous image with live video from the recent selection. This gives you the ability to switch from one view to another.</p> <p>The items that display in the navigation pane are determined by an operator's permission levels and contexts. Use the Window Filter to further limit the number of items in the navigation pane. Refer to <a href="#">Create a window filter on page 176</a> for more information.</p>
<b>Control Buttons</b>	
<b>Snapshot</b>	<p>Click <b>Snapshot</b> to capture the current image (a single frame of video) in a JPG format. You can attach this image to an e-mail message for distribution.</p> <p>The images are stored on the Windows client in the directory <code>c:\Video</code></p> <p>To change the directory where snapshots will be stored:</p> <ol style="list-style-type: none"> <li>1 Select File&gt;Preferences to open the Video Viewer Preferences window.</li> <li>2 Click the ... button to open the Select Directory dialog.</li> <li>3 Choose a directory and click OK.</li> <li>4 Click OK again to close the Video Viewer Preferences window.</li> </ol> <p>The format of the file name is:  camera tag name.ddmmyy hhmmss.jpg  An example is:  CAM Lobby.180303 072910.jpg</p>
<b>Play speed</b>	<p>Click the bar and slide to adjust the playback speed of recorded video. The DVR playback speed can be adjusted by this method from minimum to maximum speed.</p>
<b>Stop</b>	<p>Use this button to stop the video stream.</p>

**Table 69.** Video Console elements and descriptions (Continued)

Element	Description
<b>PTZ Camera Indicators</b> 	<p>Use the mouse to control the camera functions. The cursor changes to a “hand” when you move the mouse over the video window.</p> <ul style="list-style-type: none"> <li>Use the left mouse button to control the pan and tilt functions. Move the mouse up or down to tilt the camera. Move the mouse left or right to pan the camera.</li> <li>Use the right mouse button (or mouse scroll wheel) to control the zoom functions. Move the mouse up to zoom in (larger image) and down to zoom out (smaller image).</li> </ul>
<b>Camera Indicators</b> 	Indicates a fixed (non-PTZ) camera.
<b>Facility Indicators</b> 	Indicates a facility under which multiple devices can be grouped.
<b>DVR Indicator</b> 	Indicates the device is a DVR.
<b>Offline Indicator</b> 	Indicates the device is offline. Right-click on this icon, and then select Online to set the device online.
<b>Comm Fail Indicator</b> 	Indicates the device communication has failed.
<b>Alarm Indicator</b> 	Indicates the device is an alarm state.
<b>Preset Indicators</b> 	<p>Displays this icon in the navigation pane when the camera has preset positions. Select the preset position of the current camera you want to view. The camera preset positions display in alphabetical order under their associated camera in the navigation pane.</p> <p>This option displays in <b>Live</b> mode only.</p>

**Table 69.** Video Console elements and descriptions (Continued)

Element	Description
<b>Status Bar</b>	
<b>Quick Playback menu</b>	<p>Right-click on the Status Bar to view the Quick Playback menu.</p> <ul style="list-style-type: none"> <li>• <b>View Live:</b> Click to toggle from Record mode to Live mode.</li> <li>• <b>Playback:</b> Click to toggle from Live mode to Record mode. You can select to playback from 15 seconds to 5 minutes of the last recorded video.</li> <li>• <b>System Events:</b> Displays the last four system events</li> <li>• <b>Focus Near:</b> Select to change the camera focus to the foreground. Select again until the focus is satisfactory.</li> <li>• <b>Focus Far:</b> Select to change the camera focus to the background. Select again until the focus is satisfactory.</li> <li>• <b>Iris Open:</b> Select to increase the amount of light. Select again to increase in increments until the lighting is satisfactory.</li> <li>• <b>Iris Close:</b> Select to decrease the amount of light. Select again to decrease in increments until the lighting is satisfactory.</li> </ul>
<b>Mode</b>	Displays <b>Live</b> mode or <b>Recorded</b> mode.
<b>Date/Time</b>	Displays the current date and time when you are in Live mode. When you are in Recorded mode, the date and time of the video event display. This is the DVR's time zone.
<b>Camera Selection</b>	<p>Identifies the current, or active, camera that is sending video to the Video Console. The camera label identifying the camera is comprised of the tag name and description.</p> <p>Refer to <a href="#">Controlling Cameras on page 163</a> for more information.</p>
<b>Window Filter</b> 	<p>Displays an icon indicating a window filter has been applied. Right-click in the navigation pane, and select Window Filter. The contents of the list in the navigation pane are determined by which Facility Commander facilities are selected.</p> <p>Refer to <a href="#">Create a window filter on page 176</a>.</p>
<b>Server Connection Indicator</b> 	<p>Displays an icon indicating if the system with the Video Console is connected to the Facility Commander server.</p> <ul style="list-style-type: none"> <li>• Green indicates the system is communicating with the server.</li> <li>• Red indicates the system is no longer communicating with the Facility Commander server.</li> </ul>

## Controlling Cameras

This section describes how to view live video, recorded video, and use Event Action Mapping to control the camera and capture video.

## Live Video

An operator selects a camera from the navigation pane and the Video Console displays live video from that camera. If that camera has pan/tilt/zoom capabilities, only one operator can control the camera.

When an operator attempts to control the camera in use by another operator, a message displays stating: **PTZ device currently in use.**

After thirty seconds of inactivity, the lock on the camera device is released so that another operator can use the camera and this message displays: **PTZ device has been released.** The messages display in the status bar.

## Recorded Video

Multiple operators can view recorded video simultaneously from the same DVR, but the recorded video will be from the same time base.

When an operator is viewing recorded video, click **Play** and the timeout is extended for an additional thirty seconds.

**Note:** Some DVRs may not support independent playback.

## Event Action Mapping

Event Action Mapping contains two actions related to camera control: Camera Preset and Camera Preset with Video Tagging. These two actions take priority over any manual camera operation by an operator. As soon as the camera preset action has occurred, the operator can take control of the camera again.

## Viewing Live Video

### ► To view live video, follow these steps:

1. Select a camera from the navigation pane and live video displays on the Video Console. Or, drag the camera icon to a pane in the Video Console to view live video.
  - To move a camera to a different preset position, click the preset name in the navigation pane.
  - If you are unable to view video using the Video Console, verify the DVR is set to Record mode.
2. If the camera has pan/tilt/zoom capabilities, use the mouse to control the viewing area.
  - Use the right mouse button or mouse scroll wheel to zoom. Right-click and move the mouse up or down to zoom in or out (or move the mouse scroll wheel forward or backward).
  - Use the left mouse button to pan. Left-click and move the mouse in any direction to view video for a specific area.
3. To change to a different camera view, select a camera or preset position from the navigation pane. The Video Console displays video from the selected device.

## Viewing Recorded Video

### ► To view recorded video, follow these steps:

1. From the **File** menu in the Video Console, select **Play Video Clip**. The Open dialog displays.
2. Select a file from the list and click Open. The selected file opens in a new window.
3. Use the slider bar or control buttons to pause, stop, fast forward, or rewind the video clip.

## View a Single Video Frame

The Video Console permits an operator to view recorded video, frame by frame. Refer to [Control Buttons on page 161](#) to view each button.

### ► To view a single video frame, follow these steps:

1. Select the Video Console pane and select the camera from the navigation pane.
2. Use the control buttons to navigate to the portion of the clip you want to review.
3. Click **Forward Pause** to view a single frame. Continue to click to move the video forward one frame at a time. Each click pauses the video for 30 seconds. After 30 seconds, the video automatically resumes.
4. Click **Reverse Pause** to view a single frame. Continue to click to move the video backward one frame at a time.

## Create an Evidence CD

Investigators and other operators may need to provide recorded video from a certain date and time on CD or DVD. The Video Console allows an operator to create an evidence CD from a recorded video file.

► **To create an evidence CD, follow these steps:**

1. Place a blank CD or DVD into your disc drive.
2. From the **File** menu in the Video Console, select **Create Evidence CD**. The Create Evidence CD dialog displays.
3. Click the **Add** button to select one or more files from the list, and then click **Open**.
4. The selected files appear in the Create Evidence CD dialog.
5. The files can be written to windows default CD burning directory, or a directory of your choice:
  - a. Select the Windows CD Burning radio button and click Create to burn an evidence CD using Windows CD Burning directory.
  - b. Select the Directory radio button, and then the "..." button to choose a directory to write the evidence file, and then click the Create button. A Windows Explorer view of the files will appear. You can drag the contents of this directory to the CD burning software of your choice to burn the evidence file to CD.

Once the CD has been created you can use it to play the videos on any other Windows PC. If the player does not start automatically, you can start it manually by double clicking Player.exe on the CD. Note that the player program can take a long time to load when running it directly from the CD. If you wish, you may copy the contents of the CD to a hard drive and run it from there for faster response time.

## Searching for Video

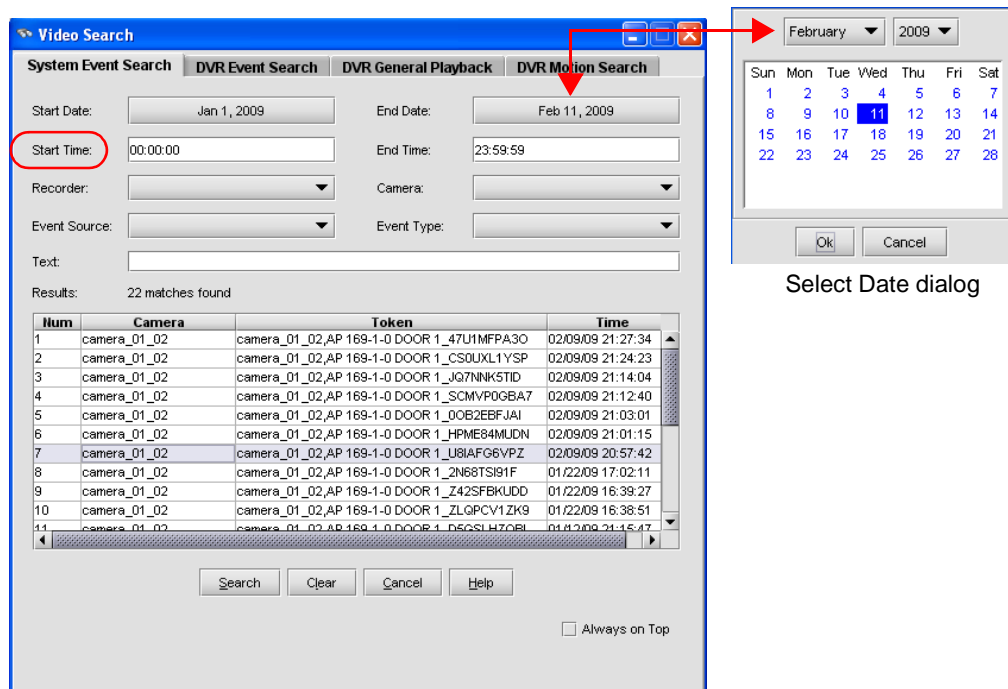
Use the Video Search feature to search for video by system event, DVR event, DVR playback, or area of motion in a camera's field of view.

### System Event Search

When investigating alarm events, investigators or other operators may need to retrieve previously recorded video clips. Use the **System Event Search** tab to locate video clips stored on the DVR devices by system event.

➤ **To search for previously recorded video clips, follow these steps:**

1. From the **File** menu, select **Video Search**. The **System Event Search** tab shown in [Figure 118](#) displays.



**Figure 118.** System Event Search tab with Select Date dialog

2. Enter the information described in [Table 70 on page 168](#) to search for a video clip. Search criteria includes: start date, start time, end date, end time, event source, event type, recorder, camera, and text description. Enter multiple values to narrow the search criteria to locate video clips.
3. Click **Search**. The number of matches found display in the Results pane. Double-click on the result you want to view and the recorded video displays in the Video Console.
4. Click **Clear** to return to the default settings and remove any matches in the Results pane.
5. Click **Close** when you are finished viewing results.

[Table 70](#) lists and describes the System Event Search tab.

**Table 70.** System Event Search tab

Element	Description
<b>Start Date</b> <b>End Date</b>	<p>To search for a specific day, click the <b>Date</b> button to display the <b>Select Date</b> window shown in <a href="#">Figure 118 on page 173</a>.</p> <ul style="list-style-type: none"> <li>Use the drop-down lists to select the month and year to display the calendar month.</li> <li>Click the day of the month to select the <b>Start Date</b> and the <b>End Date</b>.</li> </ul>
<b>Start Time</b> <b>End Time</b>	<p>To search for a specific time:</p> <ul style="list-style-type: none"> <li>Type the Operator time in the <b>Start Time</b> field to begin the search.</li> <li>Type the Operator time in the <b>End Time</b> field to end the search.</li> </ul> <p>Use this format: HH:MM:SS.</p>
<b>Event Source</b>	<p>Use the drop-down list to select the event source, such as an access point, logical input, digital input, or camera device.</p> <p>Any video events matching this event source type display in the <b>Token</b> column.</p>
<b>Event Type</b>	<p>Use the drop-down list to select the event type associated with the event source, such as an Invalid Badge or Door Forced alarm.</p> <p>Any video events matching this event type display in the <b>Token</b> column.</p>
<b>Recorder</b>	<p>Use the drop-down list to identify the DVR device where the video event is stored.</p> <p>Any video events from the specified recorder display in the <b>Token</b> column.</p>
<b>Camera</b>	<p>Use the drop-down list to identify the camera device used to record the video event.</p> <p>Any video events from the specified camera display in the <b>Token</b> column.</p>
<b>Text Search</b>	<p>Use to enter the DVR token name identifying the video clip. The token name can be up to 50 characters.</p>
<b>Results</b>	<p>Displays the number of matches found, camera tag name, the camera tag and token name, and the time of the video event.</p> <p>Double-click the token name to play the recorded video.</p>



## DVR Event Search

Use the **DVR Event Search** tab to locate video clips stored on the DVR devices by DVR event.

► **To search for previously recorded video clips, follow these steps:**

1. From the **File** menu, select **Video Search**.
2. Select the **DVR Event Search** tab. The DVR Event Search tab shown in [Figure 119](#) displays.

**Video Search**

System Event Search **DVR Event Search** DVR General Playback DVR Motion Search

Recorder: SymDec Cameras: camera\_04\_01

Start Date: Feb 26, 2009 End Date: Feb 27, 2009

Start Time: 02:00:00 End Time: 23:59:59

Search Type: ☒ Alarm ☐ Event ☐ Text

Results: 4 matches found

Num	Camera	Start Date/Time	End Date/Time
1	camera_04_01	02/26/09 02:02:23	02/26/09 08:19:34
2	camera_04_01	02/26/09 08:19:44	02/26/09 12:25:02
3	camera_04_01	02/26/09 12:25:02	02/26/09 15:40:36
4	camera_04_01	02/26/09 15:47:48	02/27/09 08:33:50

Search Clear Cancel Help

☐ Always on Top

**Figure 119.** DVR Event Search tab

3. Enter the information described in [Table 71 on page 170](#) to search for a video clip. Search criteria includes: start date, start time, end date, end time, recorder, camera, and text description. Enter multiple values to narrow the search criteria to locate video clips.
4. Click **Search**. The number of matches found display in the Results pane. Double-click the result you want to view and the recorded video displays in the Video Console.
5. Click **Clear** to return to the default settings and remove any matches in the Results pane.
6. Click **Close** when you are finished viewing results.

[Table 71](#) lists and describes the DVR Event Search tab.

**Table 71.** DVR Event Search tab

Element	Description
<b>Start Date</b> <b>End Date</b>	To search for a specific day, click the <b>Date</b> button to display the <b>Select Date</b> window shown in <a href="#">Figure 119 on page 169</a> . <ul style="list-style-type: none"><li>Use the drop-down lists to select the month and year to display the calendar month.</li><li>Click the day of the month to select the <b>Start Date</b> and the <b>End Date</b>.</li></ul>
<b>Start Time</b> <b>End Time</b>	To search for a specific time: <ul style="list-style-type: none"><li>Type the device time in the <b>Start Time</b> field to begin the search.</li><li>Type the device time in the <b>End Time</b> field to end the search.</li></ul> Use this format: HH:MM:SS.
<b>Recorder</b>	Use the drop-down list to identify the DVR device where the video event is stored.
<b>Cameras</b>	Use the drop-down list to identify the camera device used to record the video event. Any video events from the specified camera display in the <b>Camera</b> column.
<b>Text Search</b>	Use to enter the DVR token name identifying the video clip. The token name can be up to 50 characters.
<b>Results</b>	Displays the number of matches found, camera tag name, the start date/time, and end date/time of the video event.

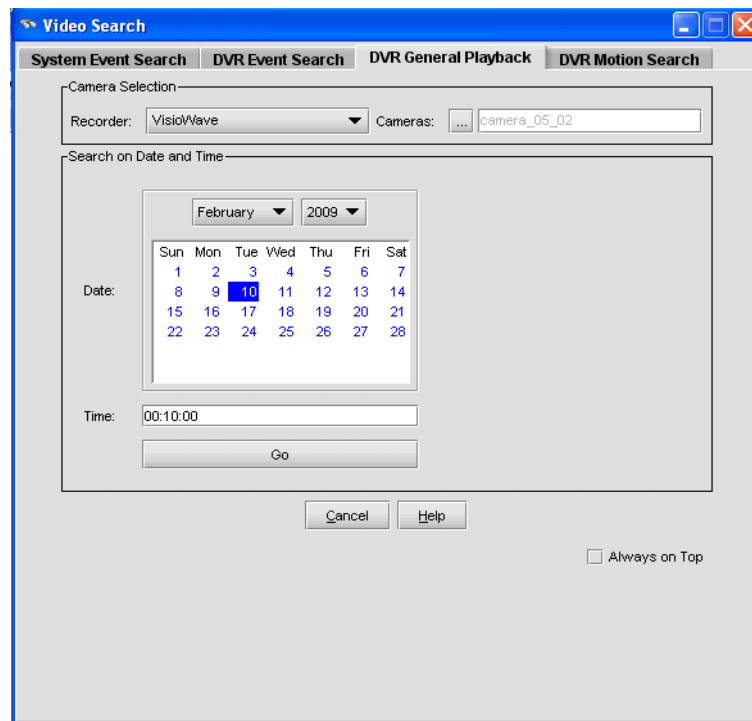
## DVR General Playback Search

Investigators and other operators may want to view previously recorded video for a specific date and time, which is not necessarily when an alarm event occurs. Facility Commander allows you to retrieve recorded video from the DVR, which differs from retrieving only a marked video clip from an alarm event.

The DVR General Playback tab allows an operator to view recorded video by selecting a DVR, a camera, and a specific date and time.

► **To search for recorded video, follow these steps:**

1. From the **File** menu, select **Video Search**.
2. Select the **DVR General Playback** tab. The DVR General Playback tab shown in [Figure 120](#) displays.



**Figure 120.** DVR General Playback tab

3. Enter the information described in [Table 72 on page 172](#) to search for recorded video.
  - Search criteria includes: recorder, cameras, date, and time. Enter multiple values to narrow the search criteria.
4. Click **Go**. The recorded video displays in the Video Console.
5. Click **Close** when you are finished viewing results.

[Table 72](#) lists and describes the DVR General Playback tab.

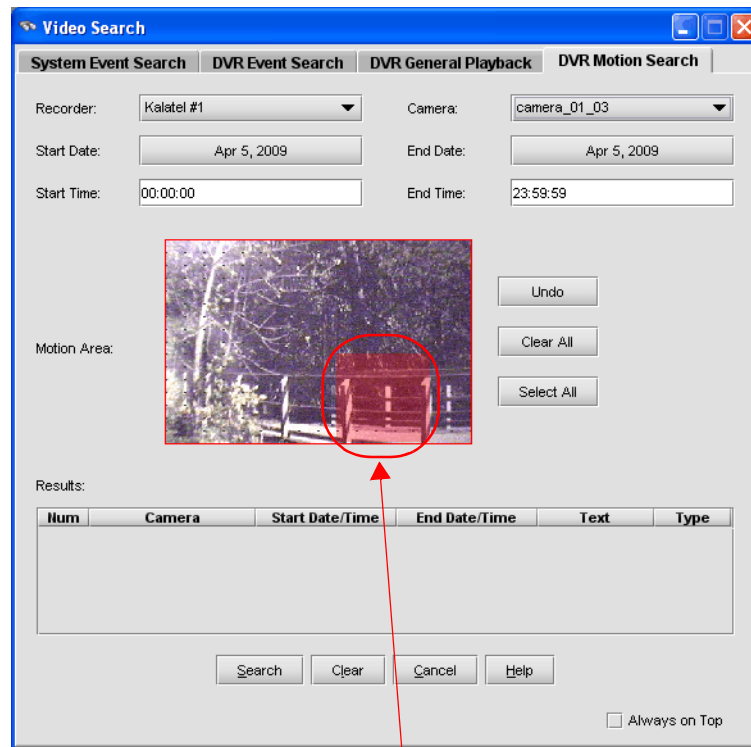
**Table 72.** DVR General Playback tab

Element	Description
<b>Camera Selection</b>	
<b>Recorder</b>	Use the drop-down list to identify the DVR device where the recorded video is stored.
<b>Camera</b>	Use the drop-down list to identify the camera device used to record the video.
<b>Search on Date and Time</b>	
<b>Date</b>	<ul style="list-style-type: none"><li>• Use the drop-down list to select the month.</li><li>• Use the drop-down list to select the year.</li></ul>
<b>Time</b>	Enter the time. The format is: HH:MM:SS.

## DVR Motion Search

- To search for recorded video that includes motion, follow these steps:

1. From the **File** menu, select **Video Search**.
2. Select the **DVR Motion Search** tab. The DVR Motion Search tab shown in [Figure 121](#) displays.



Selected area shaded in red

**Figure 121.** DVR Motion Search tab

3. Enter the information described in [Table 73 on page 174](#) to search for recorded video. Search criteria includes: recorder, camera, start date, end date, start time, and end time. Enter multiple values to narrow the search criteria.
4. Click and drag the cursor in the Motion Area pane to select an area to search. This is the area within which the system will detect if motion has occurred. The area selected will be shaded in red. You can also click on **Select All** to detect motion in the camera's entire viewing area. Click **Clear All** to remove all selected areas.
5. Click **Search**. The number of matches found display in the Results pane. Double-click the result you want to view and the recorded video displays in the Video Console.
6. Click **Clear** to return to the default settings and remove any matches in the Results pane.
7. Click **Close** when you are finished viewing results.

**Table 73.** DVR Motion Search tab

Element	Description
<b>Camera Selection</b>	
<b>Recorder</b>	Use the drop-down list to identify the DVR device where the recorded video is stored.
<b>Camera</b>	Use the drop-down list to identify the camera device used to record the video.
<b>Search on Date and Time</b>	
<b>Date</b>	<ul style="list-style-type: none"><li>• Use the drop-down list to select the month.</li><li>• Use the drop-down list to select the year.</li></ul>
<b>Time</b>	Enter the time. The format is: HH:MM:SS.

## Customizing the Video Console

The Video Console displays one viewer pane, tag name, and description as the default settings. However, an operator can customize the Video Console to display certain facilities, or a create a custom layout of camera views. Refer to the following sections:

- [Creating Custom Views on page 175](#)
- [Create a window filter on page 176](#)
- [Display Additional Video Panes on page 177](#)

### Creating Custom Views

The Video Console allows you to create your own combination of camera views by using the layout selections in the View menu. An operator can arrange the camera views in a customized layout to provide a comprehensive view of the premises.



**Figure 122.** Custom 4-Up View

► **To create a custom view:**

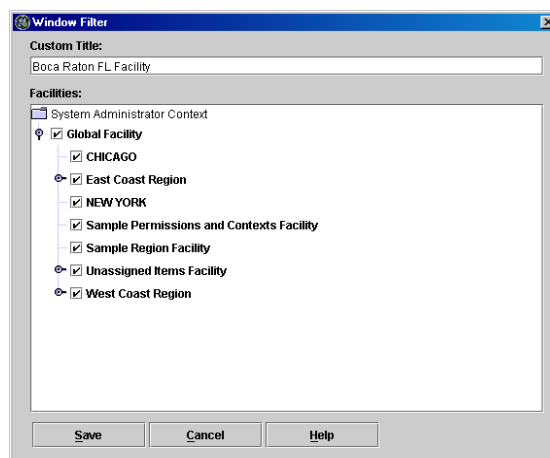
1. From the **View** menu, select one of the layouts. The Video Console displays the selected layout.
2. Select a camera from the navigation pane and drag-and-drop it to one of the empty panes in the console. The video for that camera displays in that pane.
3. Continue dragging and dropping cameras to create your own customized view.

4. When you are finished, from the **View** menu, select **Save Custom View**.
  5. The Save User View dialog displays. Enter a name for this custom view and click OK. The custom view displays in the Custom View tab of the navigation pane.
- **To upload a custom view:**
1. Select **View**, and then select **Upload Views**. The Location To Upload Views To dialog displays.
  2. Under Look In, select a location to upload your custom views.
  3. In the File Name field, type a name for the custom views file. The file name will be appended with the .views file extension.
  4. Click the **Upload** button. The custom views are saved in the specified location.
- **To download a custom view:**
1. Select **View**, and then select **Download Views**. The Select Location To Download Views From dialog displays.
  2. Under Look In, select the location where your custom views are saved.
  3. Select the custom views file. The file name is appended with the .views file extension.
  4. Click the **Download** button. The custom views are now available on the Custom View tab in the navigation pane.

## Create a window filter

The Video Console navigation pane can be filtered to view selected facilities.

- **To filter facilities from view in the navigation pane, follow these steps:**
1. Right-click in the navigation pane, and then select **Window Filter**. The window filter in [Figure 123](#) displays.



**Figure 123.** Window Filter window



2. Use the **Custom Title** field to identify a title to display on the Video Console title bar. The maximum number of characters is 256.
3. Select or clear the check boxes next to the facilities you want to display or hide from view in the navigation pane. A check mark indicates the item is selected.
4. Click **Save**. The Video Console displays a window filter icon in the status bar indicating the list of items has filtered.

## Display Additional Video Panes

► **To display video in more than one video pane, follow these steps:**

1. From the **View** menu, select **2 Up** (or another number). The Video Console displays two video panes. The Video Console can display one, two, four, nine, or sixteen video panes.
  - When increasing the number of panes in the Video Console, the additional panes are blank or inactive.
2. To view video in an inactive pane, select the frame and then select the camera from the navigation pane.
  - The control buttons reflect the active pane.
  - Double-click any active frame to display a one-up view in a separate Video Console. If it is open already, the Video Console moves to the foreground.
3. To view recorded video, see [Viewing Recorded Video on page 165](#)



## Chapter 8. Event Action Mapping

This chapter introduces the Event Action Mapping, which allows you to select event sources and specify actions, such as moving cameras to preset positions or tagging video events and more.



---

### In this chapter:

- [Overview on page 180](#)
- [Viewing Event Action Mappings on page 181](#)
- [Tagging Video Events for Access Points on page 182](#)
- [Tagging Video Events for Intercom Calls on page 183](#)
- [Activating Digital Outputs on page 184](#)
- [Events in Event Action Mapping on page 186](#)
- [Actions in Event Action Mapping on page 190](#)

## Overview

Event Action Mapping is a powerful feature that allows system administrators to select event sources and program Facility Commander to take automatic actions. For example, when an alarm event is generated, cameras can move to preset positions, e-mails can be sent to designated personnel, and outputs can be activated.

Refer to the following sections for a list of available events and actions:

- [Events in Event Action Mapping on page 186](#)
- [Actions in Event Action Mapping on page 190](#)

Refer to the following sections for additional instructions:

- [Tagging Video Events for Access Points on page 182](#)
- [Tagging Video Events for Intercom Calls on page 183](#)
- [Activating Digital Outputs on page 184](#)
- [Sending Automatic E-mails on page 185](#)

Event Action Mapping allows you to associate event sources and event types to a specific action. An event action mapping is created by identifying the following items.

- **Event Source Types** represent the type of event sources that can generate actions, such as cameras, DVRs, and doors.
- **Event Sources** are individual devices or items that can trigger actions. Event sources are specific access points, cameras, DVRs, digital inputs, logical inputs, intercom and intrusion devices, and servers.
- **Event Types by Condition** is a combination of alarm state and alarm for the device.
- **Actions** represent the action or activity you want to take place when the combination of event source, type, and condition are met. Facility Commander allows you to lock or unlock doors, tag a video event, move a camera to a preset position, send e-mails, and more.

Depending on the actions you select, the action parameters display the appropriate drop-down list and text boxes. Select from these options:

- **Access control** to issue commands, such as locking or unlocking doors, or activating an output.
- Analog Video Switcher to
- **Intrusion** to issue commands, such as arming or disarming an area.
- **Intercom** to take an action, such as making a call to an intercom station.
- **E-mails** can be sent automatically to alert the appropriate staff members, so that they can respond to the alarm condition.
- **Video** to tag video events or direct cameras to preset positions. Refer to [Tagging Video Events for Access Points on page 182](#) for instructions.

## Viewing Event Action Mappings

Use the Event Action Mappings page to add, copy, or delete event action mapping records. These records cannot be edited. Instead, copy an existing record and make the necessary changes to create a new record.

► **To view event action mapping records, follow these steps:**

1. Select **Device Management**.
2. Select **Event Action Mappings**. The Event Action Mappings page shown in [Figure 124](#) displays.

Event Action Mappings

Request was successful.

Instructions

View, add or delete event action mappings. Define actions the system will take when a specified event occurs. The event action mappings in the list below are sorted first by event source and then by subsystem.

Search:

Go

Add Event Action Mapping

◀ Page 1 of 1 ▶

Go to  Go

Items per Page 10 ▼

	Event Source	Event Type	Condition	Subsystems	Action	Parameter	Parameter	Parameter	Parameter
	AP 200101 NY COMPUTER ROOM	Door Forced Alarm	Set	Digital Video	Video Tagging	Destination: NY Cam 100			
	AP 200200 NY SHIPPING DOCK	Door Forced Alarm	Set	Access Control Manager	Activate Output	OutputDestination: DO 200116 NY FIRE SOUNDER			
	AP 200200 NY SHIPPING DOCK	Door Forced Alarm	Set	Digital Video	Video Tagging	Destination: NY Cam 100			
	AP 200300 NY LOBBY WEST	Door Forced Alarm	Set	Access Control Manager	Lock	Destination: AP 200101 NY COMPUTER ROOM			
	AP 200300 NY LOBBY WEST	Door Forced Alarm	Set	Digital Video	Video Tagging	Destination: NY Cam 100			
	NY B1 DVR	DVR Communications Alarm	Set	Mail Man	Email The Event	Header: DVR Alarm	To: Frank	From: Vincent	Subject: DVR Alarm in NY B1
	NY Lobby Bldg 1	Intercom Master Call Connected	Set	Intercom Manager	Dial Digits	OriginatingStationId: NY Lobby Bldg 1	DigitsToDial: 6156		

**Figure 124.** Event Action Mappings page

When a record is changed, such as changing the tag name, the event source name is automatically updated to reflect the new tag name. Also, if an event source is deleted, the event action mapping record is also deleted.

## Tagging Video Events for Access Points

► To tag a video event when an alarm occurs, follow these steps:

1. Select **Device Management**, and then **Event Action Mappings**. The Event Action Mapping page shown in [Figure 124 on page 181](#) displays.
2. Click **Add Event Action Mapping**. The Configure Event Action Mapping page as shown in [Figure 125](#) displays.

**Configure Event Action Mapping**

**Instructions**  
View or add the event action mapping. Define the actions the system will take when the specified event occurs.

Event	Action
<b>Event Source Type</b> * Door Access Point	<b>Subsystems</b> * Digital Video
<b>Event Sources</b> AP 200101 NY COMPUTER ROOM AP 200200 NY SHIPPING DOCK AP 200201 NY CAFETERIA * AP 200300 NY LOBBY WEST AP 200301 NY CONFERENCE ROOM AP 200400 NY LIBRARY AP 200401 NY TRAINING ROOM	<b>Subsystem Actions</b> * Camera Preset with Video Tagging
<b>Event Types By Condition</b> * Set + Door Forced Alarm Set + Door Held Alarm Set + Door Prealarm Set + Invalid Badge Alarm Set + Lost Badge Alarm Set + Suspended Badge Alarm Set + Unknown Badge Alarm Reset + Door Forced Alarm Reset + Door Held Alarm Reset + Door Prealarm	<b>Destination</b> * NY Cam 300 <b>Preset</b> * NY Cam 300 Preset

**Figure 125.** Configure Event Action Mapping page

3. Use the **Event Source Type** drop-down list to select the access point or device.
4. Use the **Event Sources** list to select one or more event sources. This list is populated with items based on the selected event source type. Press the **Ctrl** key while selecting multiple items.
5. Use the **Event Types By Condition** list to select one or more alarm conditions. Press the **Ctrl** key while selecting multiple items.
6. Use the **Subsystems** drop-down list to select **Digital Video**.
7. Select the appropriate action from the **Subsystem Actions** drop-down list.
8. Select a camera device from the **Destination** drop-down list. If the camera has preset positions, another drop-down list displays to select the preset positions.
9. Click **Submit** to save the record.

## Tagging Video Events for Intercom Calls

- To create an intercom event when an alarm occurs, follow these steps:
1. Select **Device Management**, and then **Event Action Mappings**. The Event Action Mappings page displays as shown in [Figure 124 on page 181](#).
  2. Click **Add Event Action Mapping**. The Configure Event Action Mapping page as shown in [Figure 126](#) displays.

Configure Event Action Mapping

**Instructions**  
Define the actions the system will take when the specified event occurs. When defining **Event Sources** or **Event Types By Condition**, hold the **Ctrl** key down for multiple selection.

Event

Event Source Type

\* Intercom Substation

Event Sources

\* NY Bldg 1 Intercom

Event Types By Condition

\* Set + Intercom Substation Call Button Alarm

Action

Subsystems

\* Digital Video

Subsystem Actions

\* Camera Preset with Video Tagging

Destination

\* NY Cam 100

Preset

\* NY Cam 100 PS 01

**Figure 126.** Configure Event Action Mapping page

3. Use the **Event Source Type** drop-down list to select the access point or device.
4. Use the **Event Sources** list to select one or more event sources. This list is populated with items based on the selected event source type. Press the **Ctrl** key while selecting multiple items.
5. Use the **Event Types By Condition** list to select one or more event types and alarm conditions. Press the **Ctrl** key while selecting multiple items.
6. Use the **Subsystems** drop-down list to select **Digital Video**.
7. Select the appropriate action from the **Subsystem Actions** drop-down list. The selections include:
  - **Camera Preset** to move a camera to a preset position.
  - **Camera Preset with Video Tagging** to move a camera to a preset position and mark a video clip.
  - **Video Tagging** to mark a video clip that can be retrieved later for investigation.
8. Select a camera device from the **Destination** drop-down list. If the camera has preset positions, another drop-down list displays to select the preset positions.
9. Click **Submit** to save the record.

Facility Commander Administration Guide Page 183

## Activating Digital Outputs

► To configure Facility Commander to activate a digital output, follow these steps:

1. Select **Device Management**, and then **Event Action Mappings**. The Event Action Mappings page shown in [Figure 124 on page 181](#) displays.
2. Click **Add Event Action Mapping**. The Configure Event Action Mapping page as shown in [Figure 127](#) displays.

**Figure 127.** Configure Event Action Mapping page

3. Use the **Event Source Type** drop-down list to select the access point or device.
4. Use the **Event Sources** list to select one or more event sources. This list is populated with items based on the selected event source type. Press the **Ctrl** key while selecting multiple items.
5. Use the **Event Types By Condition** list to select one or more alarm conditions. Press the **Ctrl** key while selecting multiple items.
6. Use the **Subsystems** drop-down list to select **Access Control Manager**.
7. Select the appropriate action from the **Subsystem Actions** drop-down list. Depending on the selection, additional lists or fields may display. Refer to [Actions in Event Action Mapping on page 190](#) for a complete list.
8. Select an **Output Destination**. This is the Digital Output you are associating with this event.
9. Click **Submit** to save the record.



## Sending Automatic E-mails

**Note:** To send automatic e-mails, your server must be configured for SMTP.

➤ **To automatically send an e-mail when an alarm event occurs, follow these steps:**

1. Select **Device Management**, and then **Event Action Mappings**. The Event Action Mapping page displays as shown in [Figure 124 on page 181](#).
2. Click **Add Event Action Mapping**. The Configure Event Action Mapping page similar to the one shown in [Figure 128](#) displays.

**Configure Event Action Mapping**

**Instructions**  
Define the actions the system will take when the specified event occurs. When defining **Event Sources** or **Event Types By Condition** selection.

**Event**

**Event Source Type**

\* Digital Video Recorder

**Event Sources**

AlarmRecorder

IP Legend Dome 34

Kalatel #1

\* Kalatel #2

Kalatel #3

StoreSafe Pro II

SymDec

SymDec 32

**Event Types By Condition**

Set + DVR Communications Alarm

Set + DVR Health Fail Alarm

Set + DVR Health Trouble Alarm

Set + Disk Full Alarm

\* Reset + DVR Communications Alarm

Reset + DVR Health Fail Alarm

Reset + DVR Health Trouble Alarm

Reset + Disk Full Alarm

**Action**

**Subsystems**

\* Mail

**Subsystem Actions**

\* Email The Event

**Header**

\*

**To**

\*

**From**

\*

**Subject**

\*

Submit
Cancel

**Figure 128.** Configure Event Action Mapping page

3. Use the **Event Source Type** drop-down list to select the access point or device.
4. Use the **Event Sources** list to select one or more event sources. This list is populated with items based on the selected event source type. Press the **Ctrl** key while selecting multiple items.
5. Use the **Event Types By Condition** list to select one or more alarm conditions. Press the **Ctrl** key while selecting multiple items.
6. Use the **Subsystems** drop-down list to select **Mail**.
7. Use the **Subsystem Actions** drop-down list to select **Email the Event**. Additional text boxes display to enter e-mail information.
8. Complete the required items: **Header**, **To**, **From**, and **Subject**.

9. Click **Submit** to save the record.

## Events in Event Action Mapping

Table 74 lists and describes the fields on the Configure Mapped Event page.

**Table 74.** Configure Mapped Event fields and descriptions

Event Source	Event Type	Condition
<b>Access Control</b>	Access System Comm Failure	Set, Reset
<b>Analog Switcher</b>	Analog Switcher Offline	Set, Reset
<b>Camera</b>	Video Loss Alarm	Set, Reset
	Motion Detection Alarm	Set, Reset
<b>Digital Input</b>	Input Alarm	Set, Reset, Tamper
<b>Digital Video Recorder</b>	Digital Video Recorder Comm Fail	Set, Reset
<b>External Media Server</b>	Remote Media Server Comm Failure	Set, Reset
<b>History Table Rollover</b>	Table Rollover Event	Set
<b>Intercom Exchange</b>	Intercom Exchange Comm Failure Alarm	Set, Reset
	Intercom Exchange Reset Alarm	Set
	Intercom Exchange Reset Alarm Event	Set
<b>Intercom Master Station</b>	Intercom Master Call Answered	Set
	Intercom Master Call Connected	Set
	Intercom Master Call Ringing	Set
	Intercom Master Call To Busy	Set
	Intercom Master Call To Private	Set
	Intercom Master Busy	Set
	Intercom Master Disconnected	Set

**Table 74.** Configure Mapped Event fields and descriptions (Continued)

Event Source	Event Type	Condition
<b>Intercom Substation</b>	Intercom Master Reset	Set
	Intercom Substation Call Connected	Set
	Intercom Substation Call Ringing	Set
	Intercom Substation Call To Busy	Set
	Intercom Substation Call To Private	Set
	Intercom Substation Call Button Alarm	Set, Reset
	Intercom Substation Busy	Set
	Intercom Substation Disconnected	Set
	Intercom Substation Call Button Event	Set
	Intercom Substation Reset	Set
<b>Intrusion Area</b>	Intrusion Area Alarm Event	Set, Reset
	Intrusion Area Disarmed During Alarm	Set
	Intrusion Area Failed to Arm	Set
	Intrusion Area State Armed All Clear	Set
	Intrusion Area Armed and In Alarm	Set, Reset
	Intrusion Area Armed and In Alarm Event	Set, Reset
	Intrusion Area State Disarmed	Set
	Intrusion Area State Unknown	Set
<b>Intrusion DGP</b>	Intrusion DGP Battery Low	Set, Reset
	Intrusion DGP Battery Missing	Set, Reset

**Table 74.** Configure Mapped Event fields and descriptions (Continued)

Event Source	Event Type	Condition
	Intrusion DGP Battery Test Fail	Set
	Intrusion DGP Battery Test Start	Set, Reset
	Intrusion DGP Fuse Failure	Set, Reset
	Intrusion DGP Bypassed	Set, Reset
	Intrusion Main Panel Failure Alarm	Set, Reset
	DGP Offline Alarm	Set, Reset
	DGP Polled	Set, Reset
	DGP Siren Monitor Fail	Set, Reset
	DGP Tamper Alarm	Set, Reset
	DGP Tamper	Set, Reset
	Intrusion Keypad Offline	Set, Reset
<b>Intrusion Input</b>	Intrusion Input Alarm	Set, Reset
	Intrusion Input Alarm Event	Set, Reset
	Intrusion Input Bypassed	Set, Reset
	Intrusion Input Detector Dirty	Set, Reset
	Intrusion Input Detector Low Battery	Set, Reset
	Intrusion Input Fault	Set, Reset
	Intrusion Input Holdup at Night	Set, Reset
	Intrusion Input Tamper	Set, Reset
	Intrusion Input Tamper Alarm	Set, Reset
<b>Intrusion Keypad</b>	Intrusion Keypad Bypassed	Set, Reset
	Intrusion Duress Alarm	Set, Reset
	Intrusion Duress	Set, Reset

**Table 74.** Configure Mapped Event fields and descriptions (Continued)

Event Source	Event Type	Condition
	Intrusion Keypad Offline	Set, Reset
	Keypad Tamper Alarm	Set, Reset
	Keypad Tamper	Set, Reset
	Intrusion Keypad Inhibited	Set, Reset
<b>Intrusion Panel</b>	Intrusion Panel Burglar Alarm Cancelled	Set
	Intrusion Panel Code Entered	Set
	Intrusion Panel Duress Code Entered Alarm	Set, Reset
	Intrusion Panel Exit Fault	Set
	Intrusion Panel Offline Alarm	Set, Reset
	Intrusion Panel Tamper Alarm	Set, Reset
	Intrusion Panel Tamper	Set, Reset
<b>Door Access Point</b>	Door Forced Alarm	Set, Reset
	Door Held Alarm	Set, Reset
	Door Prealarm	Set, Reset
	Invalid Badge Alarm	Set
	Lost Badge Alarm	Set
	Suspended Badge Alarm	Set
	Unknown Badge Alarm	Set
	Invalid Badge Event	Invalid Badge
	Valid Badge Event	Valid Badge
<b>Logical Input</b>	Logical Input Alarm	Set, Reset, Tamper

## Actions in Event Action Mapping

Table 75 lists and describes the fields on the Configure Mapped Event page.

**Table 75.** Configure Mapped Action fields and descriptions

Subsystem	Action	Parameter 1	Parameter 2
<b>Access Control</b>		<b>Destination</b>	<b>Duration</b>
	Unlock	Access Point	
	Unlock Duration	Access Point	seconds
	Unlock Permanent	Access Point	
	Lock	Access Point	
	Activate Output		
		<b>Output Destination</b>	<b>Duration</b>
	Activate Output Duration	Output	seconds
	Activate Output with No Reset	Output	
	Reset Output	Output	
		<b>Input Destination</b>	<b>Duration</b>
	Enable Input	Input	
	Disable Input	Input	
		<b>Logical Input Destination</b>	<b>Duration</b>
	Enable Logical Input	Logical Input	
	Disable Logical Input	Logical Input	
<b>Analog Video Switcher</b>		<b>Tag Name</b>	<b>Input Name</b>
	Switch Input to Output	Analog Switcher Tag Name	Input Name
		<b>Output Name</b>	
		Output Name	
<b>Digital Video</b>			
	Video Tagging	Camera	
	Camera Preset	Camera	Preset
	Camera Preset with Video Tagging	Camera	Preset

**Table 75.** Configure Mapped Action fields and descriptions

Subsystem	Action	Parameter 1	Parameter 2
<b>Intercom</b>		<b>Originating Station</b>	<b>Digits To Dial</b>
	Dial Digits	text	text
	Hang up	text	
		<b>Originating Station</b>	<b>Destination Station</b>
	Make Call	text	text
<b>Intrusion</b>		<b>Tag Name</b>	
	Acknowledge Input Alarm	Target Input Name	
	Area Arm	Intrusion Area	
	Start DGP Battery Test	Target DGP Name	DGP Battery Test Time
	Cancel Battery Test	Target DGP Name	
	DGP Bypass	Target DGP Name	
	DGP Unbypass	Target DGP Name	
	Disarm Area	Intrusion Area	
	Input Bypass	Target Input Name	
	Input Unbypass	Target Input Name	
	Intrusion Keypad Bypass	Target Keypad Name	
	Intrusion Keypad Unbypass	Target Keypad Name	
	Set Output	Intrusion Output Name	
	Reset Output	Intrusion Output Name	
	Panel Offline	Target Panel Name	
	Panel Online	Target Panel Name	
<b>Mail</b>		<b>Header</b>	<b>To</b>
	E-mail the Event	text	text
		<b>From</b>	<b>Subject</b>
		text	text





# Chapter 9. Configuring Alarms

This chapter describes how to set up alarms that are generated by Facility Commander. It also describes how to assign alarm colors which apply to Picture Perfect and Facility Commander alarms.



---

**In this chapter:**

[Overview on page 194](#)

[Configuring the Alarm Monitor on page 196](#)

[Setting Alarm Colors on page 197](#)

[Creating Alarm Instructions on page 199](#)

[Creating Alarm Profiles on page 201](#)

## Overview

Alarms are used to notify an operator of specific incidents, such as someone presenting an Invalid Badge at a door or someone forcing a door open. Either one of these events represents an alarm type that may require further investigation.

There can be several sources of alarm conditions — Picture Perfect and Facility Commander. Most of the alarms that are monitored will come from Picture Perfect system.

Facility Commander generates these alarms:

- Access Control System Comm Failure
- Analog Switcher Offline
- Camera Analytics Alarm
- Camera Trouble Alarm
- Motion Detection Alarm
- Video Loss Alarm
- DVR Communications Alarm
- DVR Health Fail Alarm
- DVR Health Trouble Alarm
- Disk Full Alarm
- Intercom Exchange Comm Failure Alarm
- Intercom Exchange Reset Alarm
- Intercom Substation Call Button Alarm
- Intrusion Panel Duress Code Entered Alarm
- Intrusion Panel Main Power Failure Alarm
- Intrusion Panel Offline Alarm
- Intrusion Siren Monitor Failure Alarm
- Intrusion Panel Tamper Alarm
- Intrusion DGP Panel Bypassed
- Intrusion DGP Main Power Failure Alarm
- Intrusion DGP Offline Alarm
- Intrusion DGP Siren Monitor Failure Alarm
- Intrusion DGP Tamper Alarm
- Intrusion Keypad Bypassed Alarm
- Intrusion Duress Alarm
- Intrusion Keypad Offline Alarm
- Intrusion Keypad Tamper Alarm
- Intrusion Area Failed To Arm
- Intrusion Area State Armed and In Alarm
- Intrusion Input Alarm
- Intrusion Input Bypassed Alarm

- Intrusion Input Fault Alarm
- Intrusion Input Tamper Alarm
- Remote Media Server Comm Failure

Alarm instructions for the access control systems are defined in the Picture Perfect system, while alarm instructions for Facility Commander are defined in Facility Commander.

Pre-defined alarm responses are only defined in the access control systems and are available to Picture Perfect and Facility Commander systems.

## Configuring the Alarm Monitor

A system administrator should configure the following items to take advantage of all the Alarm Monitor features. Refer to the following checklist for the server system settings and other configuration settings.

- 
- ✓ To configure Picture Perfect settings, refer to the *Picture Perfect Administration Guide* or Picture Perfect Help for instructions.
    - Alarm instructions are defined using **Messages**.
    - Alarm responses are defined using **Responses**.
    - Alarm priorities are defined using **Alarms**.
- 
- ✓ To configure Facility Commander alarm settings, refer to the following sections or Facility Commander Help:
    - [Setting Alarm Colors on page 197](#)
    - [Creating Alarm Instructions on page 199](#)
- 

## Synchronization

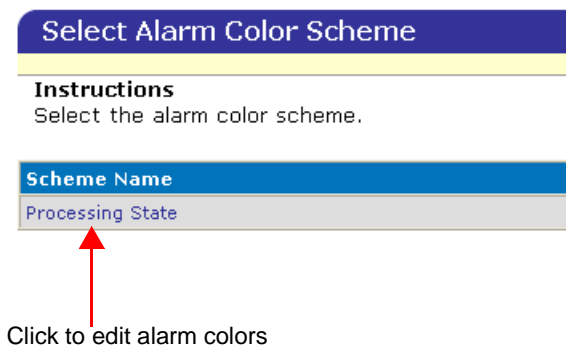
The Alarm Monitor in the access control system and Facility Commander are completely synchronized. This means when an alarm state changes, the change is reflected on both systems and when an operator from either the access control system or Facility Commander responds to an alarm that response is sent to both systems.

## Setting Alarm Colors

The Facility Commander allows you to define alarm colors based on processing state to display alarm events on the Alarm Monitor. Each alarm event appearing on the Alarm Monitor can have a different foreground and background color based on the alarm processing state.

► **To change the alarm colors, follow these steps:**

1. Select **System Administration**.
2. Select **Alarm Colors**. The Select Alarm Color Scheme list page shown in [Figure 129](#) displays.



**Figure 129.** Select Alarm Color Scheme page

3. Click on the alarm color scheme you wish to edit. The Edit Alarm Color Scheme page as shown in [Figure 130](#) displays.

Processing State	Foreground Color	Background Color
Active	yellow	red
Bumped	blue	white
Notified	yellow	green
Remote	red	yellow
Pending	blue	yellow
Completed	white	gray
Removed	black	dark gray
Purged	magenta	orange

**Figure 130.** Edit Alarm Color Scheme page

Table 76 lists and describes the items Select Alarm Color Scheme page.

**Table 76.** Edit Alarm Color Scheme page elements

Field Name	Description
<b>Processing State</b>	<p>The processing state includes: active, bumped, notified, remote, pending, completed, removed, and purged.</p> <p>Use the <b>Selection Colors</b> to define the colors when an alarm is selected on the Alarm Monitor client application.</p> <p>Use <b>Default Colors</b> to define the colors for any alarm event that is not included in the list of alarm processing states.</p>
<b>Foreground Color</b>	<p>This represents the color of the text in the alarm entry displayed on the Alarm Monitor. Use a color definition that is easy to view.</p>
<b>Background Color</b>	<p>This represents the background color of the alarm entry displayed on the Alarm Monitor. Use a color that is compatible with the foreground color so the alarm entry is easy to view.</p>

4. Use the drop-down lists to select the foreground and background colors for each type of alarm event. Use the **Tab** key to move from field to field.
5. When you are finished, click **Submit** to save your changes.

## Creating Alarm Instructions

Use the Configure Alarm Instruction page to copy or delete alarm instruction records.

- **To create custom alarm instructions, follow these steps:**
  1. Select **Device Management**.
  2. Select **Alarm Instructions**. The Alarm Instructions list page shown in [Figure 131](#) displays.













Alarm Instructions

**Instructions**  
View, edit, add or delete alarm instructions.

Search:

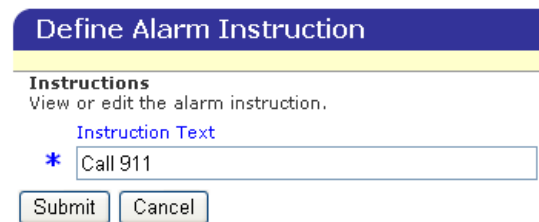
Add Alarm Instruction

◀ Page 1 of 1 ▶    Go to      Items per Page  ▼

		Instruction Text
		Call 911
		call supervisor
		Call the fire department.
		Dispatch all guards
		Evacuate Building
		Notify system administrator

**Figure 131.** Alarm Instructions page

3. Click **Add Alarm Instruction** and the Define Alarm Instruction page shown in [Figure 132](#) displays.



**Define Alarm Instruction**

**Instructions**  
View or edit the alarm instruction.

[Instruction Text](#)

\* Call 911

**Figure 132.** Define Alarm Instruction page

4. Enter between 1-100 characters to create a customized message. This message will display in the Alarm Response window.
5. Click **Submit** to save the record.



## Creating Alarm Profiles

Use the Alarm Profiles page to view, import, copy, add, and delete alarm profile records.

► **To view the alarm profiles, follow these steps:**

1. Select **Device Management**, and then **Alarm Profiles**. The Alarm Profiles page shown in [Figure 133](#) displays.

**Alarm Profiles**

**Instructions**  
View, edit, add or delete alarm profiles.

Search:

◀ Page 1 of 1 ▶ Go to   Items per Page

	Tag Name	Description	Priority
	DVR Comm Failure	DVR comm failure	5
	Emergency Procedures	Use when emergency occurs inside building.	50
	External Access System Comm Failure	PP server failure	10
	Motion Detection Alarm	Motion detection alarm	1
	Remote Media Server Comm Failure	Remote media server comm failure	50
	Video Loss Alarm	Video loss alarm	5

**Figure 133.** Alarm Profiles

## Adding an Alarm Profile

► To add an alarm profile, follow these steps:

1. Click **Add Alarm Profile** on the Alarm Profiles page. The Define Alarm Profile page shown in [Figure 134](#) displays.

**Define Alarm Profile**

**Instructions**  
View or edit the alarm profile. Select the instructions to be displayed in the alarm response window.

**Alarm Profile Information**

**Tag Name**  
\* Emergency Procedures

**Description**  
Use when emergency occurs inside building.

**Priority**  
\* 50

**Alarm Instructions**

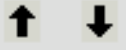
Available Instructions	Selected Instructions
Call 911 call supervisor Call the fire department. Dispatch all guards Evacuate Building Notify system administrator	

**Figure 134.** Define Alarm Profile

2. Enter the information described in described in [Table 77](#). A check mark indicates a required field.
3. Click **Submit** to save the record.

[Table 77 on page 203](#) lists and describes the fields in the Define Alarm Profile page. A check mark indicates a required field

**Table 77.** Define Alarm Profile fields and descriptions

Element	REQ	Description
Tag Name	✓	Enter a unique name to identify this profile. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Priority	✓	Identify the priority from 1-to-500. One is the highest priority.
Add/Add All		Use these buttons to add instructions to the profile.
Remove/Remove All		Use these buttons to remove instructions to the profile.
		Use the up and down arrow icons to change the sequence of the instructions that display in the Alarm Response window.



## Chapter 10. Using the Alarm Monitor

This chapter introduces the Facility Commander Alarm Monitor and describes its features. It also describes how to use the Alarm Monitor to display different time zones. The Alarm Monitor displays icons indicating video clips and site maps are available.



---

### **In this chapter:**

[Overview on page 206](#)

[Alarm Alert on page 207](#)

[Navigating the Alarm Monitor on page 208](#)

[Customizing the Alarm Monitor on page 211](#)

[Changing Window Name and Contents on page 211](#)

[Launch Video Automatically on page 214](#)

[Responding to Alarms on page 215](#)

## Overview

The Alarm Monitor is a multi-functional client application that allows you to view alarm events. The Alarm Monitor displays alarm events as a single transaction which is updated when the status of the alarm changes.

The Alarm Monitor allows an operator to:

- View alarms in colors you select.
- Launch the Video Console to view live and recorded video.
- Launch the Graphics Display to view the alarm point on a graphic display, issue commands to lock and unlock doors, and more.
- Acknowledge an alarm with a text message or use a predefined message.

If configured to do so, the Alarm Monitor window displays indicators representing video clips and site maps associated with the alarm event.

The Alarm Monitor displays incoming alarms with indicators, priority, operator time, alarm description, location, alarm state, input state, processing state, and count.

A status bar displays the number of total alarms, unacknowledged alarms, and the highest priority. The status bar also displays a server connection icon to monitor connection to the Facility Commander server.

## Automatically Launch Video Console by Alarm Priority

In addition, you can configure Facility Commander to automatically launch a Video Console when an alarm event occurs with associated video. Each time an alarm event occurs within the specified priority range, the Video Console launches and displays both live video and the recorded video clip of the event.

To configure:

- Use the Configure System Parameters page to identify the priority range, which determines when the Video Console launches automatically. Refer to [System Parameters on page 50](#) for more information.
  - The priority range is from 1-to-500. Every alarm in the specified priority level causes the Video Console to launch. If a range is not specified, the Video Console does not automatically launch.
- Use Event Action Mapping to associate the alarm event and video tagging instructions, which include camera presets, camera preset with video tagging, and video tagging. Refer to [Tagging Video Events for Access Points on page 182](#) for more information.
- Identify the workstations where you want the Video Console to launch automatically when an alarm event occurs. Refer to [Workstations on page 45](#) for more information.
- Open the Alarm Monitor to display alarm activity. If the Alarm Monitor is not opened, the Video Console does not automatically launch.

## Alarm Alert

The Alarm Alert window shown in [Figure 135](#) displays on the client workstation when an alarm event occurs and cannot be closed. However, the Alarm Alert window displays only when there are alarms; if the total number of alarms equals zero, the window does not display.

The Alarm Alert window displays a count of all the alarms in an operator's context. The window filter does not filter any alarms in this window, so all alarms that the operator can view are included in the alarm count.

To configure the Alarm Alert, refer to [Workstations on page 45](#) for more information.



**Figure 135.** Alarm Alert window

Refer to [Table 78](#) for a description of the Alarm Alert window.

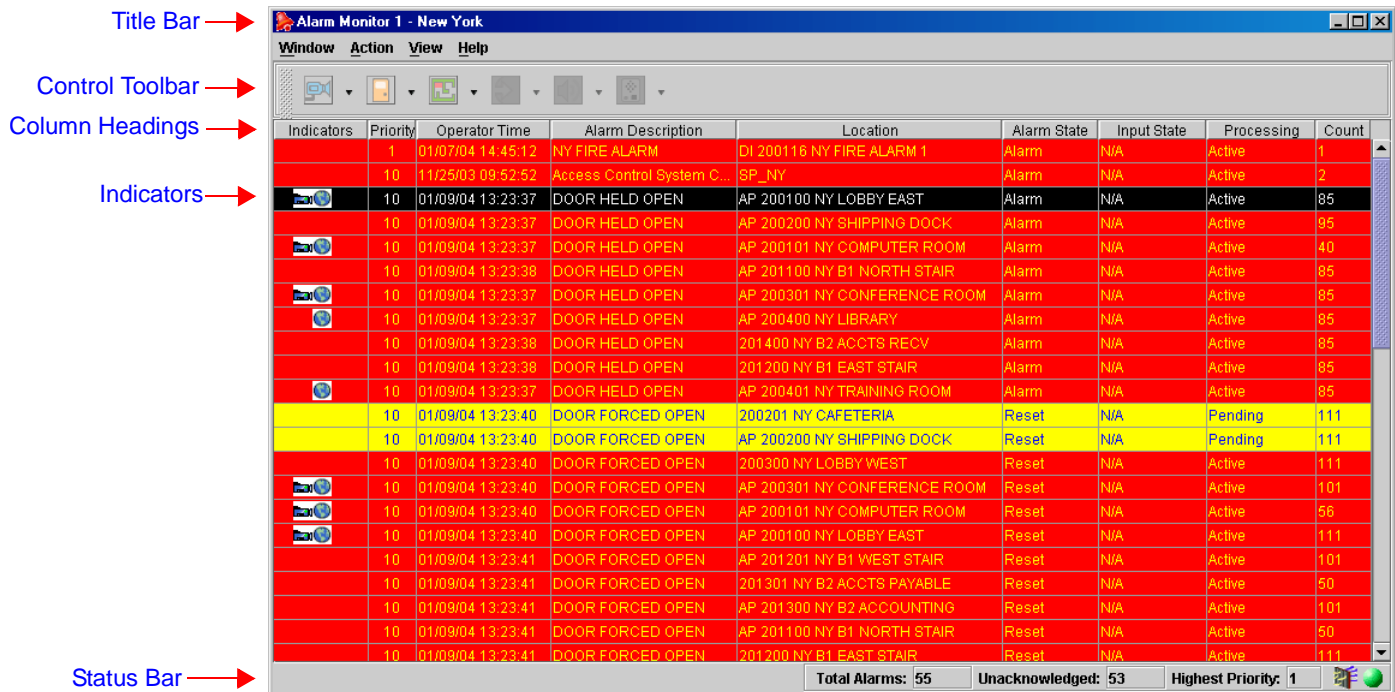
**Table 78.** Alarm Alert descriptions

Information	Description
<b>Active Alarms</b>	Displays a count of the active alarms. When the number of active alarms equals zero, the Alarm Alert window will be gray. The window is red when alarms are present.
<b>Total Alarms</b>	Displays a count of the total number of alarms.
<b>Highest Priority</b>	Displays the number of the highest priority alarm.
<b>Silence</b>	Click <b>Silence</b> to stop the sound.

## Navigating the Alarm Monitor

➤ To open the Alarm Monitor, follow these steps:

1. Launch the Facility Commander Launcher window, select **Launch** and **Alarm Monitor**, or select the **Alarm Monitor** icon from the **Viewers** toolbar.
2. The Alarm Monitor shown in [Figure 136](#) displays.



**Figure 136.** Alarm Monitor window









[Table 79](#) lists and describes the elements on the Alarm Monitor interface.

**Table 79.** Alarm Monitor descriptions

Element	Description
<b>Alarm Monitor Interface</b>	
<b>Title Bar</b>	<p>Displays Alarm Monitor, window instance number, and custom window title.</p> <ul style="list-style-type: none"> <li>Refer to <a href="#">Managing Multiple Windows on page 20</a> for more information about window instance numbers.</li> <li>Refer to <a href="#">Changing Window Name and Contents on page 211</a> for instructions to add window titles.</li> </ul>



**Table 79.** Alarm Monitor descriptions (Continued)

Element	Description
<b>Control Toolbar</b>	<p>The Control Toolbar displays buttons with icons for each type of device that can be selected, which includes cameras, intercom stations, access points, graphic displays, inputs, and outputs. Icons on the Control Toolbar are dimmed when not available.</p> <hr/> <div>  <b>Video Console.</b> The default action is view live and recorded video. </div> <hr/> <div>  <b>Access Point.</b> The default action is momentary unlock. </div> <hr/> <div>  <b>Graphic Viewer.</b> The default action is view the associated graphic display. </div> <hr/> <div>  <b>Inputs.</b> No default action. </div> <hr/> <div>  <b>Outputs.</b> No default action. </div> <hr/> <div>  <b>Intercom.</b> The default action is connect. </div> <hr/> <div>  <b>Intrusion Areas.</b> The default action is connect. </div> <hr/> <div>  <b>Intrusion Inputs.</b> The default action is connect. </div> <hr/> <p>Each button is made up of two parts — the button with icon, and a drop-down list with all the actions that are available to the operator. When a button is enabled, a tooltip identifies the default action.</p> <p>Actions appearing on the drop-down list may be dimmed if the action does not apply to the current device or if the operator does not have permission to take the action.</p>
<b>Column Headings</b>	<p>Columns cannot be moved, however, you can resize the columns to make them larger or smaller. Select the column edge and drag until the column is the correct size.</p>
<b>Indicators</b>	<p>Displays an X to indicate communication has been lost with the Picture Perfect server.</p> <p>Displays a camera and a globe icon indicating a video clip and a graphic display are available, if configured to do so.</p> <ul style="list-style-type: none"> <li>Click the camera icon to launch the Video Console.</li> <li>Click the globe icon to launch the Graphics Viewer.</li> </ul> <p>Refer to Event Mapping for information about associating video with alarm events. Refer to <a href="#">Using the Graphics Editor on page 301</a> for information about creating site maps.</p>

**Table 79.** Alarm Monitor descriptions (Continued)

Element	Description
<b>Input State</b>	<ul style="list-style-type: none"> <li>• Open indicates the input device is open.</li> <li>• Close indicates the input device is closed.</li> <li>• Cut indicates the line has been cut.</li> <li>• Short indicates the line is shorted.</li> <li>• N/A indicates the field does not apply to the alarm.</li> </ul>
<b>Processing</b>	<p>Displays the following operator processing states:</p> <ul style="list-style-type: none"> <li>• <b>Active:</b> the alarm has not been acknowledged by an operator.</li> <li>• <b>Pending:</b> the alarm has been acknowledged by an operator but not removed.</li> <li>• <b>Completed:</b> the alarm has been removed but the alarm input is waiting for a physical reset.</li> <li>• <b>Purged:</b> the alarm has been removed but the alarm input is waiting for a physical reset.</li> <li>• <b>Bumped:</b> the alarm has not been acknowledged within a specified time and has been sent to one or more specified Picture Perfect workstations.</li> <li>• <b>Notified:</b> used by Network Alarm Notification (NAN) in a Picture Perfect Enterprise system. alarms that are received by the alarm monitor (on a subhost), but are not acknowledged in a defined amount of time, and are forwarded (through a login window) to a pre-defined terminal on the network host.</li> <li>• <b>Remote Notified:</b> used by Remote Alarm Notification (RAN).</li> </ul> <p>Refer to the <i>Picture Perfect Administration Guide</i> for more information.</p>
<b>Count</b>	Displays number of times the alarm has been set and reset.
<b>Status Bar</b>	
<b>Total Alarms</b>	Displays the total number of alarms received. This includes alarms generated by the access control system and Facility Commander.
<b>Unacknowledged</b>	Displays the total number of alarms that are unacknowledged.
<b>Highest Priority</b>	Displays the highest priority number of the alarms. The alarm priority is defined in Picture Perfect.
<b>Window Filter Icon</b>	<p>Displays an icon indicating the operator has reduced the number of facilities in their view. When all of the facilities are selected, the icon no longer displays on the status bar.</p> <p>Refer to <a href="#">Changing Window Name and Contents on page 211</a> for instructions to add window titles.</p>

**Table 79.** Alarm Monitor descriptions (Continued)

Element	Description
<b>Server Connection Indicator</b>	<p>Displays an icon indicating if the system with the Alarm Monitor is connected to the Facility Commander server.</p> <ul style="list-style-type: none"> <li>• Green indicates the system is communicating with the server.</li> <li>• Red indicates the system is no longer communicating with the Facility Commander server.</li> </ul>

## Customizing the Alarm Monitor

The Alarm Monitor displays a window title, multiple time zones, and can be configured to automatically launch a Video Console. For more information, refer to the following sections:

- [Changing Window Name and Contents](#)
- [Display Multiple Time Zones](#)
- [Launch Video Automatically on page 214](#)

### Changing Window Name and Contents

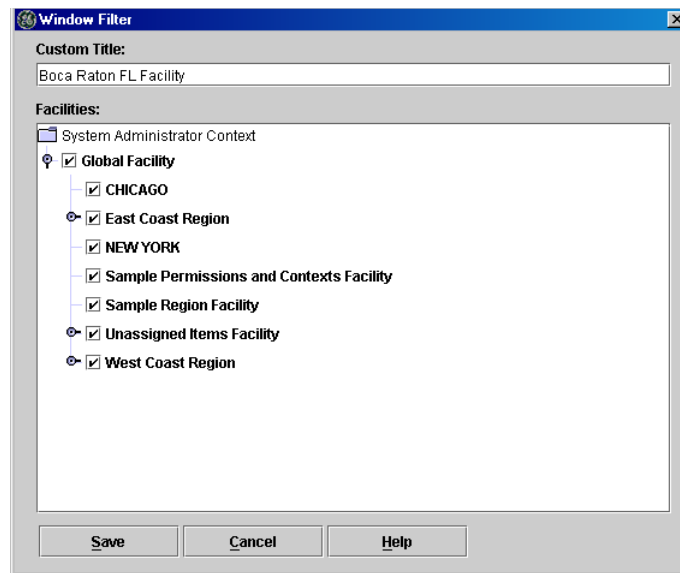
Use the **Window Filter** shown in [Figure 137](#) to modify the current display of items in the navigation pane; allowing an operator to view specific records, such as those from New York and not from Boston or Chicago.

When an operator does not have permission to modify the items in the window filter, the items are disabled. The operator is able to view the items displayed in the window, but not able to make any selections.

➤ **To filter items from view in the client applications, follow these steps:**

1. From the **View** menu, select **Window Filter**. The Window Filter

window in [Figure 137](#) displays.



**Figure 137.** Window Filter window

2. Use the **Custom Title** field to identify a title to display on the Video Console title bar. Maximum number of characters is 256.
3. Select the check boxes to indicate the items you want to display in the client applications. A check mark indicates the item is selected. Clear the check boxes to remove the items from view.
4. Click **Save**. The Alarm Monitor displays a window filter icon in the status bar indicating the operator has reduced the number of facilities in their view.

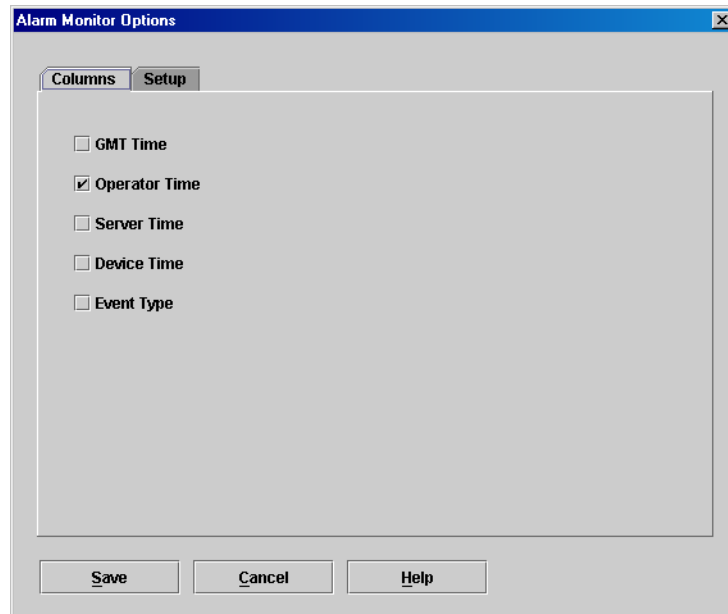
## Display Multiple Time Zones

The Alarm Monitor can display up to four columns of time zones, which include GMT, operator, server, and device. The device time zone represents the time zone of the devices associated with the alarm event.

### ► To change time zones, follow these steps:

1. From the **View** menu, select **Options**. The Alarm Monitor Options

window shown in [Figure 138](#) displays.



**Figure 138.** Alarm Monitor Options window — Columns tab

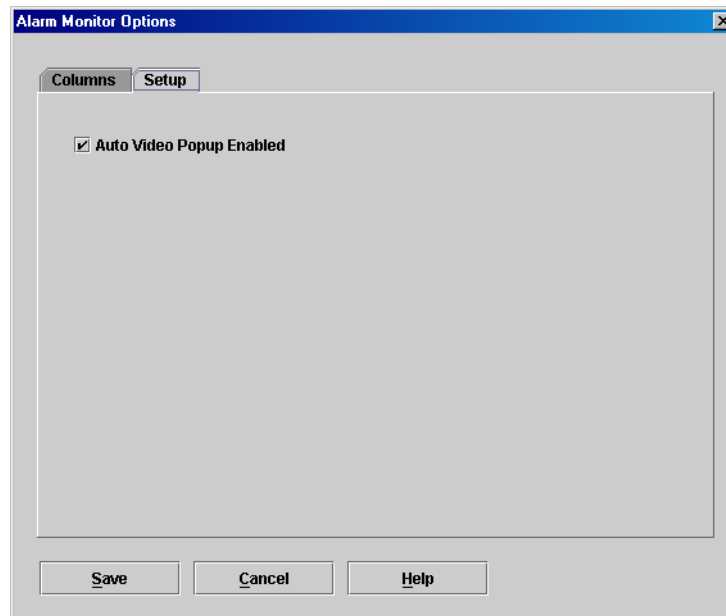
2. On the **Columns** tab page, select the check boxes indicating which time zones to display on the Alarm Monitor. A check mark indicates the item is selected. Clear the check boxes to remove the column.
3. Click **Save**. If you decide not to make any changes, click **Cancel**.

**Table 80.** Monitor Options description

Field Name	Description
<b>GMT Time</b>	Displays Greenwich Mean Time. This is the default setting.
<b>Operator Time</b>	Displays the time for the operator's location.
<b>Server Time</b>	Displays the time for the server's location. This may be different from the Operator or Device time.
<b>Device Time</b>	Displays the time for the device's location.
<b>Event Type</b>	Displays the event type general category.

## Launch Video Automatically

- To automatically launch the video popup window, follow these steps:
  1. From the **View** menu, select **Options**. The Alarm Monitor Options window as shown in [Figure 139](#) displays.



**Figure 139.** Alarm Monitor Options window — Setup tab

2. Select the **Setup** tab page and select the **Auto Video Popup Enabled** check box to automatically launch a Video Console window.
  - Clear the check box if you do not want a Video Console window to launch when an alarm is generated.
  - If you are unable to change the setting, refer to [Auto Alarm Video Popup Priority Range on page 51](#) or verify the operator's permissions setting.
3. Click **Save**.

## Responding to Alarms

The Alarm Monitor window allows operators to respond to incoming alarms by using the Alarm Response window shown in [Figure 140 on page 216](#). An operator launches the Alarm Response Window by double-clicking the alarm on the Alarm Monitor or selecting Acknowledge from the Actions menu.

Using the Alarm Response window, an operator can acknowledge, remove, or purge an alarm.

- Instructions for alarms are generated by and retrieved from the access control systems.
- If there are multiple Picture Perfect systems, the appropriate system supplies the instructions for the alarms.

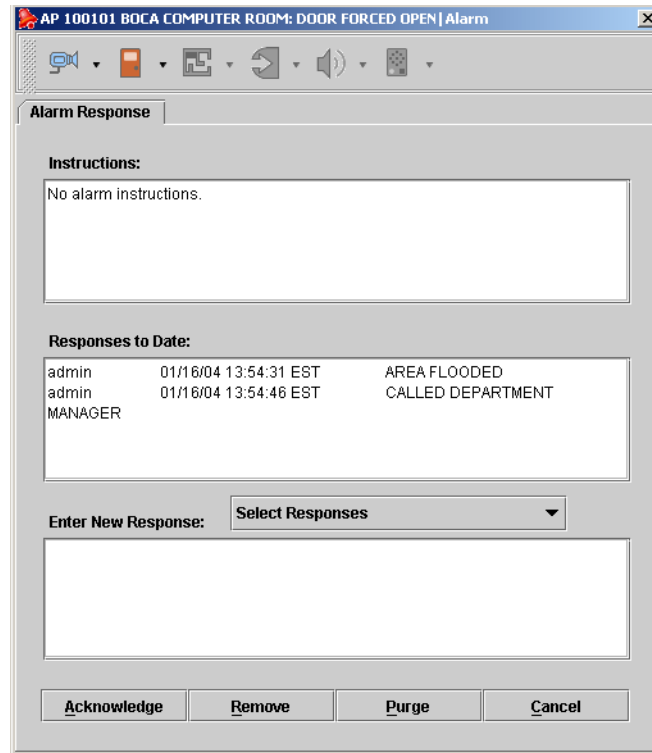
Operators can select a pre-defined alarm response or type a response in the Alarm Response window.

### Alarm Response Required

Depending on the system parameters, an operator can be required to enter a response before removing an alarm.

An alarm priority range is identified and any time an alarm event occurs within the range, an operator will be required to enter a response. If a priority range is not specified, alarms can be acknowledged without entering a response in the Alarm Response window.

If the operator does not enter the required response, the Remove and Purge alarm action will be ignored until a response is provided.



**Figure 140.** Alarm Response window

[Table 81](#) lists and describes the elements in the Alarm Response window.

**Table 81.** Alarm Response elements and descriptions

Element	Description
<b>Title Bar</b>	Displays alarm source, type, and a custom window title, if configured to do so.
<b>Control Toolbar</b>	Use the to issue commands, such as the default action or access the action menu. Refer to <a href="#">Control Toolbar on page 209</a> for more information.
<b>Instructions</b>	<p>Displays alarm instructions, such as who to call or who to dispatch to the area.</p> <ul style="list-style-type: none"> <li>Alarm instructions for Picture Perfect generated alarms are defined in the source system. Up to five messages can be assigned to each alarm.</li> <li>Alarm instructions for Facility Commander generated alarms are defined in Facility Commander.</li> </ul>
<b>Responses to Date</b>	Displays all the responses to the alarm event up to the current time. The operator's user name, the date and time of the response, and the response text displays.
<b>Enter New Response</b>	Use to enter a custom text response. Use up to 255 characters. Avoid using quote marks (") in the text, as this character is not recognized by Picture Perfect.



**Table 81.** Alarm Response elements and descriptions (Continued)

Element	Description
<b>Buttons</b>	
<b>Acknowledge</b>	Click <b>Acknowledge</b> after entering a response. The alarm remains on the Alarm Monitor and processing state changes from Active to Pending.
<b>Remove</b>	Click <b>Remove</b> when all the responses have been recorded and the alarm is no longer being investigated. The processing state changes to Completed. The alarm is not removed from the Alarm Monitor until the alarm is reset. If the alarm is not reset, it will continue to display.
<b>Purge</b>	Click <b>Purge</b> to remove the alarm from the Alarm Monitor, regardless of the alarm state. The action is allowed only if you have the correct permissions. Contact your system administrator to make changes.
<b>Cancel</b>	Click <b>Cancel</b> to return to the Alarm Monitor window.



# Chapter 11. Using the Event Monitor

This chapter introduces the Facility Commander Event Monitor and describes its features. It also describes how to use the Event Monitor to display different time zones and event types. the Event Monitor displays icons indicating video clips and site plans are available.



---

## **In this chapter:**

[Overview on page 220](#)

[Navigating the Event Monitor on page 220](#)

[Setting Event Monitor Options on page 226](#)

[Changing the Event Types Filter on page 227](#)

[Customizing Window Name and Contents on page 230](#)

## Overview

The Event Monitor is a multi-functional client application that allows you to view alarm, badge, and system events. On the Event Monitor, alarm events (alarms and resets) are displayed as individual transactions. In contrast, the Alarm Monitor displays alarm events as a single transaction which is updated when the the status of the alarm changes.

Column headings change depending on the type of event. The Event Monitor always displays Indicators, Device Time, Event Type, Description, and Location. Refer to the following sections for a description of the column headings:

- [Alarm Events List on page 223](#)
- [Badge Events List on page 224](#)
- [System Events List on page 225](#)

New events appear at the bottom of a scrollable list. Only the last 1000 events appear on the list, after which the oldest events are removed.

## Navigating the Event Monitor

➤ **To open the Event Monitor, follow these steps:**

1. Launch the Facility Commander Launcher window, select **Launch** and **Event Monitor**, or select the **Event Monitor** icon from the **Viewers** toolbar.
2. The Event Monitor shown in [Figure 141 on page 221](#) displays.

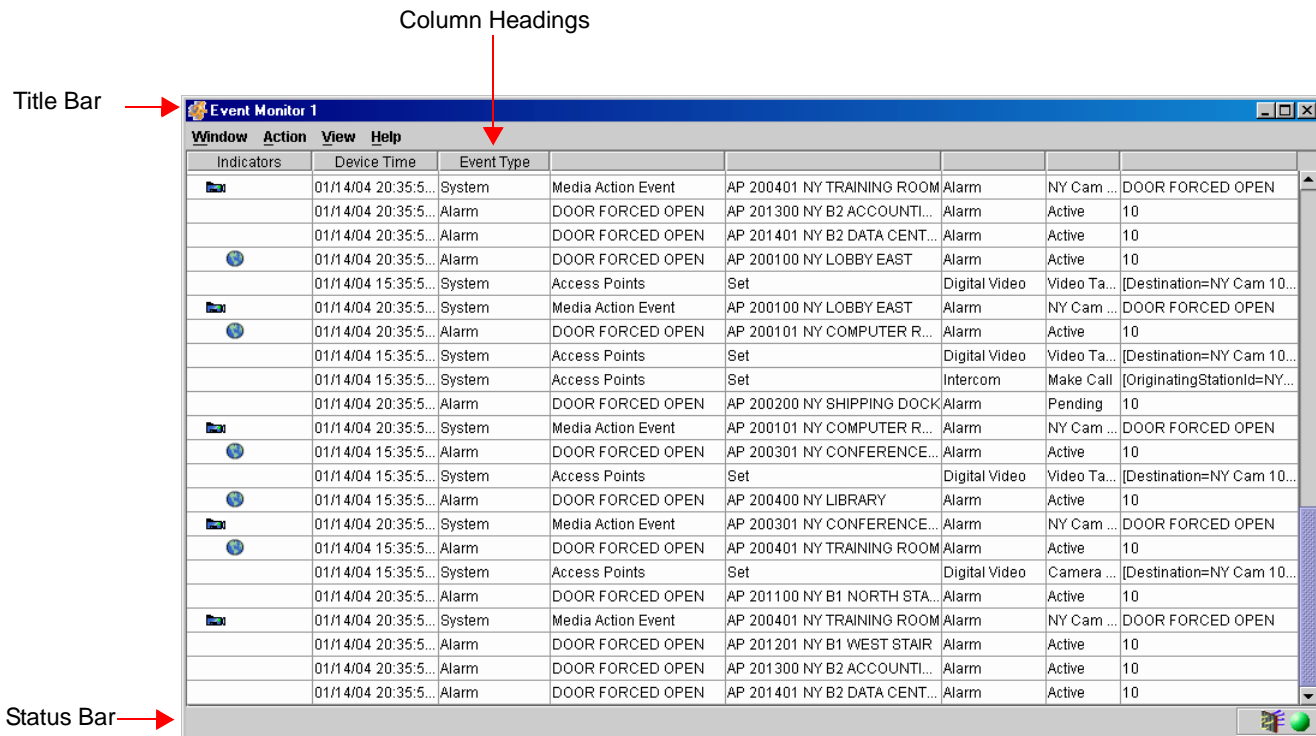


Figure 141. Event Monitor window

Table 82 lists and describes the elements on the Event Monitor interface.

Table 82. Event Monitor description

Element	Description
<b>Title Bar</b>	Displays the title Event Monitor and the window instance number, since you may open more than one occurrence of the Event Monitor. Refer to <a href="#">Managing Multiple Windows on page 20</a> for more information.
<b>Indicators</b>	<p>Displays icons representing site maps and video associated with the alarm event.</p> <ul style="list-style-type: none"> <li>Displays an X to indicate communication with the Picture Perfect server has been lost.</li> <li>Click the globe icon to launch the Graphics Viewer displaying the default site plan. Refer to <a href="#">Editing Access Points on page 76</a> for information about associating a site plan to an alarm event.</li> <li>Click the camera icon to launch the Video Console. The most recent video clip displays.</li> </ul>

**Table 82.** Event Monitor description

Element	Description
<b>Device Time</b>	<p>View the time an event occurred in one or more of the following four time stamps:</p> <ul style="list-style-type: none"> <li>• GMT: Greenwich Mean Time.</li> <li>• Operator (Default): location of the operator.</li> <li>• Server: location of the server.</li> <li>• Device: location of the device associated with the event.</li> </ul> <p>The format is month, day, year, hour, minute, and seconds (mm/dd/yy hh:mm:ss). For example: 12/10/02 16:28:04. The date format may change depending on the operator's locale.</p>
<b>Mapped Event Types</b>	<p>There are three types of events: alarm, badge, and system. Refer to the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Alarm Events List on page 223</a></li> <li>• <a href="#">Badge Events List on page 224</a></li> <li>• <a href="#">System Events List on page 225</a></li> </ul>
<b>Description</b>	Description of the event.
<b>Status Bar</b>	
<b>Window Filter Icon</b>	<p>Displays an icon indicating the list of available Facility Commander facilities has changed. When the facilities have been reset, the icon no longer displays on the status bar.</p> <p>Refer to <a href="#">Customizing Window Name and Contents on page 230</a> for instructions to add window titles.</p>
<b>Server Connection Indicator</b>	<p>Displays an icon indicating if the system with the Event Monitor is connected to the Facility Commander server.</p> <ul style="list-style-type: none"> <li>• Green indicates the system is communicating with the server.</li> <li>• Red indicates the system is no longer communicating with the Facility Commander server.</li> </ul>

## Alarm Events List

Refer to [Table 83](#) for a description of the column headings that display for alarm events.

**Table 83.** Event Monitor Alarm Events description

Element		Description
<b>Alarm State</b>		
	<b>Alarm</b>	Alarm point is in an active state.
	<b>Reset</b>	Alarm point has been reset.
	<b>Tamper</b>	The wiring to the alarm point has either been cut or shorted.
<b>Processing</b>		
	<b>Active</b>	The alarm has not been acknowledged by an operator.
	<b>Pending</b>	The alarm has been acknowledged by an operator but not removed.
	<b>Completed</b>	The alarm has been removed but the alarm input is waiting for a physical reset.
	<b>Purged</b>	The alarm has been removed but the alarm input is waiting for a physical reset.
	<b>Bumped</b>	The alarm has not been acknowledged within a specified time and has been sent to one or more specified Picture Perfect workstations.
	<b>Notified</b>	Used by Network Alarm Notification (NAN) in a Picture Perfect Enterprise system. alarms that are received by the alarm monitor (on a subhost), but are not acknowledged in a defined amount of time, and are forwarded (through a login window) to a pre-defined terminal on the network host.
	<b>Remote Notified</b>	Used by Remote Alarm Notification (RAN).
<b>Priority</b>		
	<b>Alarm</b>	Displays a value only when the event type is alarm. The range is 1 to 500. Alarms with a priority of one have the highest priority.

## Badge Events List

Refer to [Table 84](#) for a description of the column headings that display for badge events.

**Table 84.** Event Monitor Badge Events description

Element	Description
<b>First Name</b>	Displays the first name of the badgeholder.
<b>Last Name</b>	Displays the last name of the badgeholder.
<b>Employee Number</b>	Displays the employee number of the badgeholder.



## System Events List

Refer to [Table 85](#) for a description of the column headings that display for system events.

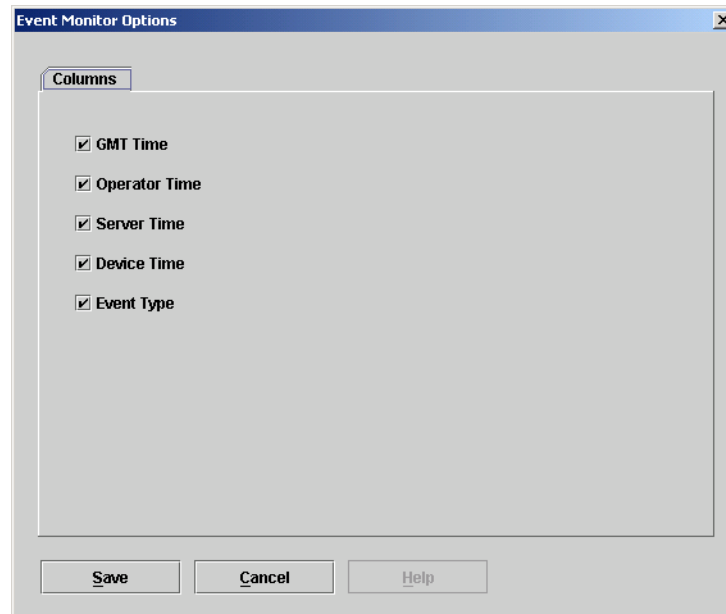
**Table 85.** Event Monitor System Events description

Element		Description
<b>Video</b>		
	<b>Mapped Event Location</b>	Displays the location of the event
	<b>Mapped Event State</b>	Displays the event state.
	<b>Video Token ID</b>	Displays the video token ID associated with the recorded video clip.
<b>Intercom</b>		
	<b>From Extension</b>	Enter the intercom extension number. Refer to <a href="#">Adding Intercom Stations on page 241</a> for more information.
	<b>Station Description</b>	Enter the intercom station description. Refer to <a href="#">Adding Intercom Stations on page 241</a> for more information.
	<b>To Extension</b>	Enter the intercom extension number to be dialed.
	<b>Station Description</b>	Enter the intercom extension number of the station being dialed.

## Setting Event Monitor Options

► To set the options, follow these steps:

1. From the **View** menu, select **Options**. The Event Monitor Options window in [Figure 142](#) displays.



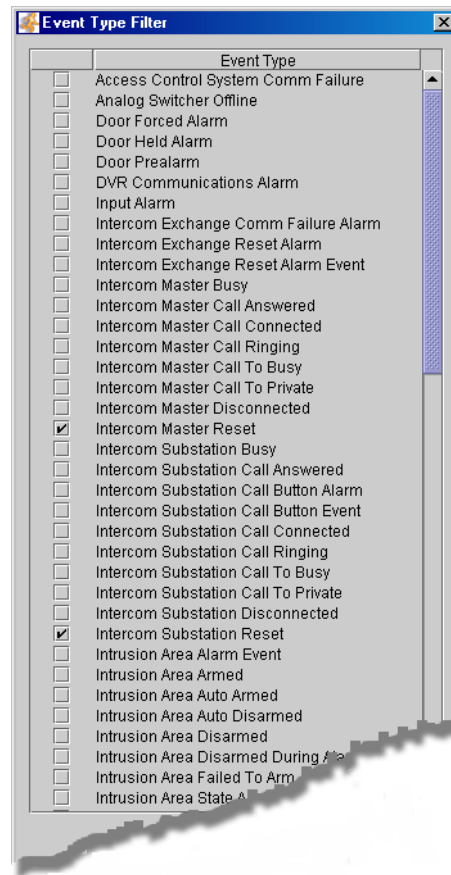
**Figure 142.** Event Monitor Options window

2. Select the check boxes to indicate the time stamps you want to display on the Event Monitor. The default setting is all check boxes are selected. A check mark indicates the time stamp is selected.
  - Clear the check boxes to remove the time stamp from view.
3. Select the check box to display the column on the Event Monitor.
4. Click **Save**.

## Changing the Event Types Filter

► To filter the event types from view, follow these steps:

1. From the **View** menu, select **Event Type Filter**. The Event Monitor Filter window in [Figure 143](#) displays.



**Figure 143.** Event Type Filter

2. Select the check boxes to indicate the event types you want to display on the Event Monitor. A check mark indicates the event type is selected. Refer to [Table 86 on page 228](#) for a complete list of event types.
  - Clear the check boxes to remove the event types from view.
3. Click **OK**.

## Event Types List

Table 86 lists the event types that display on the Event Monitor.

**Table 86.** Event Monitor Event Types

Event Types	Event Types
Access Control Comm Failure	Intercom Substation Reset
Analog Switcher Offline	Intrusion Area Alarm Event
Door Forced Alarm	Intrusion Area Armed
Door Held Alarm	Intrusion Area Auto Disarmed
Door Prealarm	Intrusion Area Disarmed During Alarm
DVR Communications Alarm	Intrusion Area Failed To Arm
Input Alarm	Intrusion Area State Armed All Clear
Intercom Exchange Comm Failure Alarm	Intrusion Area Armed and In Alarm
Intercom Exchange Reset Alarm	Intrusion Area Armed and In Alarm Event
Intercom Exchange Reset Alarm Event	Intrusion Area State Disarmed
Intercom Master Busy	Intrusion Area Unknown
Intercom Master Call Answered	Intrusion Battery Test Failure
Intercom Master Call Connected	Intrusion Battery Test Finish
Intercom Master Call Ringing	Intrusion Battery Test Start
Intercom Master Call To Busy	Intrusion DGP Main Power Failure Alarm
Intercom Master Call To Private	Intrusion DGP Offline Alarm
Intercom Master Call Disconnected	Intrusion DGP Siren Monitor Failure Alarm
Intercom Master Reset	Intrusion DGP Tamper Alarm
Intercom Substation Busy	Intrusion Input Alarm
Intercom Substation Call Answered	Intrusion Input Alarm Event
Intercom Substation Call Button Alarm	Intrusion Input Bypassed
Intercom Substation Call Button Alarm Event	Intrusion Input Bypassed Alarm
Intercom Substation Call Connected	Intrusion Input Detector Dirty
Intercom Substation Call Ringing	Intrusion Input Detector Low Battery
Intercom Substation Call To Busy	Intrusion Input Detector Supervision

**Table 86.** Event Monitor Event Types (Continued)

Event Types	Event Types
Intercom Substation Call To Private	Intrusion Input Fault
Intercom Substation Disconnected	Intrusion Input Fault Alarm
Intrusion Input Holdup At Night	Intrusion Input Holdup At Night
Intrusion Input Tamper	Intrusion Input Tamper
Intrusion Input Tamper Alarm	Intrusion Input Tamper Alarm
Intrusion Keypad Bypassed Alarm	Invalid Badge Event
Intrusion Keypad Offline Alarm	Logical Input Alarm
Intrusion Keypad Tamper Alarm	Intrusion Input Tamper Alarm
Intrusion Low Panel Battery	Lost Badge Alarm
Intrusion Panel Burglar Alarm Cancelled	Mapped Event Action Audit
Intrusion Panel Code Entered	Media Action Event
Intrusion Panel Exit Fault	Motion Detection Alarm
Intrusion Panel Main Power Failure	Reader Supervised Exit Alarm
Intrusion Panel Main Power Failure Alarm	Remote Media Server Comm Failure
Intrusion Panel Offline Alarm	Lost Badge Alarm
Intrusion Panel Tamper	Supervised Reader Alarm
Intrusion Panel Tamper Alarm	Suspended Badge Alarm
Intrusion Siren Monitor Failure	Table Rollover Event
Intrusion Siren Monitor Failure Alarm	Unknown Badge Alarm
Invalid Badge Alarm	Valid Badge Event
Intrusion Input Holdup At Night	Video Loss Alarm
Intrusion Input Tamper	Supervised Reader Alarm
	Suspended Badge Alarm

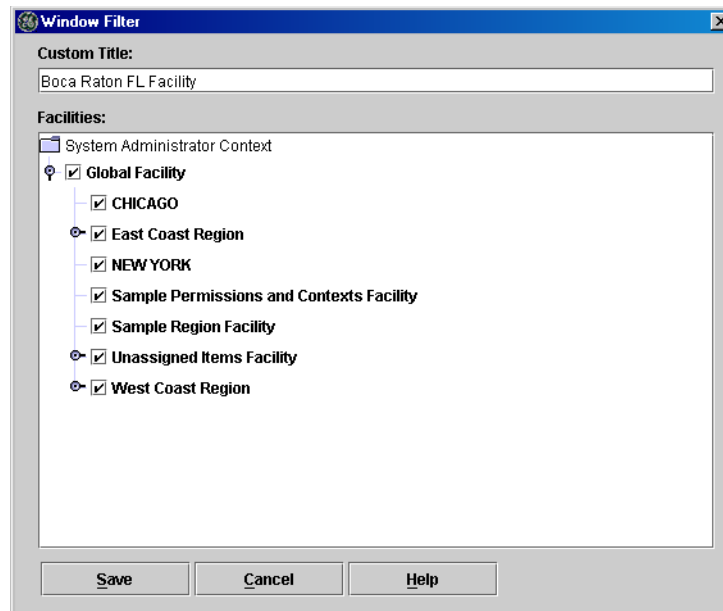
## Customizing Window Name and Contents

Use the **Window Filter** shown in [Figure 144](#) to modify the current display of items displayed in the navigation pane; allowing an operator to view specific records, such as those from New York and not from Boston or Chicago.

When an operator does not have permission to modify the items in the **Window Filter**, the items are disabled. The operator is able to view the items displayed in the window, but is not able to make any selections.

► **To filter items from view in the navigation pane, follow these steps:**

1. From the **View** menu, select **Window Filter**. The window filter in [Figure 144](#) displays.



**Figure 144.** Window Filter window

2. Use the **Custom Title** field to identify a title to display on the Video Console title bar. Maximum number of characters is 256.
3. Select the check boxes to indicate the items you want to display in the navigation pane of the client application. A check mark indicates the item is selected.
  - Clear the check boxes to remove the items from view.
4. Click **Save**. The Event Monitor displays a window filter icon in the status bar indicating the list of items has changed

## Chapter 12. Configuring Intercom Devices

This chapter describes how to configure intercom exchanges and intercom stations.

Readers should be knowledgeable about hardware configuration for the intercom equipment. Refer to the vendor's documentation for instructions to install and configure the equipment.



---

**In this chapter:**

[Overview on page 232](#)

[Configuring Intercom Exchanges on page 233](#)

[Configuring Intercom Stations on page 240](#)

[Tips for Creating Symbol Schemes on page 246](#)

## Overview

The intercom feature in Facility Commander allows operators to connect calls from substations to master stations. Using the Graphics Viewer, operators can view intercom call station events on graphic displays.

## Terminology

Facility Commander uses these terms to describe intercom devices:

<b>Exchange</b>	Intercom hardware, which is typically located in the control center and serves as a switch to physically connected devices.
<b>Master Station</b>	Intercom which is typically located at an operator's workstation. The master station has a keypad.
<b>Substation</b>	Intercom which is typically located at door entrances. The substation has a button, which is used to communicate, but does not have a keypad.

## Checklist

A system administrator should use the checklist below to implement the intercom feature in Facility Commander.

✓	Configure the intercom exchange. Refer to <a href="#">Adding an Intercom Exchange on page 234</a> for more information.
✓	Configure intercom stations. Refer to <a href="#">Adding Intercom Stations on page 241</a> for more information.
✓	Create a symbol scheme with intercom devices to use on a graphic display. Refer to <a href="#">Creating Symbol Schemes on page 285</a> for more information.
✓	Create a graphic display and place symbols representing intercom devices. Refer to <a href="#">Creating Graphic Displays on page 299</a> for more information.



## Configuring Intercom Exchanges

Use the Intercom Exchanges page to add, edit, copy, and delete intercom exchange records. Refer to the following sections for instructions:

- [Viewing Intercom Exchanges on page 233](#)
- [Adding an Intercom Exchange on page 234](#)

### Viewing Intercom Exchanges

► **To view intercom exchange records, follow these steps:**

1. Select **Device Management**.
2. Select **Intercom Exchanges**. The Intercom Exchanges page shown in [Figure 145 on page 233](#) displays.

Tag Name	Description	Reference ID	IP Address or Host Name	Exchange Number
AlphaCom Exchange	NY Intercom Exchange		3.18.100.1	6000

**Figure 145.** Intercom Exchanges page

## Adding an Intercom Exchange

- To add an intercom exchange, follow these steps:
1. Select **Device Management**, and then **Intercom Exchanges**. The Intercom Exchanges page displays.
  2. Click **Add Intercom Exchange**. The Configure Intercom Exchange page as shown in [Figure 146](#) displays.

**Figure 146.** Configure Intercom Exchanges page

3. Enter the information described in [Table 87](#). A check mark indicates a required field. Continue to add information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 87.** Configure Intercom Exchange fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify the item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## Model Tab

**Figure 147.** Configure Intercom Exchanges — Model tab

5. Select the **Model** tab as shown in [Figure 147](#) and enter the information described in [Table 88](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 88.** Configure Intercom Exchange fields and descriptions

Field Name	REQ	Description
<b>Model</b>	✓	Use the drop-down list to select the intercom exchange model name.
<b>Facility Commander Server</b>	✓	Use the drop-down list to select the Facility Commander server that controls communication with this intercom exchange.
<b>Time Zone</b>	✓	Use the drop-down list to select the time zone where this device is located. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.

## Addresses Tab

**Figure 148.** Configure Intercom Exchanges — Addresses tab

6. Select the **Addresses** tab as shown in [Figure 148](#) and enter the information described in [Table 89](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 89.** Configure Intercom Exchange fields and descriptions

Field Name	REQ	Description
Exchange Number		Enter an exchange number <i>only when there are multiple intercom exchanges</i> with overlapping station numbers.
IP Address or Host Name	✓	Enter the intercom station IP address or host name. The host name is case-sensitive.
Port	✓	Enter the port number.

## Advanced Tab

The screenshot shows a web interface with five tabs: Model, Addresses, Advanced, Alarms, and Facility. The 'Advanced' tab is selected and highlighted with a red rectangular box. Below the tabs, there are two input fields, each preceded by a blue asterisk indicating a required field. The first field is labeled 'Status Polling Interval (seconds)' and contains the number '30'. The second field is labeled 'Command Retry Interval (seconds)' and also contains the number '30'.

**Figure 149.** Configure Intercom Exchanges — Advanced tab

7. Select the **Advanced** tab as shown in [Figure 147](#) and enter the information described in [Table 90](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 90.** Configure Intercom Exchange fields and descriptions

Field Name	REQ	Description
<b>Status Polling Interval (seconds)</b>	✓	Enter the number of seconds to wait before Facility Commander polls the intercom device. The default value is 15 seconds.
<b>Command Retry Interval (seconds)</b>	✓	Enter the number of seconds to wait before trying to reconnect to the Facility Commander server. The default value is 30 seconds.

## Alarms Tab

The screenshot shows a configuration window with five tabs: Model, Addresses, Advanced, Alarms, and Facility. The 'Alarms' tab is selected and highlighted with a red circle. Below the tabs, there are two sections for configuring alarms. The first section is 'Intercom Exchange Comm Failure Alarm' with a dropdown menu showing 'IntercomExchangeProfile'. The second section is 'Intercom Exchange Reset Alarm' with a dropdown menu showing 'IntercomExchangeResetProfile'.

**Figure 150.** Configure Intercom Exchanges — Alarms tab

8. Select the **Alarms** tab as shown in [Figure 148](#) and enter the information described in [Table 91](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 91.** Configure Intercom Exchange fields and descriptions

Field Name	REQ	Description
<b>Intercom Exchange Comm Failure Alarm</b>		Use the drop-down list to select the appropriate alarm profile when the intercom exchange is no longer communicating with the Facility Commander server.
<b>Intercom Exchange Reset Alarm</b>		The intercom exchange can reset itself and if it does, this alarm is generated.

## Facility Tab

The screenshot shows a configuration window with five tabs: Model, Addresses, Advanced, Alarms, and Facility. The Facility tab is selected and highlighted with a red circle. Below the tabs, there is an 'Assigned to' field and an 'Available' list. The 'Available' list contains the following items: BOCA RATON, CHICAGO, DALLAS, East Coast Region, Global Facility, LOS ANGELES, NEW YORK, PP GLOBAL, Sample Permissions and Contexts Facility, and Sample Region Facility.

**Figure 151.** Configure Intercom Exchanges — Facility tab

9. Select the **Facility** tab as shown in [Figure 151](#) and enter the information described in [Table 92](#). A check mark indicates a required field.

**Table 92.** Configure Intercom Exchange fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Configuring Intercom Stations

Use the Intercom Stations page to add, edit, copy, and delete intercom station records. Refer to the following sections for more information:

- [Viewing Intercom Stations](#)
- [Adding Intercom Stations on page 241](#)

### Viewing Intercom Stations

► **To view intercom stations, follow these steps:**

1. Select **Device Management**.
2. Select **Intercom Stations**. The Intercom Stations page as shown in [Figure 145](#) displays.

	Tag Name	Description	Reference ID	Extension	Master Station	Intercom Exchange
	NY Bldg 1 Intercom	NY Bldg 1 Intercom in Lobby		6300	No	AlphaCom Exchange
	NY Intercom Bldg 1_Master	Main Intercom System in Bldg 1		6200	Yes	AlphaCom Exchange

**Figure 152.** Intercom Stations list page



## Adding Intercom Stations

► To add an intercom station, follow these steps:

1. Select **Device Management**, and then **Intercom Stations**. The Intercom Stations page displays.
2. Click **Add Intercom Station**. The Configure Intercom Station page as shown in [Figure 153](#) displays.

**Figure 153.** Configure Intercom Station page

3. Enter the information described in [Table 93](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 93.** Configure Intercom Station fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

**Figure 154.** Configure Intercom Station — General tab

5. Select the **General** tab as shown in [Figure 154](#) and enter the information described in [Table 94](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 94.** Configure Intercom Station fields and descriptions

Field Name	REQ	Description
<b>Intercom Exchange</b>	✓	Use the drop-down list to select the intercom exchange switch physically connected to the intercom station.
<b>Extension</b>	✓	Enter the extension number of the intercom station.
<b>Master Station</b>		Select this check box to indicate if this is a master intercom station.
<b>Time Zone</b>	✓	Use the drop-down list to select the time zone where this device is located. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.

## Monitoring Tab

The screenshot shows the 'Monitoring' tab selected in a configuration window. The tab is highlighted with a red border. Below the tab are four dropdown menus with the following values:

- Graphic Display: NY Floor 02
- Camera: NY Cam 100
- Preset: NY Cam 100 PS 01
- Access Point: AP 200101 NY COMPUTER ROOM

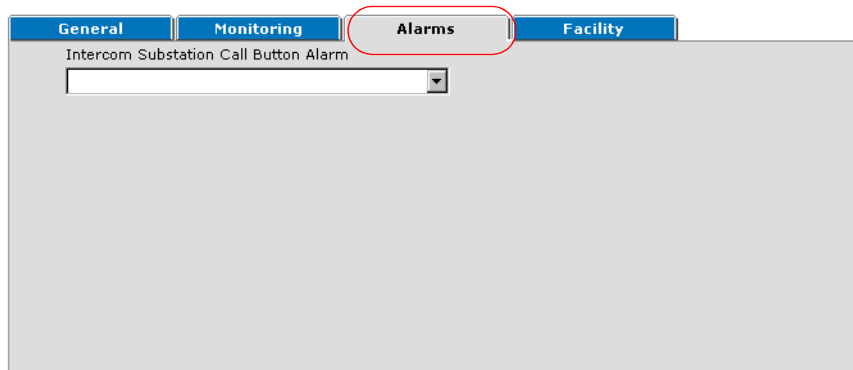
**Figure 155.** Configure Intercom Station — Monitoring tab

6. Select the Monitor tab as shown in [Figure 154](#) and enter the information described in [Table 95](#). A check mark indicates a required field. Continue to add information on the tabbed pages.
7. Click **Submit** to save the record.

**Table 95.** Configure Intercom Station fields and descriptions

Field Name	REQ	Description
Graphic Display		Use the drop-down list to create the default action for the device. When an operator uses the Control Toolbar, this graphic display will be listed. Refer to <a href="#">Control Toolbar on page 209</a> for more information.
Camera		Use the drop-down list to create the default action for the device. When an operator uses the Control Toolbar, this camera will be listed. Refer to <a href="#">Control Toolbar on page 209</a> for more information.
Preset		Use the drop-down list to create the default action for the device. When an operator uses the Control Toolbar, to select the camera, the camera will move to this preset position. Refer to <a href="#">Control Toolbar on page 209</a> for more information.
Access Point		Use the drop-down list to create the default action for the device. When an operator uses the Control Toolbar, this access pointed will be listed. Refer to <a href="#">Control Toolbar on page 209</a> for more information.

## Alarms Tab



The screenshot shows a web interface with four tabs: General, Monitoring, Alarms, and Facility. The Alarms tab is selected and highlighted with a red circle. Below the tabs, the text "Intercom Substation Call Button Alarm" is displayed above a drop-down menu.

**Figure 156.** Configure Intercom Station — Alarms tab

8. Select the **Alarms** tab as shown in [Figure 156](#) and enter the information described in [Table 96](#). Continue to the next tabbed page. A check mark indicates a required field.

**Table 96.** Configure Intercom Station fields and descriptions

Field Name	REQ	Description
<b>Intercom Substation Call Button Alarm</b>		Use the drop-down list to select the appropriate alarm profile to generate when someone presses the intercom call button. No alarm is generated if this is not selected. <i>Do not select this alarm if this is a master station record.</i>

## Facility Tab

The screenshot shows a web interface with four tabs: General, Monitoring, Alarms, and Facility. The Facility tab is selected and highlighted with a red circle. Below the tabs, there are two main sections. The first section is labeled 'Assigned to' and contains a text box with the value 'NEW YORK'. The second section is labeled 'Available' and contains a list box with the following items: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEW YORK' (which is highlighted in blue), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. A blue asterisk is positioned to the left of the 'Available' list box.

**Figure 157.** Configure Intercom Stations — Facility tab

Select the Facility tab as shown in [Figure 157](#) and enter the information described in [Table 97](#). A check mark indicates a required field.

**Table 97.** Configure Intercom Stations fields and descriptions

Field Name	REQ	Description
<b>Assigned to</b>		Items can belong to more than one facility. This is a read-only field and cannot be edited.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Tips for Creating Symbol Schemes

Intercom stations have many states associated with them, such as Intercom Master Call Answered, Intercom Master Call Connected, Intercom Master Call Ringing, and many more.

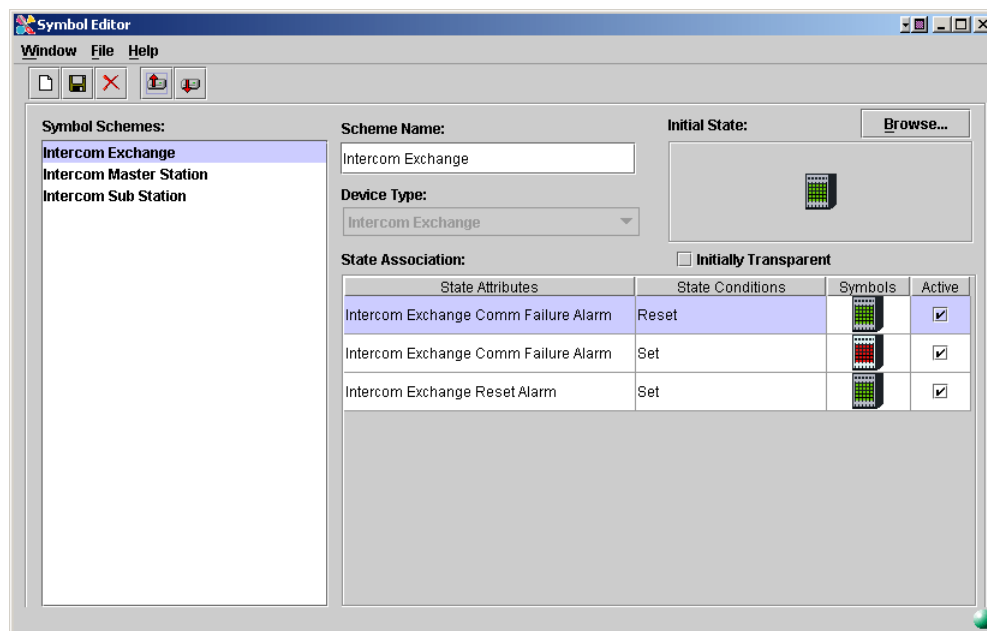
Because there are so many states, a system administrator could have a difficult time creating the symbol scheme and displaying the intercom states correctly on the graphic displays.

To assist the system administrator in creating these symbol schemes, a few examples are included:

- [Intercom Exchange Symbol Scheme](#)
- [Intercom Master Station Symbol Scheme on page 247](#)
- [Intercom Substation Symbol Scheme on page 248](#)

### Intercom Exchange Symbol Scheme

Figure 158 shows a symbol scheme for an Intercom Exchange. In this example, the Intercom Exchange Comm Failure Alarm is a red symbol and all of the other states are green symbols, including the initial state symbol. This helps to convey the online/offline status of the intercom exchange.



**Figure 158.** Example Intercom Exchange Symbol Scheme

## Intercom Master Station Symbol Scheme

Figure 159 shows a symbol scheme for an Intercom Master Station.

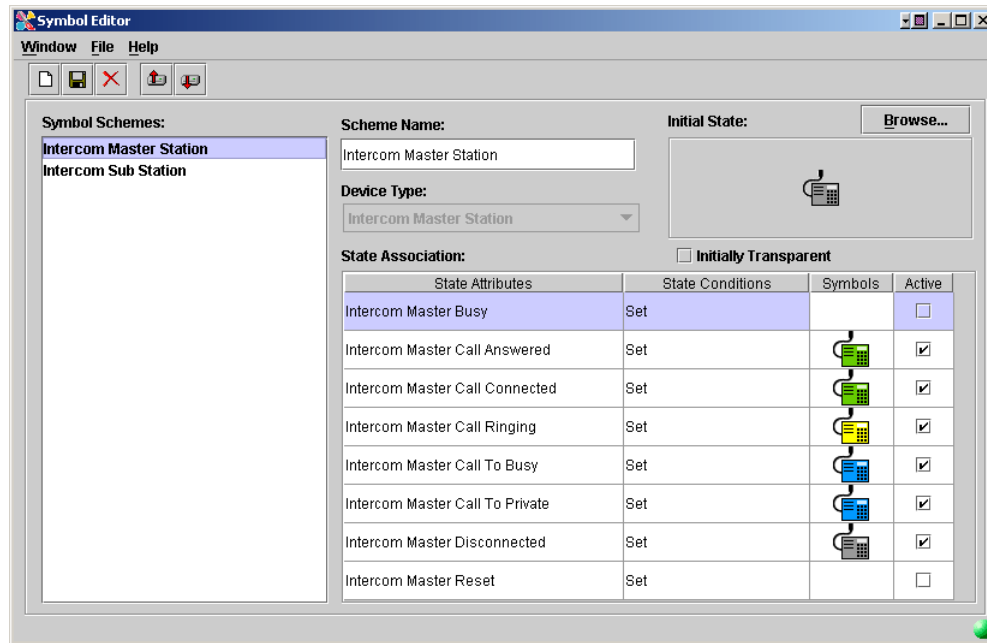
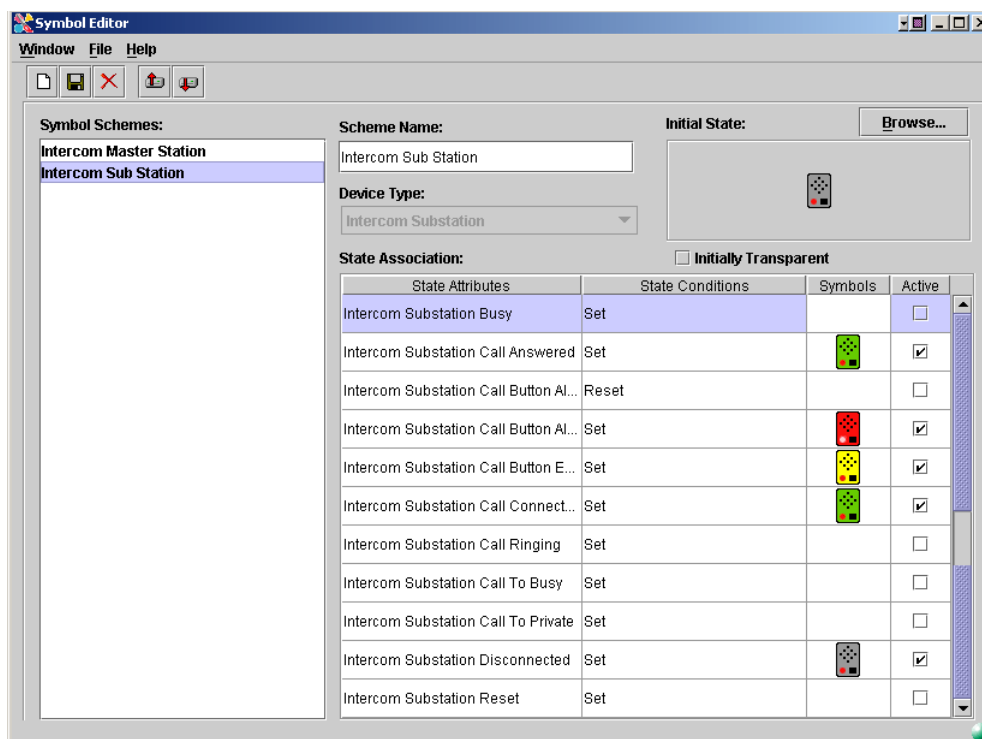


Figure 159. Example Intercom Master Station Symbol Scheme

## Intercom Substation Symbol Scheme

Figure 160 shows a symbol scheme for an Intercom Substation.



**Figure 160.** Example Intercom Substation Symbol Scheme



# Chapter 13. Configuring Intrusion Devices

This chapter describes how to configure intrusion panels, intrusion areas, and intrusion inputs. Instructions to connect the RS-232 cable are included, as well as the parameters to configure the device server.

Readers should know how the current intrusion panel is configured. The Facility Commander configuration should reflect the intrusion panel's internal configuration.



---

## In this chapter:

- [Overview on page 250](#)
- [Connecting Intrusion Panels on page 251](#)
- [Configuring Intrusion Panels on page 254](#)
- [Configuring Intrusion DGPs on page 261](#)
- [Configuring Intrusion Keypads on page 266](#)
- [Configuring Intrusion Areas on page 271](#)
- [Configuring Intrusion Inputs on page 276](#)
- [Configuring Intrusion Outputs on page 281](#)

## Overview

The intrusion feature in Facility Commander allows operators to view intrusion areas using the Graphics Viewer, view alarms and events from an intrusion panel, and arm or disarm an intrusion area. The following sections describe the feature in more detail:

- [Terminology](#)
- [Connecting Intrusion Panels on page 251](#)
- [Configuring Intrusion Devices on page 251](#)

## Terminology

The security industry sometimes uses different terminology to describe intrusion devices. Facility Commander uses the terms defined below:

<b>Area</b>	A collection or group of input devices. An area may be armed, which means that an alarm is generated when the intrusion device is triggered.
<b>Arm/Disarm</b>	<ul style="list-style-type: none"><li>• The arm state means the inputs associated with the area can generate alarms when an input is active.</li><li>• The disarm state means the inputs will not generate alarms even if the input is active.</li></ul>
<b>Data Gathering Panel (DGP)</b>	A type of intrusion sub-panel that is part of the ATS Intrusion system. The main intrusion panel controls the DGP.
<b>Input</b>	An intrusion sensor such as a motion detector and glass break detector. Also called point or zone. Inputs are wired to a panel.
<b>Keypad</b>	A device used by the operator to control an intrusion panel. Use the keypad to arm and disarm areas.
<b>Output</b>	A relay device is used to control a light or siren.
<b>Panel</b>	A panel controls one or more areas. In this release, only the ATS 4017 Intrusion Panel is supported.

## Configuring Intrusion Devices

Refer to the checklist below for the configuration order to implement the intrusion feature in Facility Commander.

- |   |   |
|---|---|
| ✓ | Connect Facility Commander server to the Tecom ATS 4017 Panel with the RS-232 internal communications board. Refer to <a href="#">Connecting Intrusion Panels on page 251</a> . |
| ✓ | Configure the intrusion panel. Refer to <a href="#">Configuring Intrusion Panels on page 254</a> .  |
| ✓ | Configure the intrusion area for each area defined in the panel. Refer to <a href="#">Configuring Intrusion Keypads on page 266</a> page.                                       |
| ✓ | Configure the intrusion input defined for each panel. Refer to <a href="#">Configuring Intrusion Inputs on page 276</a> .   |

## Connecting Intrusion Panels

Facility Commander supports both Ethernet connections and RS-232 connections to the AL 4017 Intrusion Panel. Refer to:

- [Ethernet Connection](#)
- [RS-232 Connection on page 253](#)

### Ethernet Connection

Encryption is available for Ethernet connections. If you choose to use encryption, enter the same encryption key as configured on the ATS panel.

The ATS panel uses the UDP/IP protocol, which unlike TCP/IP is blocked from passing through network routers by many IT Departments. The Facility Commander server and ATS panel should be located on subnets that allow UDP packets to be exchanged.

Configure this device using the Lantronix Device Installer application. [Table 98](#) lists the parameters.

**Table 98.** Device Installer Parameters

Device Installer Parameters	
Serial Port Settings	
Serial Protocol	RS-232
Speed	4800
Character Size	8
Parity	None

**Table 98.** Device Installer Parameters (Continued)

Device Installer Parameters	
Stopbit	1
Flow Control	None
Connect Mode Settings	
UDP Datagram Mode	Disable
Incoming Connection	Unconditional
Response	Nothing
Startup	No active connection startup
Dedicated Connection	
Local Port	Installers choice. Must match the panel configuration.
Flush Mode Input Buffer (Line to Network)	
On Active Connection	Enable
On Passive Connection	Enable
At Time to Disconnect	Enable
Flush Mode Input Buffer (Network to Line)	
On Active Connection	Enable
On Passive Connection	Enable
At Time to Disconnect	Enable
Packing Algorithm	
Packing Algorithm	Disable
Additional Settings	
Disconnect Mode	Ignore
Check for Cntl-D	Disable
Port Password	Disable
Telnet Mode	Disable
Inactivity Timeout	Enable

## RS-232 Connection

To communicate with an RS-232 device, you must use a Lantronix® bridge, UDS100 Device server. This device allows messages sent by the ATS panel's RS-232 connector to be received by the Facility Commander ethernet connection.

If installers decide to provide their own RS-232 cable, they should consider:

- The wire carrying the CTS (Clear-To-Send) signal on the RS-232 cable should be disconnected at the panel.
- The wires carrying the RTS/CTS (Request-To-Send) signal on the RS-232 should be wired together at the panel.
- The cable should be constructed as a "null modem cable", which is also known as a crossover cable. This means the transmit and receive signals should be crossed, so the transmit signal from the panel becomes the receive signal at the other end of the cable.

## Configuring Intrusion Panels

Use the Intrusion Panels page to add, edit, copy, and delete records. Refer to the following sections for instructions:

- [Viewing Intrusion Panels](#)
- [Adding Intrusion Inputs on page 277](#)

### Viewing Intrusion Panels

► **To view intrusion panels, follow these steps:**

1. Select **Device Management**.
2. Select **Intrusion Panels**. The Intrusion Panels page as shown in [Figure 161](#) displays.

	Tag Name	Description	Reference ID	Facility Commander Server
	ATS Panel			FCServer

**Figure 161.** Intrusion Panels page

## Adding Intrusion Panels

► To add an intrusion panel, follow these steps:

1. Select **Device Management**, and then **Intrusion Panels**. The Intrusion Panels page displays.
2. Click **Add Intrusion Panel**. The Configure Intrusion Panel page as shown in [Figure 162](#) displays.

**Figure 162.** Intrusion Panel page

3. Enter the information described in [Table 99](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 99.** Intrusion Panel fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## Model Tab

**Figure 163.** Intrusion Panel — Model tab

5. Select the **Model** tab as shown in [Figure 163](#) and enter the information described in [Table 100](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 100.** Configure Intrusion Panel fields and descriptions

Field Name	REQ	Description
<b>Model</b>	✓	Use the drop-down list to select the model name.
<b>Facility Commander Server</b>	✓	Use the drop-down list to select the main Facility Commander that controls communication with this intrusion panel.
<b>Time Zone</b>	✓	Use the drop-down list to select the time zone for this server. This time zone displays on the Alarm Monitor and Event Monitor. The default time zone setting is GMT.
<b>Command Retry Interval (seconds)</b>	✓	Enter the number of seconds to wait before trying to re-send a command, such as a query for status of outputs, to the intrusion panel. The default value is two seconds.
<b>Maximum Command Retry Attempts</b>	✓	Enter the maximum number of times to try re-sending a command to the intrusion panel. The default value is three.



## Addresses Tab

**Figure 164.** Intrusion Panel — Addresses tab

6. Select the **Addresses** tab as shown in and enter the information described in [Table 101](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 101.** Configure Intrusion Panel fields and descriptions

Field Name	REQ	Description
IP Address or Host Name	✓	<ul style="list-style-type: none"> <li><b>Ethernet:</b> Enter the IP address or host name of the intrusion panel.</li> </ul>
Port	✓	<ul style="list-style-type: none"> <li><b>Ethernet:</b> Enter the port number configured in the intrusion panel, such as 3001</li> </ul>
Panel Address	✓	Enter the intrusion panel address.
<b>Connection Type</b>		
Ethernet	✓	Select this check box to use an Ethernet connection.
Status Polling Interval (Milliseconds)	✓	Enter the number of milliseconds indicating the frequency Facility Commander polls the intrusion panel. The range is from 200 to 30,000 milliseconds. The default value is 5,000 milliseconds.

## Advanced Tab

The screenshot shows the 'Advanced' tab of the Intrusion Panel configuration interface. The tab is highlighted with a red circle. Below the tab are several input fields: 'User Name' with a text box, 'Password' with a text box and a blue asterisk indicating it is required, 'Confirm Password' with a text box and a blue asterisk, 'Encryption Enabled' with an unchecked checkbox, and 'Encryption Key' with a text box.

**Figure 165.** Intrusion Panel — Advanced tab

7. Select the **Advanced** tab as shown in [Figure 162](#) and enter the information described in [Table 102](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 102.** Configure Intrusion Panel fields and descriptions

Field Name	REQ	Description
User Name		Enter a valid user name.
Password	✓	Enter the password used to access the intrusion panel. The password must match the password defined on the intrusion panel. The password must be ten digits. The format is: 0000000000. The password must be correct because if Facility Commander tries to connect using an incorrect password, the intrusion panel locks out any further attempts. The password will have to be reset by an intrusion support engineer.
Confirm Password	✓	Enter the password again for confirmation.
Encryption Enabled		Select this check box if you want to enable encryption between Facility Commander and the intrusion panel.
Encryption Key (Windows only.)		Obtain the encryption key from the vendor's web site. The format is: 000-000-000-000-000-000-000-000-000-000-000-000-000-000-000-000-000-000. There are 16 groups of three numbers, separated by a hyphen. The range of numbers is from 000 to 255. If the number 2 is given as part of the encryption key, you must enter 002.

## Alarms Tab

The screenshot shows the 'Alarms' tab selected in a configuration window. The tab is highlighted with a red border. Below the tab, there are five dropdown menus, each with a label and a downward arrow icon. The labels are: 'Intrusion Panel Duress Code Entered Alarm', 'Intrusion Panel Main Power Failure Alarm', 'Intrusion Panel Offline Alarm', 'Intrusion Siren Monitor Failure Alarm', and 'Intrusion Panel Tamper Alarm'.

**Figure 166.** Intrusion Panel — Alarms tab

8. Select the **Alarms** tab as shown in [Figure 163](#) and enter the information described in [Table 103](#). A check mark indicates a required field. Continue to the next tabbed page.

**Table 103.** Configure Intrusion Panel fields and descriptions

Field Name	REQ	Description
<b>Intrusion Panel Duress Code Entered Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when a duress code has been entered.
<b>Intrusion Panel Main Power Failure Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the intrusion panel main power fails.
<b>Intrusion Panel Offline Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the intrusion panel is offline.
<b>Intrusion Siren Monitor Failure Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the intrusion siren monitor fails.
<b>Intrusion Panel Tamper Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when someone tampers with an intrusion panel.

## Facility Tab

The screenshot shows the 'Facility' tab of the Intrusion Panel. The 'Assigned to' field is set to 'NEW YORK'. The 'Available' list includes: BOCA RATON, East Coast Region, Global Facility, NEW YORK (highlighted), PP GLOBAL (marked with a blue asterisk), Sample Permissions and Contexts Facility, Sample Region Facility, and West Coast Region. A note at the bottom indicates 'Hold the Ctrl key down for multiple selection.'

**Figure 167.** Intrusion Panel — Facility tab

9. Select the **Facility** tab as shown in [Figure 167](#) and enter the information described in [Table 104](#). A check mark indicates a required field.

**Table 104.** Configure Intrusion Panel fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Configuring Intrusion DGPs



Use the Configure Intrusion DGPs (data gathering panel) page to add, edit, copy, and delete records. Refer to the following sections for instructions:

- [Viewing Intrusion DGPs on page 261](#)
- [Adding Intrusion DGPs on page 262](#)

### Viewing Intrusion DGPs

► **To view intrusion DGPs, follow these steps:**

1. Select **Device Management**.
2. Select **Intrusion DGPs**. The Intrusion DGPs page as shown in [Figure 168](#) displays.

	Tag Name	Description	Reference ID	Intrusion Panel	DGP Number
 	DGP 10	Computer Lab		ATS Panel	10

**Figure 168.** Intrusion DGPs page

## Adding Intrusion DGPs

- To add an intrusion DGP, follow these steps:
1. Select **Device Management**, and then **Intrusion DGPs**. The Intrusion DGPs page displays.
  2. Click **Add Intrusion DGP** and the Configure Intrusion DGP page as shown in [Figure 169](#) displays.

**Figure 169.** Configure Intrusion DGP page

**Table 105.** Configure Intrusion DGP fields and descriptions

Field Name	REQ	Description
<b>Tag Name</b>	✓	Enter a unique name to identify this item. Use 2-36 characters.
<b>Description</b>		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
<b>Reference ID</b>		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

The screenshot shows a web-based configuration interface for an Intrusion DGP. It features three tabs: 'General' (highlighted with a red box), 'Alarms', and 'Facility'. The 'General' tab contains two required fields, each marked with an asterisk (\*): 'Intrusion Panel' is a dropdown menu currently showing 'Intrusion Panel', and 'DGP Number' is a text input field containing the value '10'. Below the form fields are 'Submit' and 'Cancel' buttons.

**Figure 170.** Configure Intrusion DGP — General tab

3. Select the **General** tab as shown in [Figure 170](#). Enter the information described in [Table 106](#). A check mark indicates a required field.
4. Click **Submit** to save the record.

**Table 106.** Configure Intrusion DGP fields and descriptions

Field Name	REQ	Description
Intrusion Panel	✓	Use the drop-down list to select the appropriate intrusion panel to use with this DGP.
DGP Number	✓	Enter the DGP number.

## Alarms Tab

The screenshot shows a configuration window with three tabs: 'General', 'Alarms', and 'Facility'. The 'Alarms' tab is selected and highlighted with a red circle. Below the tabs, there are five dropdown menus, each with a label and a downward arrow icon. The labels are: 'Intrusion DGP Panel Bypassed', 'Intrusion DGP Main Power Failure Alarm', 'Intrusion DGP Offline Alarm', 'Intrusion DGP Siren Monitor Failure Alarm', and 'Intrusion DGP Tamper Alarm'.

**Figure 171.** Configure Intrusion DGP — Alarms tab

5. Select the **Alarms** tab as shown in [Figure 171](#). Enter the information described in [Table 107](#). A check mark indicates a required field.

**Table 107.** Configure Intrusion DGP fields and descriptions

Field Name	REQ	Description
<b>Intrusion DGP Panel Bypassed</b>		Use the drop-down list to select the appropriate alarm profile to use when the intrusion DGP panel is bypassed. This is the generated alarm.
<b>Intrusion DGP Main Power Failure Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when there is a DGP main panel failure. This is the generated alarm.
<b>Intrusion DGP Offline Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the DGP goes offline. This is the generated alarm.
<b>Intrusion DGP Siren Monitor Failure Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the intrusion DGP siren monitor fails. This is the generated alarm.
<b>Intrusion DGP Tamper Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when tampering with the DGP has occurred. This is the generated alarm.



## Facility Tab

**Figure 172.** Configure Intrusion DGP — Facility tab

6. Select the **Facility** tab as shown in [Figure 172](#) and enter the information described in [Table 108](#). A check mark indicates a required field.

**Table 108.** Configure Intrusion DGP fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Configuring Intrusion Keypads

Use the Configure Intrusion Keypads page to view, add, edit, copy, or deleted intrusion outputs records. Refer to the following sections for instructions:

- [Viewing Intrusion Keypads](#)
- [Adding Intrusion Outputs on page 282](#)

### Viewing Intrusion Keypads

► To view the intrusion keypads, follow these steps:

1. Select **Device Management**.
2. Select **Intrusion Keypads**. The Intrusion Keypads page as shown in [Figure 173](#) displays.

	Tag Name	Description	Reference ID	Intrusion Panel	Keypad Number
	intrusion keypad	keypad located by computer lab		ATS Panel	1

**Figure 173.** Intrusion Keypad page

## Adding Intrusion Keypads

➤ To add an intrusion keypad, follow these steps:

1. Select **Device Management**, and then **Intrusion Keypads**. The Configure Intrusion Keypad page displays.
2. Click **Add Intrusion Keypad**. The Configure Intrusion Keypad page shown in [Figure 174](#) displays.

**Figure 174.** Configure Intrusion Outputs page

3. Enter the information described in [Table 109](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 109.** Configure Intrusion Keypad fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

The screenshot shows the 'General' tab of a configuration window. The 'General' tab is selected and highlighted with a red circle. Below the tabs, there are two required fields: 'Intrusion Panel' with a dropdown menu showing 'ATS Panel', and 'Keypad Number' with a text box containing '1'. Both fields are marked with a blue asterisk.

**Figure 175.** Configure Intrusion Keypad — General tab

5. Enter the information described in [Table 110](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 110.** Configure Intrusion Outputs fields and descriptions

Field Name	REQ	Description
Intrusion Panel	✓	Use the drop-down list to select the intrusion panel associated with this intrusion outputs. This number must match the area configured for this output.
Keypad Number	✓	Enter the keypad number to represent this intrusion keypad. The number must be between 1 and 16.

## Alarms Tab

The screenshot shows a configuration window with three tabs: General, Alarms, and Facility. The 'Alarms' tab is selected and highlighted with a red rectangle. Below the tabs, there are four dropdown menus, each with a label and a downward arrow:

- Intrusion Keypad Bypassed Alarm
- Intrusion Duress Alarm
- Intrusion Keypad Offline Alarm
- Intrusion Keypad Tamper Alarm

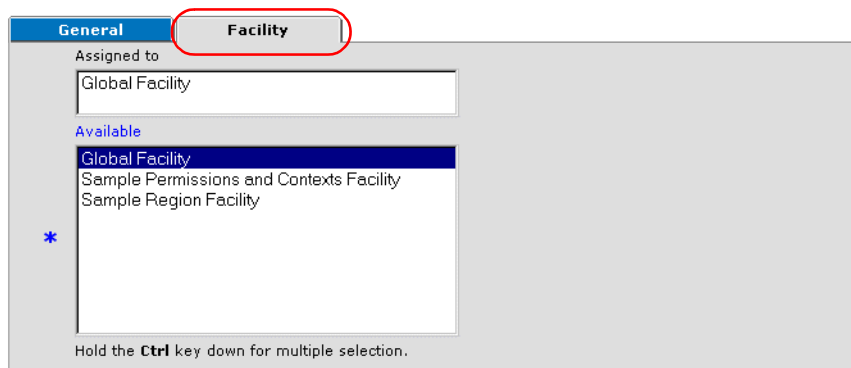
**Figure 176.** Configure Intrusion Keypad — Alarms tab

6. Enter the information described in [Table 111](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 111.** Configure Intrusion Keypad fields and descriptions

Field Name	REQ	Description
<b>Intrusion Keypad Bypassed Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when there is an attempt to bypass the keypad. This is the generated alarm.
<b>Intrusion Duress Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when there is a duress alarm. This is the generated alarm.
<b>Intrusion Keypad Offline Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the keypad goes offline. This is the generated alarm.
<b>Intrusion Keypad Tamper Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when tampering with the intrusion keypad has occurred. This is the generated alarm.

## Facility Tab



The screenshot shows the 'Facility' tab selected in the 'Configure Intrusion Keypad' interface. The 'Assigned to' field contains 'Global Facility'. The 'Available' list contains three items: 'Global Facility', 'Sample Permissions and Contexts Facility', and 'Sample Region Facility'. A blue asterisk is next to the 'Available' list. A note at the bottom says 'Hold the Ctrl key down for multiple selection.'

**Figure 177.** Configure Intrusion Keypad — Facility tab

7. Select the **Facility** tab as shown in [Figure 177](#) and enter the information described in [Table 112](#). A check mark indicates a required field.

**Table 112.** Configure Intrusion Keypad fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Configuring Intrusion Areas

Use the Intrusion Areas page to view, add, edit, copy, or deleted intrusion area records. Refer to the following sections for instructions:

- [Viewing Intrusion Areas](#)
- [Adding Intrusion Areas on page 272](#)

### Viewing Intrusion Areas

► **To view the intrusion area records, follow these steps:**

1. Select **Device Management**.
2. Select **Intrusion Areas**. The Intrusion Areas page as shown in [Figure 178](#) displays.

**Intrusion Areas**

**Instructions**  
View, edit, add or delete intrusion areas.

Search:

◀ Page 1 of 1 ▶ Go to   Items per Page

	Tag Name	Description	Intrusion Panel	Area Number
	NY Computer Lab		ATS Panel	200

**Figure 178.** Intrusion Areas page

## Adding Intrusion Areas

- To add an intrusion area, follow these steps:
1. Select **Device Management**, and then **Intrusion Areas**. The Intrusion Areas page displays.
  2. Click **Add Intrusion Area** and the Configure Intrusion Area page as shown in [Figure 179](#) displays.

**Figure 179.** Configure Intrusion Area page

3. Enter the information described in [Table 113](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 113.** Configure Intrusion Area fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.



## General Tab

**Figure 180.** Configure Intrusion Area — General tab

5. Enter the information described in [Table 114](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 114.** Configure Intrusion Area fields and descriptions

Field Name	REQ	Description
Intrusion Panel	✓	Use the drop-down list to select the intrusion panel associated with this intrusion area.
Area Number	✓	Enter a number from 1 to 256 that corresponds to the area number configured in the intrusion panel.

## Alarms Tab

The screenshot shows a configuration window with three tabs: 'General', 'Alarms', and 'Facility'. The 'Alarms' tab is active and highlighted with a red circle. Below the tabs, there are two dropdown menus. The first dropdown is labeled 'Intrusion Area Failed To Arm' and the second is labeled 'Intrusion Area State Armed and In Alarm'.

**Figure 181.** Configure Intrusion Area — Alarms tab

6. Enter the information described in [Table 115](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 115.** Configure Intrusion Area fields and descriptions

Field Name	REQ	Description
<b>Intrusion Area Failed to Arm</b>		Use the drop-down list to select the appropriate alarm profile to use when a command is sent to arm an area and an active input prevents the operation. This is the generated alarm.
<b>Intrusion Area State Armed and In Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when an area is armed and an input becomes active. This is the generated alarm.

## Facility Tab

**Figure 182.** Configure Intrusion Area — Facility tab

7. Select the **Facility** tab as shown in [Figure 182](#) and enter the information described in [Table 116](#). A check mark indicates a required field.

**Table 116.** Configure Intrusion Area fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

## Configuring Intrusion Inputs

Use the Configure Intrusion Input page to view, add, edit, copy, or deleted intrusion input records. Refer to the following sections for instructions:

- [Viewing Intrusion Input](#)
- [Adding Intrusion Inputs on page 277](#)

### Viewing Intrusion Input

► **To view the intrusion input, follow these steps:**

1. Select **Device Management**.
2. Select **Intrusion Inputs**. The Intrusion Inputs page as shown in [Figure 183](#) displays.

Tag Name	Description	Reference ID	Intrusion Area	Input Number
Motion Detectors	NY Computer Lab		NY Computer Lab	50

**Figure 183.** Intrusion Inputs page

## Adding Intrusion Inputs

► To add an intrusion input, follow these steps:

1. Select **Device Management**, and then **Intrusion Inputs**. The Intrusion Inputs page displays.
2. Click **Add Intrusion Input**. The Configure Intrusion Inputs page shown in [Figure 184](#) displays.

**Figure 184.** Configure Intrusion Inputs page

3. Enter the information described in [Table 117](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 117.** Configure Intrusion Inputs fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

The screenshot shows a configuration interface with three tabs: 'General', 'Alarms', and 'Facility'. The 'General' tab is active and highlighted with a red circle. Below the tabs, there are two required fields, each marked with a blue asterisk (\*):

- Intrusion Area**: A dropdown menu with 'NY Computer Lab' selected.
- Input Number**: A text input field containing the value '50'.

**Figure 185.** Configure Intrusion Inputs — General tab

5. Enter the information described in [Table 118](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 118.** Configure Intrusion Inputs fields and descriptions

Field Name	REQ	Description
Intrusion Area	✓	Use the drop-down list to select the intrusion area associated with this intrusion inputs. This number must match the area configured for this input.
Input Number	✓	Enter the input number that to represent this intrusion inputs.

## Alarms Tab

The screenshot shows a configuration window with three tabs: General, Alarms, and Facility. The Alarms tab is selected and highlighted with a red rectangle. Below the tabs, there are four drop-down menus, each with a label and a downward arrow:

- Intrusion Input Alarm
- Intrusion Input Bypassed Alarm
- Intrusion Input Fault Alarm
- Intrusion Input Tamper Alarm

**Figure 186.** Configure Intrusion Inputs — Alarms tab

6. Enter the information described in [Table 119](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 119.** Configure Intrusion Inputs fields and descriptions

Field Name	REQ	Description
<b>Intrusion Input Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the input is in an alarm state. This is the generated alarm.
<b>Intrusion Input Bypassed Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the input is bypassed. This is the generated alarm.
<b>Intrusion Input Fault Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when the input is a fault state. This is the generated alarm.
<b>Intrusion Input Tamper Alarm</b>		Use the drop-down list to select the appropriate alarm profile to use when tampering with the intrusion input has occurred. This is the generated alarm.

## Facility Tab

The screenshot shows a configuration window with three tabs: 'General', 'Alarms', and 'Facility'. The 'Facility' tab is selected and highlighted with a red circle. Below the tabs, there are two sections: 'Assigned to' and 'Available'. The 'Assigned to' section has a text box containing 'NEW YORK'. The 'Available' section has a list box containing several facility names: 'BOCA RATON', 'East Coast Region', 'Global Facility', 'NEW YORK' (which is highlighted in blue), 'PP GLOBAL', 'Sample Permissions and Contexts Facility', 'Sample Region Facility', and 'West Coast Region'. A blue asterisk is positioned to the left of the 'Available' list box.

**Figure 187.** Configure Intrusion Inputs — Facility tab

7. Select the **Facility** tab as shown in [Figure 187](#) and enter the information described in [Table 120](#). A check mark indicates a required field.

**Table 120.** Configure Intrusion Inputs fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>



## Configuring Intrusion Outputs



Use the Configure Intrusion Outputs page to view, add, edit, copy, or deleted intrusion outputs records. Refer to the following sections for instructions:

- [Viewing Intrusion Outputs](#)
- [Adding Intrusion Outputs on page 282](#)

### Viewing Intrusion Outputs

► To view the intrusion outputs, follow these steps:

1. Select **Device Management**.
2. Select **Intrusion Outputs**. The Intrusion Outputs page as shown in [Figure 188](#) displays.

	Tag Name	Description	Reference ID	Intrusion Panel	Output Number
 	warning siren	warning siren by computer lab		ATS Panel	150

**Figure 188.** Intrusion Outputs page

## Adding Intrusion Outputs

- To add an intrusion output, follow these steps:
1. Select **Device Management**, and then **Intrusion Outputs**. The Intrusion Outputs page displays.
  2. Click **Add Intrusion Output**. The Configure Intrusion Outputs page shown in [Figure 189](#) displays.

**Figure 189.** Configure Intrusion Outputs page

3. Enter the information described in [Table 121](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.
4. Click **Submit** to save the record.

**Table 121.** Configure Intrusion Outputs fields and descriptions

Field Name	REQ	Description
Tag Name	✓	Enter a unique name to identify this item. Use 2-36 characters.
Description		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
Reference ID		Enter a name to associate this item to a blue print or wiring diagram. Use 1-20 characters.

## General Tab

The screenshot shows a configuration window with two tabs: 'General' and 'Facility'. The 'General' tab is active and highlighted with a red border. Below the tabs, there are two required fields, each marked with a blue asterisk (\*). The first field is labeled 'Intrusion Panel' and is a dropdown menu currently showing 'ATS Panel'. The second field is labeled 'Output Number' and is a text box containing the value '150'.

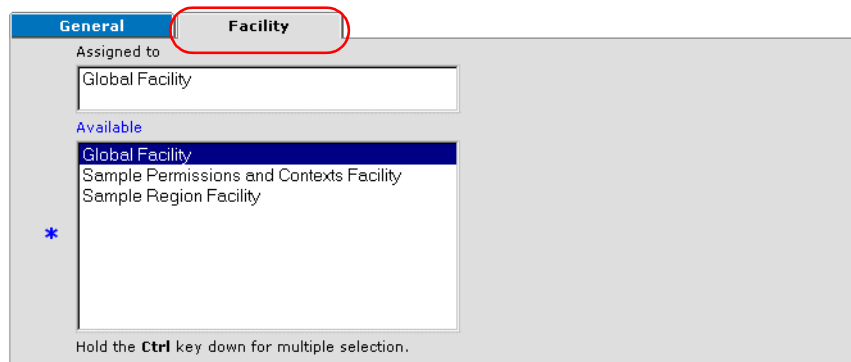
**Figure 190.** Configure Intrusion Outputs — General tab

5. Enter the information described in [Table 122](#). A check mark indicates a required field. Continue to enter information on the tabbed pages.

**Table 122.** Configure Intrusion Outputs fields and descriptions

Field Name	REQ	Description
Intrusion Panel	✓	Use the drop-down list to select the intrusion panel associated with this intrusion outputs. This number must match the area configured for this output.
Output Number	✓	Enter the output number to represent this intrusion output.

## Facility Tab



The screenshot shows a configuration window with two tabs: 'General' and 'Facility'. The 'Facility' tab is selected and highlighted with a red box. Below the tabs, there is an 'Assigned to' field containing the text 'Global Facility'. Below this is an 'Available' list containing three items: 'Global Facility', 'Sample Permissions and Contexts Facility', and 'Sample Region Facility'. A blue asterisk is positioned to the left of the 'Available' list. At the bottom of the window, a note states: 'Hold the **Ctrl** key down for multiple selection.'

**Figure 191.** Configure Intrusion Output — Facility tab

6. Select the **Facility** tab as shown in [Figure 191](#) and enter the information described in [Table 123](#). A check mark indicates a required field.

**Table 123.** Configure Intrusion Output fields and descriptions

Field Name	REQ	Description
Assigned to		Items can belong to more than one facility. This is a read-only field and cannot be edited.
Available	✓	<p>Use to assign or change the facility membership for this item. The facilities that display in this list depend on the operator's context and permissions.</p> <ul style="list-style-type: none"> <li>• To assign the item to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li> <li>• If this item is already assigned to a facility listed in the Assigned To list, press the <b>Ctrl</b> key before selecting the new facility assignment.</li> <li>• To assign the item to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li> </ul>

# Chapter 14. Creating Symbol Schemes

This chapter describes how to create a symbol scheme with icons representing access points, cameras, and more.



---

**In this chapter:**

[Overview on page 286](#)

[Using the Symbol Editor on page 287](#)

[Creating a Symbol Scheme on page 291](#)

[Managing Symbol Editor Files on page 294](#)

## Overview

The Symbol Editor and Graphics Editor allow you to use site maps of your premises and associate symbols (graphic images or icons) to device types such as access points, camera types, digital inputs, logical inputs, and digital outputs. When an alarm event occurs, one or more of the symbols changes its appearance based on the alarm state condition, if configured to do so.

A symbol scheme is created by selecting a device type, an icon to represent the initial state of the device, and a collection of icons representing the different state attributes and state conditions.

- **Device types** represent door access points, cameras, logical inputs, digital inputs, digital outputs, intercom, and intrusion devices.
- **State attributes** represent the type of alarm generated, such as an Invalid Badge or Door Forced alarm and more. The state attributes that display are appropriate for the selected device type.
- **State conditions** represent the state of the alarm point, such as set, reset and tamper.

As an example, the Door Access Point includes state attributes, such as Door Forced and others. The state attributes for a Door Forced alarm include the conditions — set and reset. Each state attribute and state condition is represented on the site map by a different symbol, such as:

- initial state is represented by a gray door icon
- set condition is represented by a red door icon
- reset condition is represented by a green door icon

Refer to [State Associations and Conditions on page 295](#) for a complete list.

Before you can associate the symbols with event point types, you need to import access points, inputs, input groups, and outputs from Picture Perfect. Refer to [Importing Records on page 55](#) for more information. When the devices are imported, the system administrator selects which graphic display to use when an alarm event is generated.

To create site maps and link alarms, use the following tools:

- **Symbol Editor** allows you to associate device types, such as access points and cameras with symbols representing alarm state conditions. Use the Symbol Editor to create, delete, save, upload, and download symbol schemes.
  - Refer to [Using the Symbol Editor on page 287](#) for more information.
- **Graphics Editor** allows you to place symbols representing devices such as doors and cameras, and more on site maps. Start with a floor plan and place symbols on the map to indicate their location, and then link these symbols to event sources. In addition, you can add text to create labels and print the site maps.
  - Refer to [Using the Graphics Editor on page 301](#) for more information.

- **Graphics Viewer** provides a graphical view of the premises and allows an operator to locate alarm events as they occur, such as doors and cameras. Operators can issue commands and launch applications, such as locking and unlocking doors and viewing video.
  - Refer to [Viewing Graphic Displays on page 333](#) for more information.

## Using the Symbol Editor

Use the Symbol Editor shown in [Figure 192](#) to associate symbols with device types, such as cameras, door access points, and more. The symbols represent the state condition, such as set and reset, for each device type and condition. *This collection of symbols and specific attributes represents a symbol scheme.*

To define a scheme, select a device type and assign a symbol to each state condition. To create customized symbols, graphics in several formats are supported, including GIF and JPG. The recommended graphic size is 32 x 32 pixels.

Once a scheme is created, use the **Upload** button to copy the scheme to the Facility Commander server. Once the scheme is copied to the server, the scheme is ready to use with the Graphics Editor and is also available to other users.

The symbol schemes are used with the Graphics Editor to create display maps. Refer to [Using the Graphics Editor on page 301](#) for more information.

➤ **To open the Symbol Editor, follow these steps:**

1. From the Facility Commander Launcher window, select **Launch** and **Symbol Editor**, or select the **Symbol Editor** icon from the Editors toolbar.
2. The Symbol Editor shown in [Figure 192 on page 288](#) window displays.

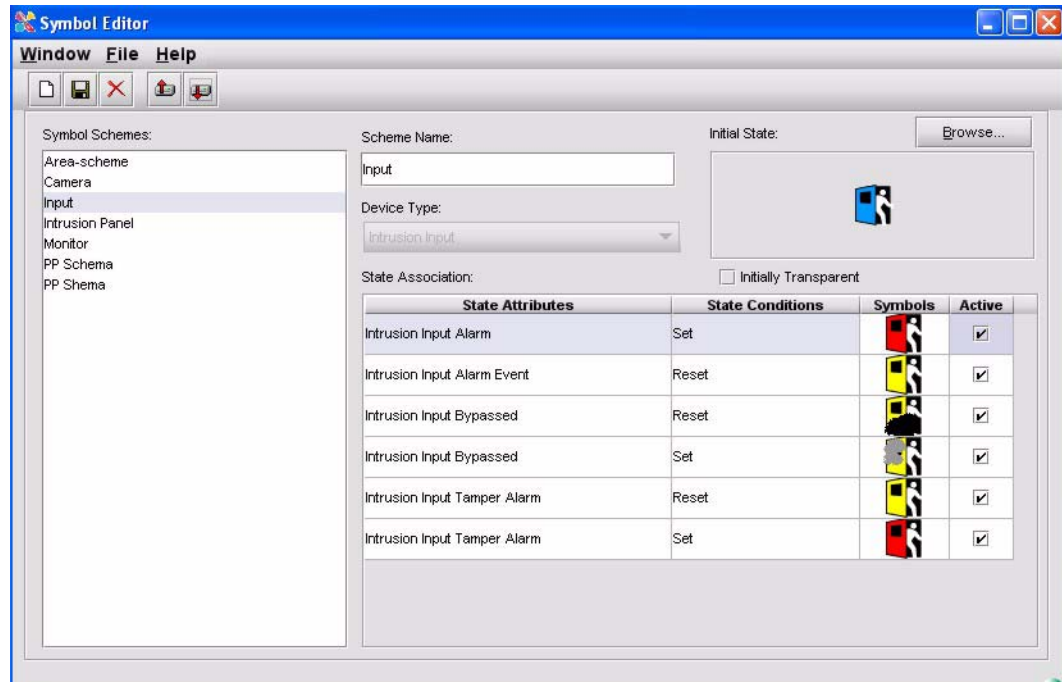


Figure 192. Symbol Editor window

Table 124 lists and describes the Symbol Editor fields and buttons.

Table 124. Symbol Editor fields and description





Field Name	Description
<b>Title Bar</b>	Displays Symbol Editor and the window instance number. Refer to <a href="#">Managing Multiple Windows on page 20</a> for more information.
<b>New</b> 	Use to create a new symbol scheme. Refer to <a href="#">Creating a Symbol Scheme on page 291</a> for more information.
<b>Save</b> 	Use to save a symbol scheme to the local computer. To publish the scheme for use with the Graphics Editor, the scheme must be uploaded to the Facility Commander server. Refer to <a href="#">Upload and Download</a> for more information.
<b>Delete</b> 	Use to delete a symbol scheme from the local computer. To delete a scheme from the Facility Commander server, refer to <a href="#">Deleting a Symbol Scheme on page 295</a> .



Table 124. Symbol Editor fields and description (Continued) (Continued)

Field Name	Description
<b>Upload and Download</b> 	<p>Use to upload new or modified symbol schemes to the Facility Commander server.</p> <p>Use to download a symbol scheme from the server to the local computer to make changes. After the scheme has been modified and you are ready to publish the changes, click <b>Upload</b>.</p> <p>Refer to <a href="#">Uploading a Symbol Scheme on page 294</a> and <a href="#">Downloading a Symbol Scheme on page 294</a> for more information.</p>
<b>Symbol Schemes</b>	Displays a list of previously defined symbol schemes in alphabetical order.
<b>Scheme Name</b>	<p>Use this field to enter a name identifying a new symbol scheme.</p> <p>Use up to 128 characters. Scheme names cannot contain any of the following characters:  \, /, :, *, ?, ", &lt;, &gt;, or  .</p>
<b>Initial State Icon</b>	Displays the symbol representing the alarm in its initial state condition. This symbol displays in the Graphics Editor Device Palette. Refer to <a href="#">Device Palette on page 303</a> for more information.
<b>Browse</b>	Click <b>Browse</b> to locate the folder with the symbols you want to use. Refer to <a href="#">Figure 193 on page 291</a> .
<b>Device Type</b>	<p>Use this drop-down list to select a device type, which includes:</p> <ul style="list-style-type: none"> <li>• Camera</li> <li>• Digital Input</li> <li>• Digital Output</li> <li>• Door Access Point</li> <li>• Logical Input</li> <li>• Intercom Exchange</li> <li>• Intercom Master Station</li> <li>• Intercom Substation</li> <li>• Intrusion Area</li> <li>• Intrusion DGP</li> <li>• Intrusion Keypad</li> <li>• Intrusion Input</li> <li>• Intrusion Output</li> <li>• Monitor</li> </ul>
<b>State Association</b>	
<b>Initially Transparent</b>	Select this check box to make the symbol for the initial state icon transparent until an alarm event occurs.

**Table 124.** Symbol Editor fields and description (Continued) (Continued)

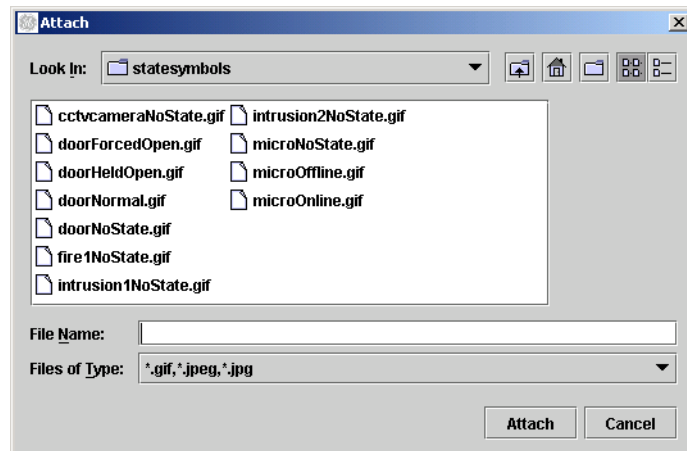
Field Name	Description
<b>State Attributes</b>	Displays the attributes of the point type. If Door Access Point is selected, the attributes include Door Forced, Door Held, and different badge events. Refer to <a href="#">Table 126</a> for a complete list.
<b>State Conditions</b>	Displays the appropriate condition for the state attribute. Refer to <a href="#">Table 126</a> for a complete list.
<b>Symbols</b>	Displays the symbol associated with the state condition. Use the <b>Active</b> check box to select the symbol.
<b>Active</b>	Click the <b>Active</b> check box and the Attach window displays. Select the graphic image you want to represent the state condition. Click <b>Attach</b> . A check mark displays to indicate this symbol.  When the <b>Active</b> check box is selected, the graphic image can be used when creating graphic displays. If you clear the check box to remove the symbol, it will no longer appear on the graphic displays when the alarm condition changes.
<b>Status Bar</b>	Displays an icon indicating if the system with the Graphics Editor is connected to the Facility Commander server and the layer number currently active (or visible). <ul style="list-style-type: none"> <li>• Green indicates the Graphics Editor is communicating with the server.</li> <li>• Red indicates the Graphics Editor is no longer communicating with the server.</li> </ul>

## Creating a Symbol Scheme

If you are creating a symbol scheme for an intrusion area, refer to [Creating an Intrusion Symbol Scheme on page 292](#) for more information.

➤ **To create a symbol scheme, follow these steps:**

1. From the **Facility Commander Launcher**, select **Launch** and **Symbol Editor**, or select the Symbol Editor icon from the Editors toolbar. The Symbol Editor window shown in [Figure 192 on page 288](#) displays.
2. Click the **New** button.
3. Enter the name of the scheme in the **Scheme Name** field.
4. Select the type from the **Device Type** drop-down list. The appropriate alarm state attributes and state conditions display for each device type.
5. Click **Browse** to display the Attach window shown in [Figure 193](#).



**Figure 193.** Attach window with available symbols

6. Select the file you want to use as a symbol to represent the state condition. Click **Attach**. The symbol displays in the **Initial State Icon** window. The Graphics Editor will use this image to represent the scheme.
7. Select the **Active** check box to display the Attach window. Select the image you want to display for each state condition. Click **Attach**. This image displays on the map when an alarm is generated and the state condition changes. The **Active** check box displays a check mark indicating this image has been associated with the alarm state condition.
8. Click **Save** when you are finished. If you want to create another symbol scheme, click **New** to clear the information and continue making new selections.

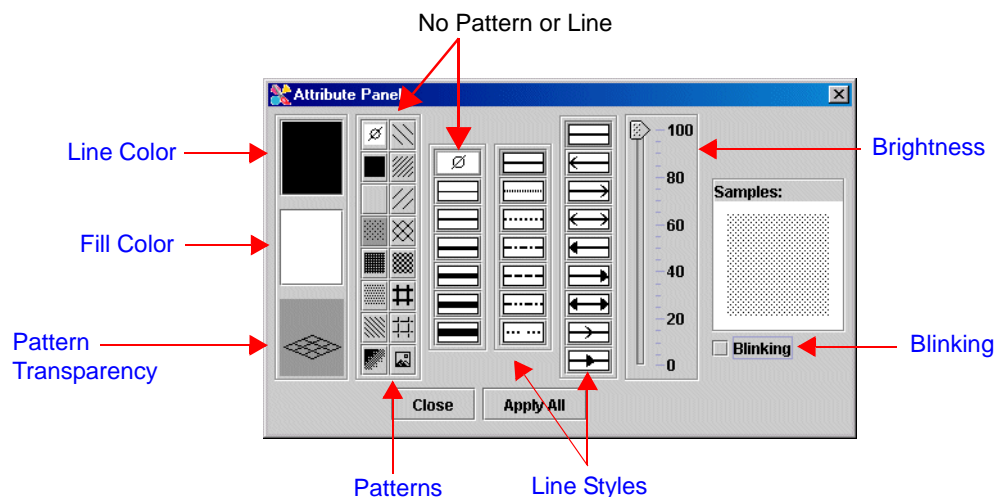
To create multiple schemes using the same point types, select the scheme you want to use, change the scheme name, and click **Save**. From the Windows menu, click **Exit** to close the Symbol Editor window.

## Creating an Intrusion Symbol Scheme

A symbol scheme for an intrusion area is different than symbol schemes for other devices. Instead of using an icon representing a device, the intrusion area is represented by a pattern.

➤ **To create an intrusion symbol scheme, follow these steps:**

1. From the Facility Commander Launcher, select Launch>Symbol Editor, or select the Symbol Editor icon from the Editors toolbar. The Symbol Editor window shown in [Figure 192 on page 288](#) displays.
2. Click the **New** button.
3. Enter the name of the scheme in the **Scheme Name** field.
4. Select Intrusion Area from the **Device Type** drop-down list. The appropriate alarm state attributes and state conditions display.
5. Double-click on a pattern in the Symbols column to display the Attribute Panel window shown in [Figure 194](#).



**Figure 194.** Attribute Panel


6. Select the attributes that you want to apply, such as color, pattern, line, and brightness. The selection displays in the Samples pane. Refer to [Table 125](#) for instructions.
7. Select the **Blinking** check box if you want the pattern to blink when an alarm is generated.
8. Click **Apply All** to apply the selected attributes. The symbol displays in the **Initial State Icon** window. The Graphics Editor will use this image to represent the scheme.
9. Select the **Active** check box to display the Attribute Panel window. Select the attributes that you want to apply, such as color, pattern, line, and brightness. The selection displays in the Samples pane.
  - This image displays on the map when an alarm is generated

and the state condition changes.

- The **Active** check box displays a check mark indicating this image has been associated with the alarm state condition.
10. Click **Save** when you are finished. If you want to create a symbol scheme for another intrusion area, click **New** to clear the information and continue making new selections.

Table 125 lists and describes the elements in the Graphic Attributes window.

**Table 125.** Graphic Attributes elements and description

Element	Description
<b>Line Color</b>	Click <b>Line Color</b> to display the Edit Line Color palette. Select a line color and click <b>OK</b> .
<b>Fill Color</b>	Click <b>Fill Color</b> to display the Fill Line Color palette. Select a fill color and click <b>OK</b> .
<b>Pattern Transparency</b> 	Click to display the fill color in the drawn image or a shape drawn with the Create Hyperlink Area tool. Click to remove the fill color. When you remove the fill color, only the pattern displays with a white background.
<b>Patterns</b>	Click to apply a pattern to the image. Use <b>Line Color</b> to select a color for the pattern.
<b>Line Styles</b>	Select the line type such as, solid, dotted, or arrows.
<b>Brightness</b>	Use the slider to indicate the brightness of the line and fill color. 100 is the brightest.
<b>Blinking</b>	Select this check box if you want the area to “blink” when it is in an alarm state.

## Managing Symbol Editor Files

Symbol schemes are stored on the local system, until they are uploaded to the server system for centralized storage and backup. Once the files are uploaded they are available to use with the Graphics Editor to create site maps and associate symbols.

After a symbol scheme has been uploaded to the server system, if you need to modify the symbol scheme, make sure you download the most current version before making changes.

Refer to the following sections for more information:

- [Uploading a Symbol Scheme](#)
- [Downloading a Symbol Scheme on page 294](#)
- [Deleting a Symbol Scheme on page 295](#)

### Uploading a Symbol Scheme

► **To upload a symbol scheme to the Facility Commander server, follow these steps:**

1. From the **Symbol Schemes** column, select the scheme name you want to upload to the server.
2. Select **File** and then **Upload**, or select the **Upload** icon from the toolbar. A window with this message displays: **Are you sure you want to upload current scheme?**
  - If the scheme has already been uploaded to the server, this message displays: **Are you sure you want to overwrite the server symbol scheme - file name?**
3. Click **Yes** to upload the symbol scheme to the server for distribution.

Next, use the Graphics Editor to associate the symbol scheme to a map. Refer to [Using the Graphics Editor on page 301](#) for instructions.

### Downloading a Symbol Scheme

► **To download a symbol scheme, follow these steps:**

1. From the **File** menu, select **Download** or select the **Download** icon from the toolbar. The window shown in [Figure 195 on page 295](#) displays.



**Figure 195.** Input window

2. Use the drop-down list to select which symbol scheme you want to download from the server. Click **OK**. The file is copied from the server system to your local system.

## Deleting a Symbol Scheme

- **To delete a symbol scheme from the local system, follow these steps:**
  1. Select the scheme you want to delete from the Symbol Schemes list. The information for this record displays.
  2. From the **File** menu, select **Delete** or select the **Delete** icon from the toolbar. A window displays a message asking: **Are you sure you want to remove this scheme?** Click **Yes** to remove the scheme.
    - This removes the symbol scheme from the local system only. If it has been uploaded to the server system and you want to delete it, the file must be removed using Delete Resources.
  3. From the **File** menu, select **Exit** to close the Symbol Editor window.

## State Associations and Conditions

Table 126 lists and describes the event sources, state attributes, and conditions.

**Table 126.** Event Sources, State Attributes, and Conditions

Event Source	State Attributes	Conditions
Camera	Initial State	
	Motion Detection	Set, Reset
	Video Loss	Set, Reset
Intercom Exchange	Initial State	
	Communication Failure	Set, Reset

**Table 126.** Event Sources, State Attributes, and Conditions (Continued)

Event Source	State Attributes	Conditions
	Intercom Exchange Reset	Set
Intercom Master Station	Initial State	
	Busy	Set
	Call Answered	Set
	Call Connected	Set
	Call Ringing	Set
	Call To Busy	Set
	Call To Private	Set
	Disconnected	Set
	Reset	Set
Intercom Substation	Initial State	
	Busy	Set
	Call Answered	Set
	Call Button Alarm	Set, Reset
	Call Button Event	Set
	Call Connected	Set
	Call Ringing	Set
	Call To Busy	Set
	Call To Private	Set
	Disconnected	Set
	Reset	Set
Intrusion Area	Initial State	
	State Armed All Clear	Set
	State Armed and In Alarm	Set
	State Disarmed	Set
	State Unknown	Set



**Table 126.** Event Sources, State Attributes, and Conditions (Continued)

Event Source	State Attributes	Conditions
Intrusion DGP	Initial State	
	DGP Bypassed	Set, Reset
	DGP Offline Alarm	Set, Reset
	DGP Tamper Alarm	Set, Reset
	Main Power Failure Alarm	Set, Reset
Intrusion Input	Initial State	
	Input Alarm	Set
	Input Alarm Event	Reset
	Input Bypassed	Set, Reset
	Input Tamper	Set, Reset
Intrusion Keypad	Initial State	
	Intrusion Duress Alarm	Set, Reset
	Intrusion Keypad Bypassed	Set, Reset
	Intrusion Keypad Offline	Set, Reset
	Keypad Tamper Alarm	Set, Reset
Intrusion Output	Initial State (No state attributes.)	
Intrusion Panel	Initial State	
	Duress Code Entered Alarm	Set, Reset
	Offline Alarm	Set, Reset
	Tamper Alarm	Set, Reset
Monitor	Initial State (No state attributes.)	
Picture Perfect Digital Input	Initial State	
	Input Alarm	Set, Reset, Tamper
Picture Perfect Digital Output	Initial State (No state attributes.)	

**Table 126.** Event Sources, State Attributes, and Conditions (Continued)

Event Source	State Attributes	Conditions
Picture Perfect Door Access Point	Initial State	
	Door Forced Alarm	Set, Reset
	Door Held Alarm	Set, Reset
	Door Prealarm	Set, Reset
	Invalid Badge Alarm	Set
	Lost Badge Alarm	Set
	Suspended Badge Alarm	Set
	Unknown Badge Alarm	Set
Picture Perfect Logical Input	Initial State	
	Logical Input Alarm	Set, Reset, Tamper

# Chapter 15. Creating Graphic Displays

This chapter describes how to create or import a site map and link symbols created with the Symbol Editor to represent access points, cameras, and other devices. Readers should be familiar with using other graphic drawing programs.



---

**In this chapter:**

- [Overview on page 300](#)
- [Using the Graphics Editor on page 301](#)
- [Drawing Tools on page 305](#)
- [Graphic Attributes on page 306](#)
- [Creating a Graphic Display on page 308](#)
- [Importing AutoCAD Drawings on page 314](#)
- [Linking Graphic Displays on page 318](#)
- [Building Hierarchical Displays on page 320](#)
- [Working with Layers on page 323](#)
- [Managing Graphic Display Files on page 326](#)
- [Editing Graphic Display Records on page 330](#)

## Overview

This feature allows you to design site maps of your premises and associate graphic images (symbols) to access points and their locations. When an alarm event occurs, one or more of the icons will change its appearance based on the alarm state condition, if configured to do so.

[Table 127](#) lists the steps needed to complete a graphic display and references to where you will find detailed instructions to complete these tasks.

**Table 127.** Task Overview

✓	Create symbol scheme and upload to the server. Refer to <a href="#">Using the Symbol Editor on page 287</a> for more information.
✓	Import a site map or graphic image, which becomes the background layer in the Graphic Editor. <ul style="list-style-type: none"><li>Refer to <a href="#">Importing AutoCAD Drawings on page 314</a> for instructions to import existing drawings with DXF extensions.</li><li>You can also use the drawing tools to create a graphic display. Refer to <a href="#">Drawing Tools on page 305</a> for more information.</li></ul>
✓	Place symbols representing access points, cameras, and more. Symbols can be grouped on different layers to improve visibility when viewing the completed graphic displays. Add text labels, if needed. Refer to the following sections: <ul style="list-style-type: none"><li><a href="#">Creating a Graphic Display on page 308</a>,</li><li><a href="#">Associating Access Points and Other Devices on page 309</a></li><li><a href="#">Associating Camera Devices on page 310</a></li><li><a href="#">Associating Intercom Devices on page 311</a></li><li><a href="#">Configuring Intrusion Keypads on page 266</a></li><li><a href="#">Adding Text Labels to the Site Map on page 313</a></li></ul>
✓	Save file and upload completed graphic display to the server. Refer to <a href="#">Managing Graphic Display Files on page 326</a> for more information.
✓	Link two graphic displays together using the Create Hyperlinks icon. Refer to <a href="#">Linking Graphic Displays on page 318</a> for more information.
✓	Build hierarchal graphic displays using the Create Hyperlink Area icon. Refer to <a href="#">Building Hierarchical Displays on page 320</a> .

## Using the Graphics Editor

The Graphics Editor allows you to associate symbol schemes to site maps. The symbol scheme identifies icons that represent doors, cameras, or other device in different alarm conditions. These icons are associated with an event type and when an alarm is generated, the appropriate icon displays on the site map.

For example, a scheme with icons representing doors in an alarm state may include a:

- gray door to represent the initial state
- red door to represent a set condition
- green door to represent a reset condition

When an alarm is generated at the specific door access point, the appropriate icon for the state condition displays on the map. Refer to [Creating a Symbol Scheme on page 291](#) for more information.

If you create site maps and link them in a hierarchal arrangement, the associated icons on each level also displays the icon in its alarm state condition. Refer to [Building Hierarchical Displays on page 320](#).

There are three ways to create a site map, which are:

- Create map with the drawing tools provided by the Graphics Editor.
  - Using the drawing tools, such as circles, lines, polylines, rectangles, and text entries, you can create a site map, or a graphical representation of your facilities. Refer to [Drawing Tools on page 305](#) for more information.
- Use an existing JPG or GIF graphics file.
  - Most professional drawing applications usually have the capability to save a drawing in a JPG or GIF format. Refer to [Create New Image Entry on page 302](#) for more information.
- Import DXF drawings created with AutoCAD®.
  - Site maps and drawings with a DXF extension can be imported if they are saved in a DXF R12 format using AutoCAD. Refer to [Importing AutoCAD Drawings on page 314](#) for instructions.

To achieve the best results in your site map, draw the map as close to the size of the window in which it will be displayed. If you are importing a JPG or GIF graphic image file, try to size the image to fit the window in which it will be displayed. Whenever possible, be consistent and keep all of your displays the same size.

### ► To open the Graphics Editor, follow these steps:

1. From the Facility Commander Launcher window, select **Launch** and **Graphics Editor**, or select the **Graphics Editor** icon from the Editors toolbar.
2. The Graphics Editor shown in [Figure 177 on page 302](#) window displays.

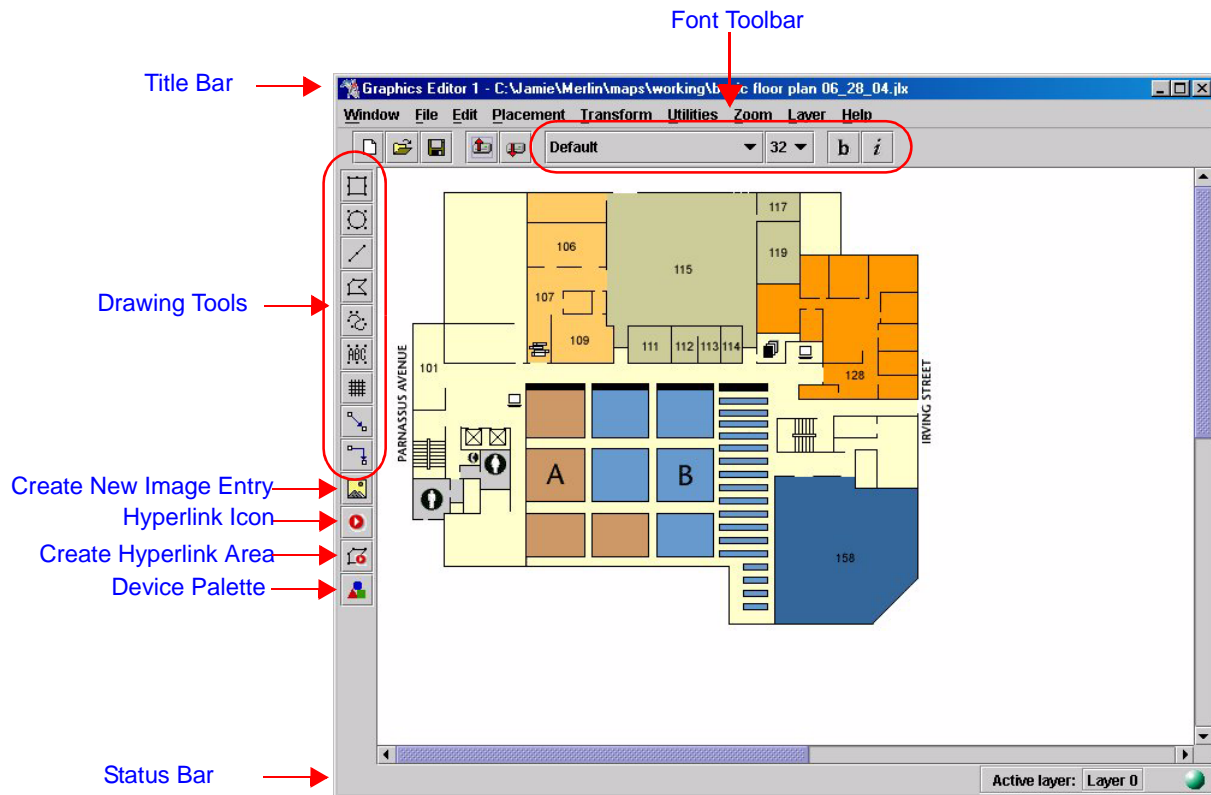
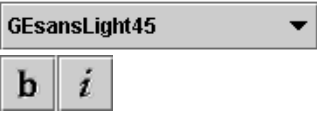






Figure 177. Graphics Editor window

Table 128 lists and describes the Graphics Editor icons and tooltips.


Table 128. Graphics Editor icons, tooltips, and descriptions

Element	Description
<b>Title Bar</b>	Displays the program name and window instance number. Refer to <a href="#">Client Application Title Bars on page 21</a> for more information.
<b>Font Toolbar</b> 	Use the drop-down lists to select a font type and font size. The available fonts are determined by the workstation where the Graphics Editor is being used to create drawings.  If fonts used in the drawing are unavailable on the workstation where the drawing is displayed, substitute fonts are used.  Select the icons to make the font <b>bold</b> or <i>italic</i> .
<b>Drawing Tools</b>	Refer to <a href="#">Drawing Tools on page 305</a> for instructions on how to use these drawing tools.
<b>Create New Image Entry</b> 	Click the <b>Create New Image Entry</b> icon to display the Open window, which allows you to select a GIF or JPG file to use as the site map.

**Table 128.** Graphics Editor icons, tooltips, and descriptions (Continued)

Element	Description
<b>Hyperlink Icon</b> 	<p>Use the Hyperlink icon to link two or more site maps together. A graphic image or icon displays on the site map when it is viewed with the Graphics Viewer. Click the graphic image or icon on the default site map and the associated site map displays.</p> <p>You can choose to have the associated site map display in the current Graphics Viewer window or to launch a new Graphics Viewer window.</p> <p>Refer to <a href="#">Linking Graphic Displays on page 318</a> for instructions on how to link site maps together.</p>
<b>Create Hyperlink Area</b> 	<p>Use the <b>Create Hyperlink Area</b> icon to draw a border around an irregular shape, creating a custom hyperlink path or border on a site map.</p> <ul style="list-style-type: none"> <li>Click the <b>Create Hyperlink Area</b> icon and move the mouse cursor to the drawing area.</li> <li>Click and drag the mouse to draw a line.</li> <li>Click again to create an anchor point and continue until the border (or path) is complete.</li> <li>Right-click to release the drawing tool. The shape automatically fills with the defined graphic attributes.</li> </ul> <p>Refer to <a href="#">Building Hierarchical Displays on page 320</a> for additional instructions.</p>
<b>Device Palette</b> 	<p>Use to display the Device Palette window. The Device Palette window displays the initial state icons for each scheme created using the Symbol Editor.</p> <p>Tabs used to group the devices include:</p> <ul style="list-style-type: none"> <li>Cameras</li> <li>Door Access Points</li> <li>Digital Inputs</li> <li>Logical Inputs</li> <li>Digital Outputs</li> <li>Intercom Devices</li> <li>Intrusion Devices</li> </ul> <p>Use the tooltips to identify the scheme name.</p>

**Table 128.** Graphics Editor icons, tooltips, and descriptions (Continued)

Element	Description
<b>Status Bar</b>	
	<p>Displays the layer number or name currently active (or visible).</p> <ul style="list-style-type: none"><li>• To change layers, select <b>Layer Settings</b> from the <b>Layer</b> menu. Refer to <a href="#">Working with Layers on page 323</a>.</li></ul> <p>Displays an icon indicating if the system with the Graphics Editor is connected to the Facility Commander server.</p> <ul style="list-style-type: none"><li>• Green indicates the Graphics Editor is communicating with the server.</li><li>• Red indicates the Graphics Editor is no longer communicating with the server.</li></ul>



## Drawing Tools







The Graphics Editor provides drawing tools to create site maps or other graphic displays.

► **To use the drawing tools, follow these steps:**




1. Select the appropriate icon. You must select a tool each time before moving to the drawing area.
2. Position the mouse where you want to begin drawing. Follow the instructions listed in [Table 129](#) to use the tools.

[Table 129](#) lists and describes the Graphics Editor drawing tools.

**Table 129.** Drawing tools description

Tool	Description
<b>Rectangle</b> 	Use to draw a rectangle or a square. <ul style="list-style-type: none"> <li>• To create a rectangle, use the mouse to click and drag to reach the correct size.</li> <li>• To create a square, click and hold the <b>Shift</b> key while dragging the mouse.</li> </ul>
<b>Circle</b> 	Use to draw a circle or an ellipse. <ul style="list-style-type: none"> <li>• To draw a circle, click and hold the <b>Shift</b> key while dragging the mouse.</li> <li>• To draw an ellipse, click and drag the mouse to reach the correct size.</li> </ul>
<b>Line</b> 	Use to draw a horizontal, vertical, or diagonal line. <ul style="list-style-type: none"> <li>• Click to begin the line and drag the mouse to the correct location to end the line.</li> </ul>
<b>Polyline</b> 	Use to create a free-form shape. <ul style="list-style-type: none"> <li>• Click in the drawing area and begin to move mouse to create the shape.</li> <li>• When one side is complete, left-click to change direction.</li> <li>• When finished, right-click to complete the shape.</li> </ul>
<b>New Path</b> 	Use to create a set of straight, cubic, or quadratic segments. The Path Tools window displays with four segment types: straight line, isometric, two-dimensional, and three-dimensional. <ul style="list-style-type: none"> <li>• Left-click to create each point. Right-click to complete the shape.</li> </ul>
<b>Text Entry</b> 	Use to add text to the drawing. <ul style="list-style-type: none"> <li>• Click in the drawing area and the Text Input window displays. Enter the text you want to add to the drawing and click <b>OK</b>.</li> <li>• Resize the text by stretching or shrinking the text in the drawing area.</li> </ul>

**Table 129.** Drawing tools description (Continued)

Tool	Description
<b>Array</b> 	<p>Use to draw a grid with four columns and four rows. This can be a square or rectangle shape.</p> <ul style="list-style-type: none"> <li>Click in the drawing area where you want the grid to display and move the mouse until the grid is the size you want.</li> <li>Resize by stretching or shrinking the grid in the drawing area.</li> </ul>
<b>Link</b> 	<p>Use to connect objects. This option groups objects together so they can be moved together, instead of moving each object individually.</p> <ul style="list-style-type: none"> <li>Click the icon and all the objects in the drawing area are selected.</li> <li>From the <b>Transform</b> menu, select <b>Group</b>. The objects are now linked, or grouped together.</li> </ul>
<b>Orthogonal Link</b> 	<p>Use to link objects together. Choose a direction, either horizontal or vertical, for the first segment; following segments will use the same direction as the first segment.</p>

## Graphic Attributes

When you use any of the drawing tools or the Create Hyperlink Area icon to create a drawing, you can change the appearance of the drawing using the Graphics Attributes window.

► **To use the Graphic Attributes window, follow these steps:**

1. Double-click the image to display the Graphic Attributes window as shown in [Figure 178 on page 307](#). If you want to select more than one image, click and drag in the drawing area to include other images.
2. Select the attributes that you want to apply, such as color, pattern, line, and brightness. Refer to [Table 130](#) for instructions.
3. Click **Apply All** to apply the selected attributes. Click **Close** when finished.

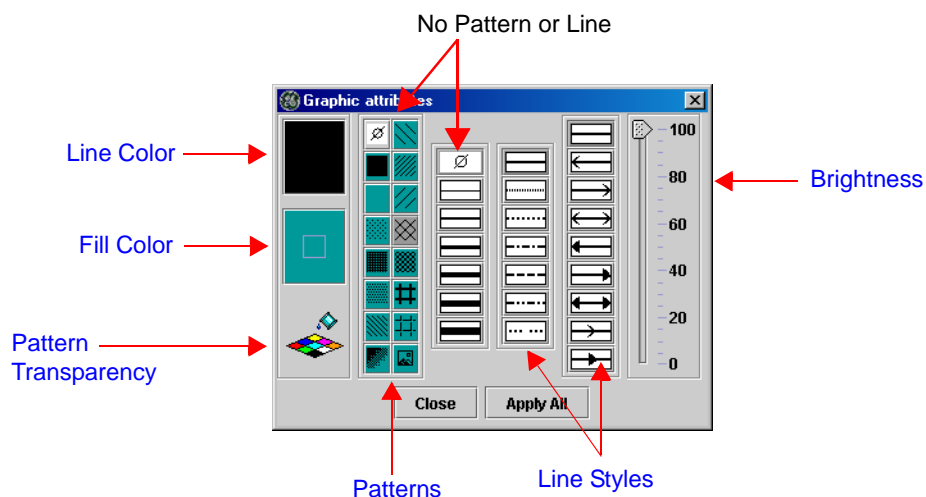



Figure 178. Graphic Attributes window

Table 130 lists and describes the elements in the Graphic Attributes window.

Table 130. Graphic Attributes elements and description

Element	Description
<b>Line Color</b>	Click <b>Line Color</b> to display the Edit Line Color palette. Select a line color and click <b>OK</b> .
<b>Fill Color</b>	Click <b>Fill Color</b> to display the Fill Line Color palette. Select a fill color and click <b>OK</b> .
<b>Pattern Transparency</b> 	Click to display the fill color in the drawn image or a shape drawn with the Create Hyperlink Area tool. Click to remove the fill color. When you remove the fill color, only the pattern displays with a white background.
<b>Patterns</b>	Click to apply a pattern to the image. Use <b>Line Color</b> to select a color for the pattern.
<b>Line Styles</b>	Select the line type such as, solid, dotted, or arrows.
<b>Brightness</b>	Use the slider to indicate the brightness of the line and fill color. 100 is the brightest.

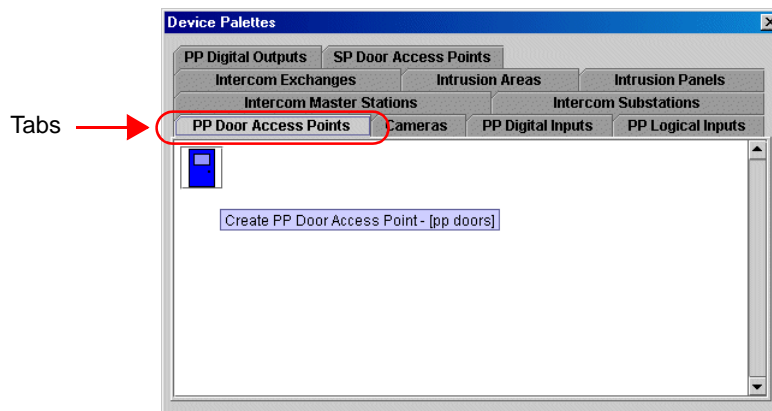
## Creating a Graphic Display

*A graphic display is composed of a basic site map and the symbols that represent devices or access points.*

Symbol schemes must be created before this step to identify the symbols that will be used with the display. If the symbols do not display, use the Symbol Editor to upload the symbol scheme to the Facility Commander server.

► **To create a graphic display, follow these steps:**

1. From the Facility Commander Launcher window, select **Launch** and **Graphics Editor**, or select the **Graphics Editor** icon from the Editors toolbar. The Graphics Editor window displays.
2. Using the Graphics Editor drawing tools, create the graphic display.
  - If you have an existing site map in a JPG or GIF format, use the **Create New Image Entry** icon to import the map file. Refer to [Create New Image Entry](#) in [Table 128](#) for more information on how to do this.
  - If you have an existing site map in a DXF format, refer to [Importing AutoCAD Drawings on page 314](#) for more information.
3. Select the **Device Palette** icon to display the Device Palettes window as shown in [Figure 179](#).



**Figure 179.** Device Palette window

4. Select the appropriate tab to display the symbols. Select the appropriate symbol; using tooltips to display the scheme name. After the symbol is selected, it displays in the upper-left hand corner of the drawing area.

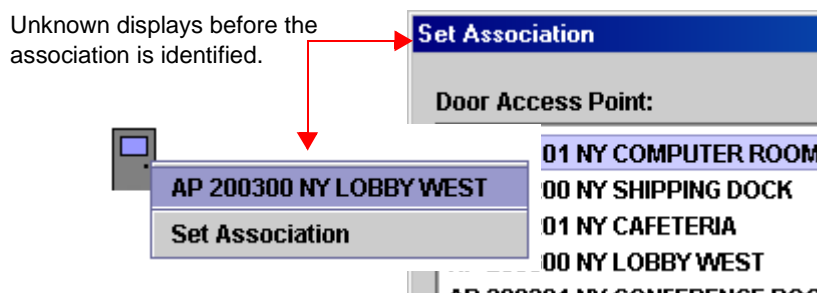
5. Drag the image to the appropriate location on the site map.
  - If the image represents an access point, refer to [Associating Access Points and Other Devices on page 309](#).
  - If the image represents a camera, refer to [Associating Camera Devices on page 310](#).
  - If the image represents an intrusion area, refer to [Viewing Intrusion Areas on page 271](#).

## Associating Access Points and Other Devices

Use this option to associate a symbol icon to a specific access point, digital input, logical input, digital output, intercom, or intrusion devices.

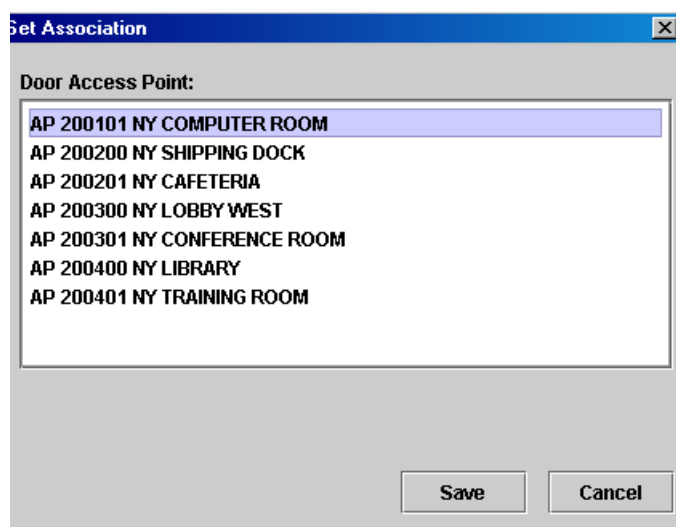
► **To associate a symbol icon to a specific point, follow these steps:**

1. Right-click on the icon to display the **Set Association** button as shown in [Figure 180](#).



**Figure 180.** Set Association button

2. Click **Set Association** to display the window shown in [Figure 181](#).



**Figure 181.** Set Association window

3. Use the list to select the access point that you want to associate with this symbol. Click **Save**.

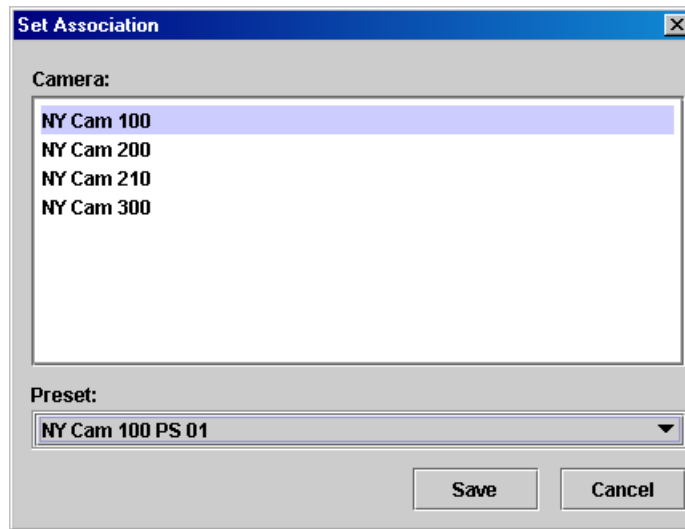
Continue to the next section if you are also defining cameras. If not, continue to [Adding Text Labels to the Site Map on page 313](#).

## Associating Camera Devices

Use this option to associate a symbol icon to specific cameras.

► **To associate a camera symbol to a specific camera, follow these steps:**

1. Right-click on the icon to display the **Set Association** button as shown in [Figure 180 on page 309](#).
2. Click **Set Association** to display the window shown in [Figure 182](#).



**Figure 182.** Set Association window

3. Select the camera from the list that you want to associate to this symbol. If the camera has preset positions, select the preset position from the **Preset** drop-down list.
4. Click **Save**.

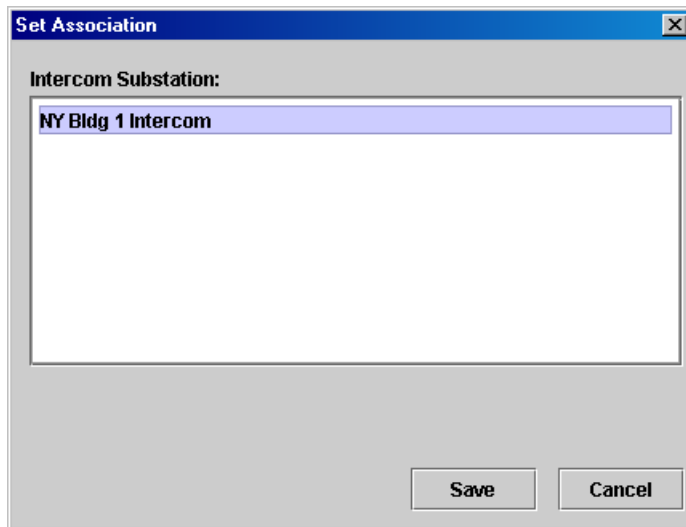
Continue to [Adding Text Labels to the Site Map on page 313](#).

## Associating Intercom Devices

Use this option to associate a symbol icon to specific intercom device.

► **To associate an intercom symbol to a specific intercom device, follow these steps:**

1. Right-click on the icon to display the **Set Association** button as shown in [Figure 180 on page 309](#).
2. Click **Set Association** to display the window shown in [Figure 183](#).



**Figure 183.** Set Association window

3. Select the intercom device from the list that you want to associate to this symbol.
4. Click **Save**.

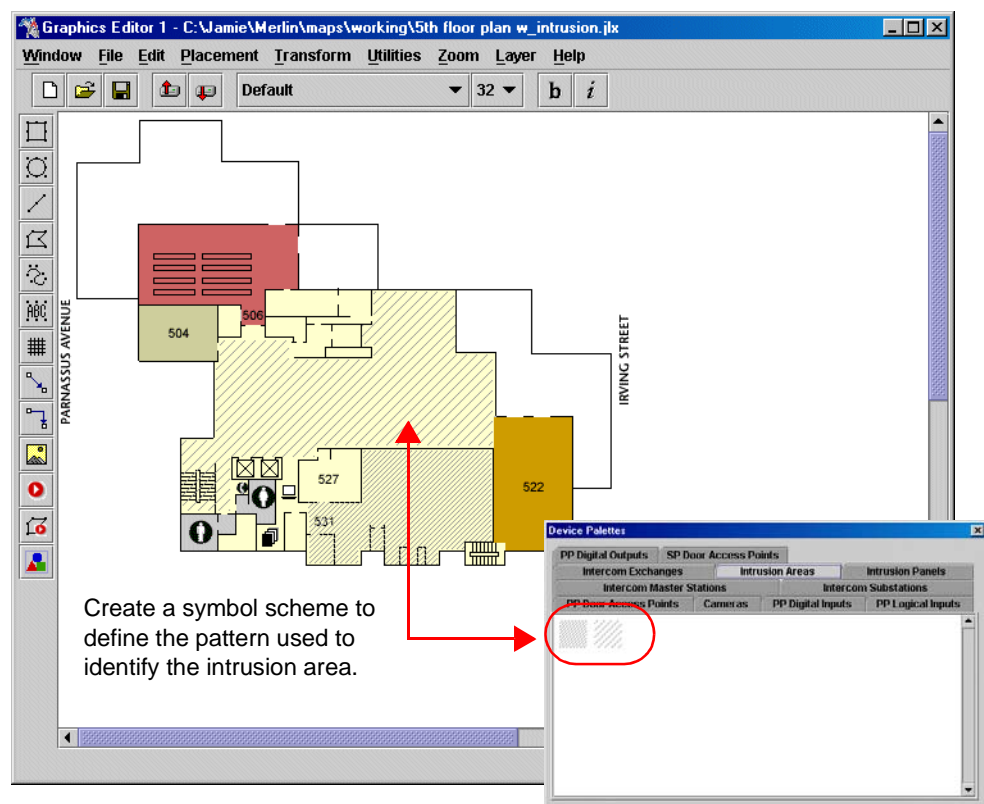
## Creating Intrusion Areas

A symbol scheme must be created before this step to identify the “fill pattern” to use with the display. A fill pattern may be a solid color, cross-hatch design, gradient fill, and more.

A symbol scheme usually identifies a symbol or icon to place on the graphic display representing a door access point or another device. However when you create an intrusion area, a pattern is used to identify the intrusion area state, such as Armed All Clear, Disarmed, and more.

➤ **To define an intrusion area, follow these steps:**

1. Select the **Device Palette** icon to display the Device Palette window as shown in [Figure 184](#).



**Figure 184.** Graphic Editor with defined intrusion area

2. Select the **Intrusion Area** tab to display the defined intrusion area symbols (or patterns). Select the appropriate symbol; using tooltips to display the scheme name.
3. Move the mouse cursor to the drawing area (the cursor changes to a crosshair shape). Click in the drawing area to create the first point on the site plan.
  - Trace the area using horizontal, vertical, or diagonal lines created by clicking to create an anchor point and moving the cursor to the next anchor point.



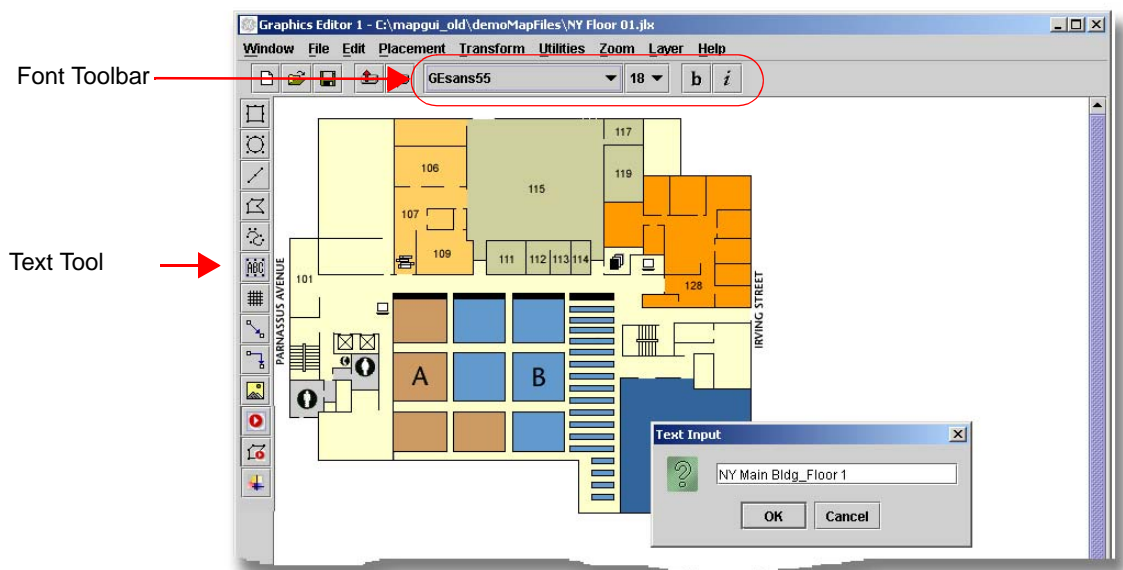
- Use the **Zoom** menu to increase the size of the display and make it easier to trace the border.
- Right-click to end the path when you are finished and apply the scheme.

## Adding Text Labels to the Site Map

This feature allows you to add a text label to identify the building name, identify a link to another site map, or identify a particular symbol icon on the site map.

► **To add a text label follow these steps:**

1. Select the **Text Tool** icon on the Graphics Editor toolbar.



**Figure 185.** Adding text to drawing in Graphics Editor window

2. Click in the drawing area where you want to place the text label. The mouse pointer changes to a crosshair shape and the **Text Input** window as shown in [Figure 185](#) displays.
3. Enter the text to use as the label or description of the symbol. Click **OK**.
4. The text displays on the drawing area with an active border surrounding the text. Select the text and move it to the correct position. Use the **Font** toolbar to change the text attributes.
  - Use the **Font** drop-down list to select the font.
  - Use the **Size** drop-down list to select the font size.
  - Click the **Bold** icon to change the font to bold.
  - Click the **Italic** icon to change the font to italics.

Continue to the next section to save the site map.

## Saving the Site Map

➤ **To save the file, follow these steps:**

1. From the **File** menu and select **Save**. The Save window displays.
2. Enter the file name. Click **Save**. The file is automatically saved with a J LX extension. When an alarm event is generated, the icon associated with the alarm state displays on the map.

## Importing AutoCAD Drawings

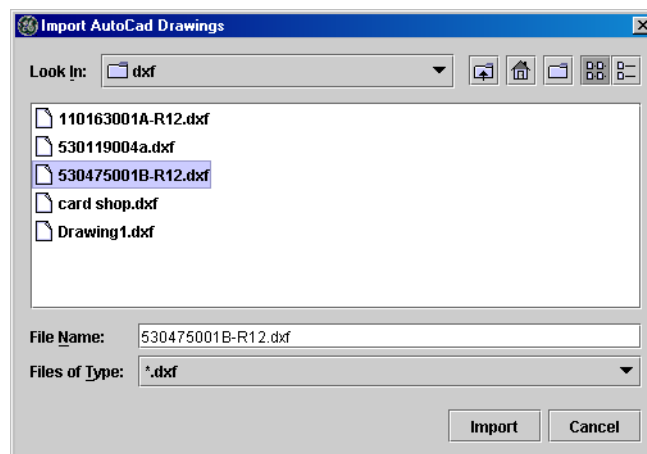
Facility Commander allows you to import site maps, or drawings, created with AutoCAD. Only two-dimensional drawings are supported; model information in drawings is not used.

When you import an AutoCAD drawing, it must be saved in a DXF R12 format, you can select which layers you want to import. If you want the site map or drawing to remain as one object, no further steps are required.

However, if you want to maintain the layers, use the Edit Objects feature after the drawing is imported. These layers can be deleted later if not used. Imported layer names cannot be changed. Refer to [Maintain Layers in AutoCAD Drawings on page 317](#) for more information.

➤ **To import an AutoCAD drawing, follow these steps:**

1. From the **File** menu, select **Import AutoCAD Drawings**. The window in [Figure 186](#) displays.



**Figure 186.** Import AutoCAD Drawings window

2. Select the drawing name you want to import. The name displays in the **File Name** field. Click **Import**. The Drawing Limits window shown in [Figure 187 on page 315](#) displays.

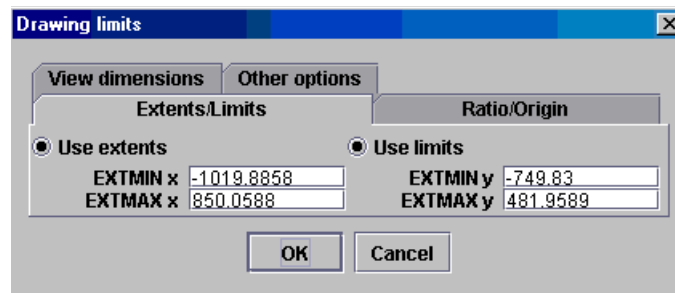
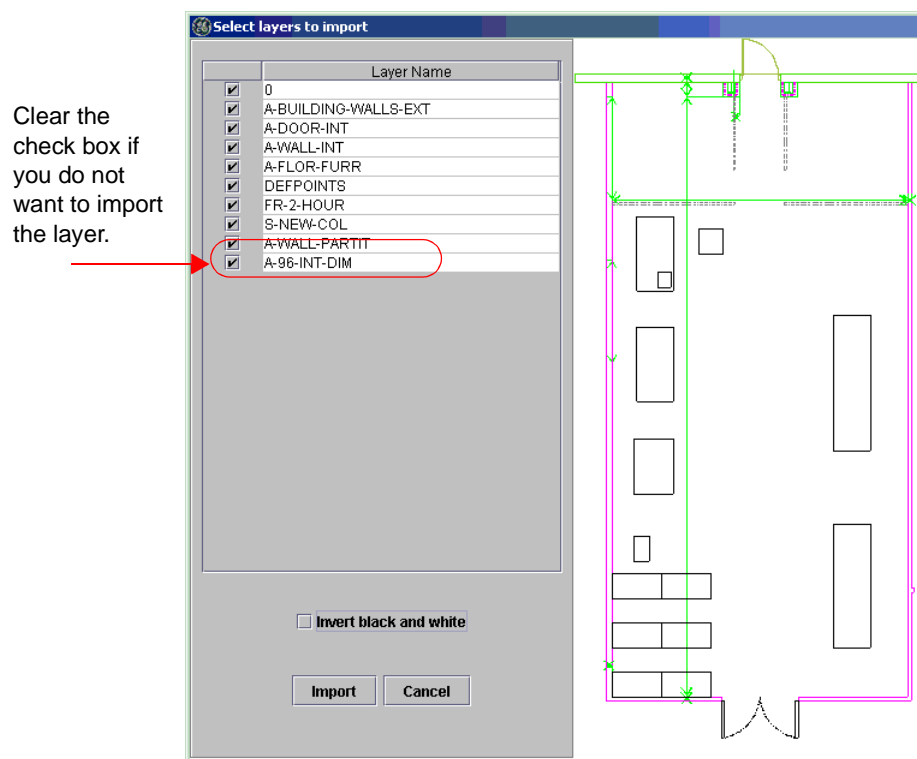


Figure 187. Drawing limits window

- Use the **Extents/Limit** tab to change the original coordinate system, which is taken from the imported DXF file.
  - Use the **Ratio/Origin** tab to indicate if the aspect ratio of the original drawing should be maintained.
  - Use the **View Dimensions** tab to convert the DXF file coordinates to coordinates used by the Graphic Editor.
  - Use the **Other Options** tab to select the **Invert black and white** check box. Select this check box to change the color attributes. If the text map is not visible, such as a drawing with white ruling lines, select the check box to invert the black and white attributes of the drawing.
3. Click **OK**. The **Select Layers to Import** window shown in [Figure 188 on page 316](#) displays.



**Figure 188.** Select Layers to Import window

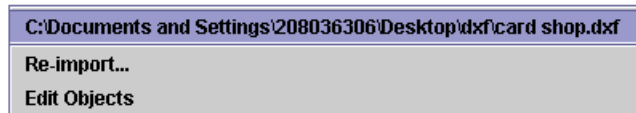
4. The Select Layers to Import window lists each of the multiple layers in the drawings. To import all the layers, click **Import**.
  - To import some of the layers, clear the check boxes of the layers you do not want to import. Only layers with check marks are imported. The display area reflects the changes in layers as you select or clear the check boxes.
5. When the imported drawing is displayed, you can re-import the drawing immediately if necessary. Right-click on a path in the drawing or a border. The shortcut menu in [Figure 189 on page 317](#) displays. (*This menu is not accessible again after you select the Edit option.*)
6. Select **Re-Do** and the Open window in [Figure 186 on page 314](#) displays. The imported drawing's name is highlighted. You can either re-import the same drawing or select a different one.
7. Click **Open** to re-import the drawing and the Select Layers to Import window shown in [Figure 188](#) displays. Click **Open** to re-import the drawing.

## Maintain Layers in AutoCAD Drawings

Use the Edit Object feature to maintain the layers in the AutoCAD drawings, otherwise the drawing is treated as one object.

► **To maintain the layers in the AutoCAD drawings, follow these steps:**

1. Right-click on a border or path in the drawing. The shortcut menu in [Figure 189 on page 317](#) displays. (This menu is not accessible again after you select the **Edit** option.)

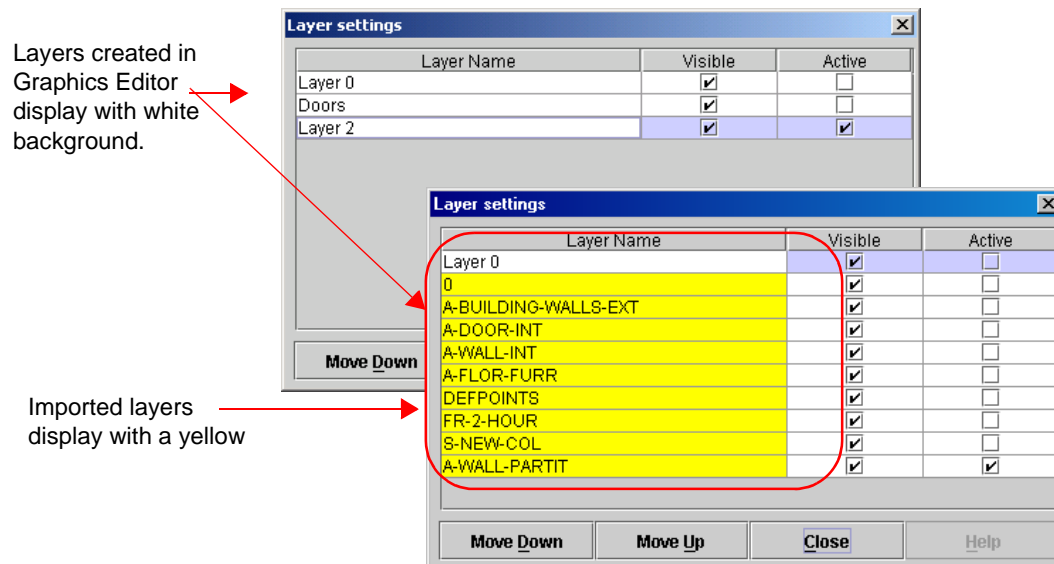


**Figure 189.** Import DXF menu options

2. Select **Edit Objects**. If you do not select this option, the drawing remains as a single object on one layer. When this option is selected, Facility Commander identifies each layer of the imported drawing.

**Note:** Importing a drawing with each separate layer may take some time to complete.

3. From the **Layer** menu, select **Layer Settings**. The window in [Figure 190](#) displays.



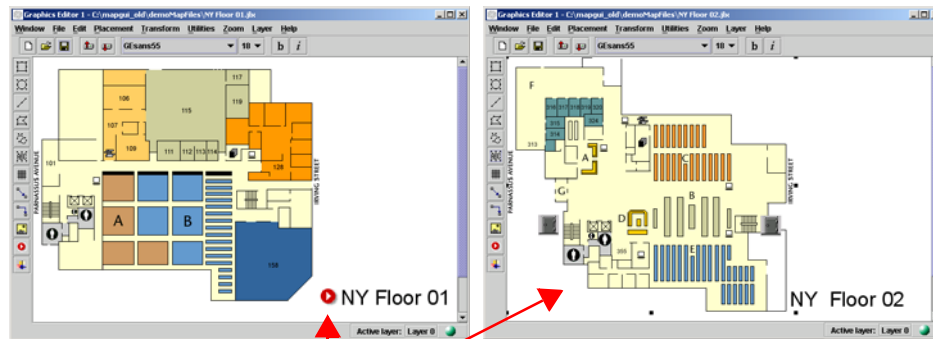
**Figure 190.** Layer Settings with imported and non-imported layers

4. To display a layer, select the appropriate **Visible** check box and the Graphics Editor displays the selected layer.
5. To modify a layer, select the appropriate **Active** check box and the Graphics Editor displays the active layer. The remaining layers are visible while you make changes to the selected layer.
  - To view all the items on the active layer, select the **Edit** menu and then **Select All**. All the items on this layer are highlighted.

## Linking Graphic Displays

Using the **Create Hyperlink** icon in the Graphics Editor application, you can link two displays together. (You can replace the hyperlink icon with another icon or graphical image.)

When an alarm event is generated, the Graphics Viewer opens and displays the specified graphic display. To link another site map, select the hyperlink symbol and the linked graphic display appears in the same Graphics Viewer window or a new window. Refer to the illustration shown in [Figure 191](#).



Click the hyperlink symbol to display the associated map or graphic display. (NY Floor 01 is linked to NY Floor 02.)

**Figure 191.** Hyperlink icon and associated graphic display

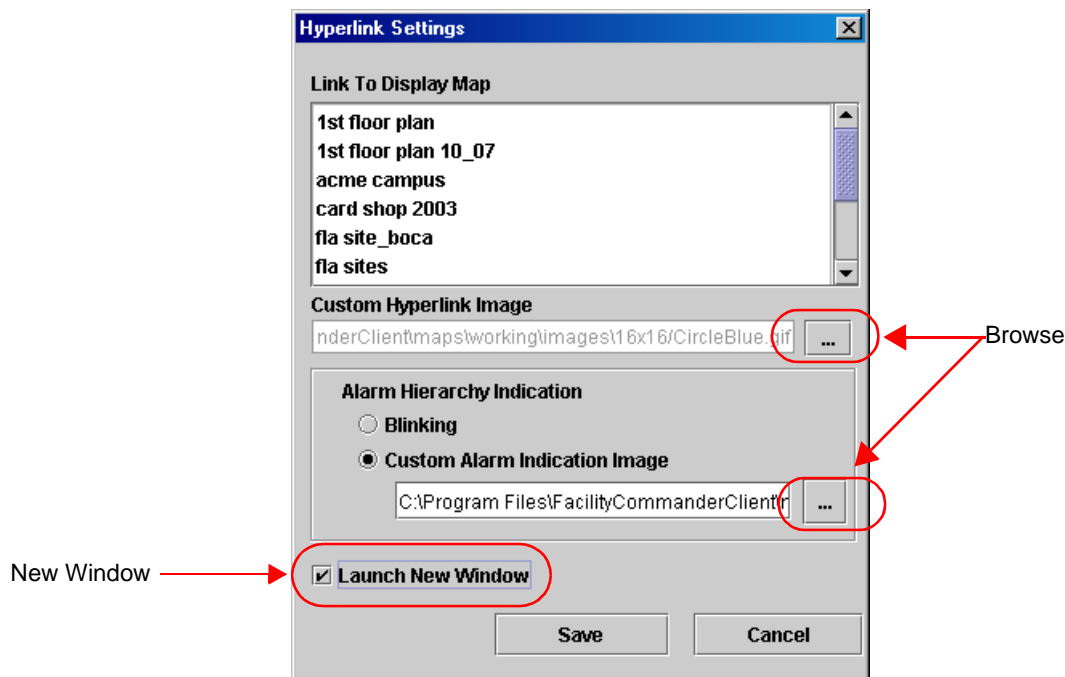
► **To link graphic displays to each other, follow these steps:**

1. From the **Facility Commander Launcher** window, select **Launch** and **Graphics Editor**. The Graphics Editor shown in [Figure 177](#) on page 302 displays.
2. Click **File** and then **Open**.
3. Select the map file you want to use. The file will have a JLX extension.
4. Click the **Create Hyperlink** icon on the toolbar as shown in [Figure 192](#). The icon displays in the upper-left hand corner of the drawing area.
5. Drag the icon to the appropriate location on the site map.
6. Right-click the **Create Hyperlink** icon to display the **Change Linking Properties** button as shown in [Figure 192](#).



**Figure 192.** Change Linking Properties button

7. Click **Change Linking Properties** to display the Hyperlink Settings window in [Figure 193 on page 319](#).



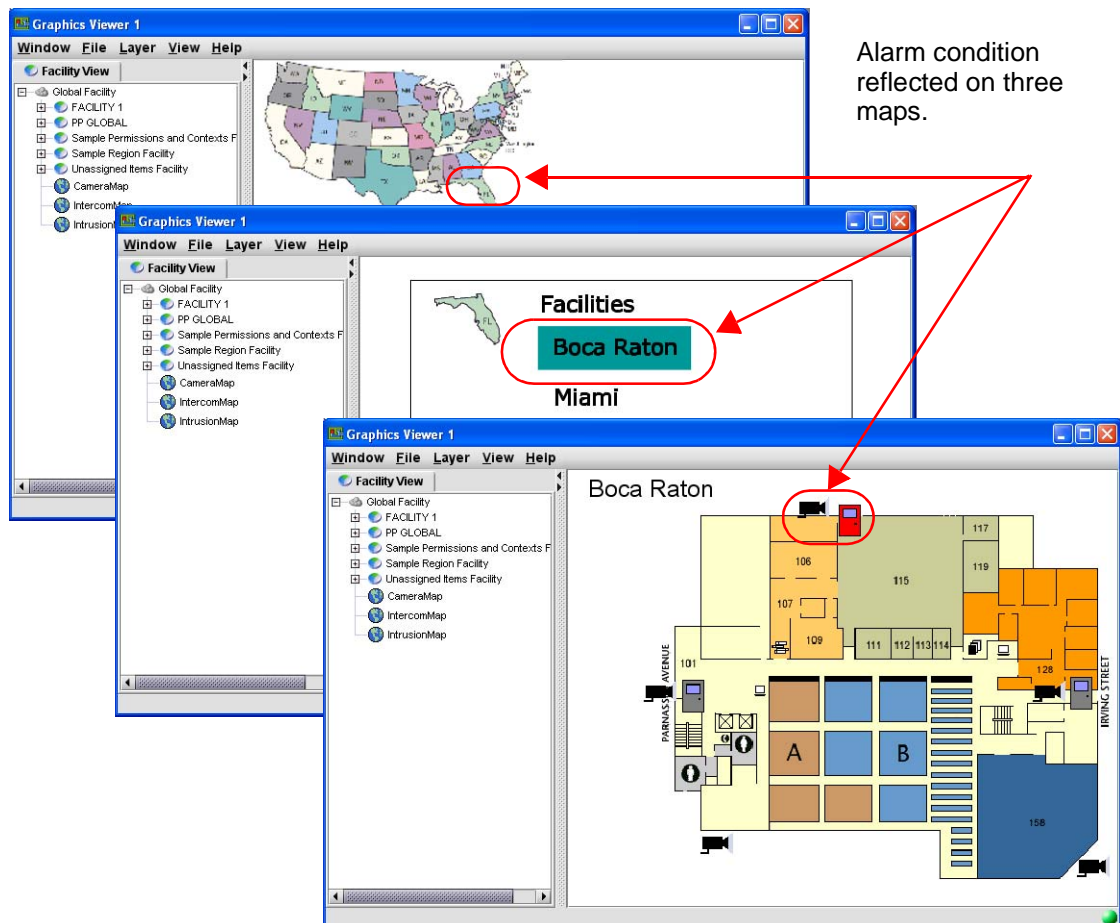
**Figure 193.** Hyperlink Settings window

8. Use the **Link to Display Map** list to select the site map you want to display when the hyperlink icon is selected on the Graphics Viewer.
9. To use a custom graphic image instead of the red hyperlink icon, use the **Browse** button to locate the graphic image. The path name displays in the **Custom Hyperlink Image** field. This icon displays on the site map representing a link to an associated map.
10. Select the appropriate option to indicate how the hyperlink image changes when an alarm event is generated. The options are:
  - Select **Blinking** if you want the hyperlink image to blink when an alarm event is generated.
  - Select **Custom Alarm Indication Image** if you want to select a different hyperlink image to display when an alarm event is generated. Use the **Browse** button to navigate to the folder with the graphic image you want to display on the site map representing an alarm event.
11. Select the **Launch New Window** check box if you want the associated site map to display in a new Graphics Viewer window.
  - If you want the associated site map to display in the same Graphics Viewer window, do not select this check box.
12. Click **Save**.
13. In the Graphics Editor window, use the text tool to add a label to identify the link. [Adding Text Labels to the Site Map on page 313](#).
14. Save your work and upload the new site map to the Facility Commander server for distribution.

## Building Hierarchical Displays

Using the **Create Hyperlink Area** icon in the Graphics Editor application to draw a hyperlink path around an object on a site map. This feature is useful to associate multiple site maps in a hierarchically arrangement.

When an alarm event occurs, the designated hyperlink icon reflects the alarm state condition on each level or site map in the hierarchy as shown in [Figure 188](#). If an alarm is generated at an access point or other device on a lower-level map, the alarm condition displays on each level of the map.



**Figure 194.** Hierarchical map arrangement

In this example, there are three site maps — United States, Florida, and Boca Raton.

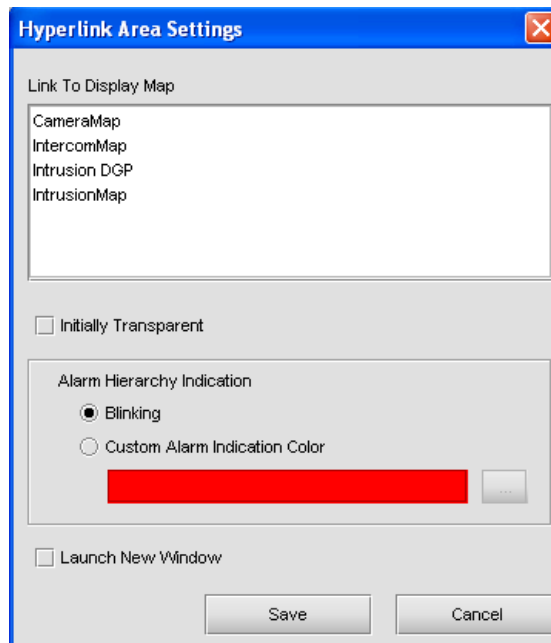
- The United States map has three states designated as hyperlink images, including California, Florida, and New York. When an alarm is generated in Boca Raton, the outline around Florida is configured to blink. The operator clicks the icon to display the Florida map.



- Florida is represented by a list of the facilities, including Boca Raton, Miami, and others. When an alarm occurs, the facility name is configured to blink. Operators select the name to view the graphic display.
- The Boca Raton graphic display represents the actual facility with associated access points and camera devices. The door access point where the alarm occurred is configured to change to a red door icon.

► **To build hierarchical graphic displays, follow these steps:**

1. From the **Facility Commander Launcher** window, select **Launch** and **Graphics Editor**. The Graphics Editor shown in [Figure 177 on page 302](#) displays.
2. From the **File** menu, select **Open**. The Open window displays.
3. Select the top-level map you want to use. The file will have a JLX extension.
4. Click the **Create Hyperlink Area** icon on the toolbar. Move the mouse cursor to the drawing area (the cursor changes to a crosshair shape). Click on the drawing area to create the first point on the site plan.
  - Trace the object using horizontal, vertical, or diagonal lines created by clicking to create an anchor point and moving the cursor to the next anchor point.  
Use the **Zoom** menu to increase the size and make it easier to trace an irregular shaped border.
  - When you are finished, right-click to end the path and apply the default graphic attributes.
  - Double-click in the area to display the Graphics Attributes window. Use to adjust border lines and change the default attributes, such as color, pattern, line, brightness, and more.  
Refer to [Graphic Attributes on page 306](#) for instructions.
5. Right-click to display the **Change Linking Properties** button. Click again to display the Hyperlink Area Settings window as shown in [Figure 195 on page 322](#).



**Figure 195.** Hyperlink Area Settings window

6. Use the **Link to Display Map** list to select the site map you want to display when the hyperlink image is selected on the Graphics Viewer.
7. Select the **Initially Transparent** check box if you want the hyperlink border to be transparent when there is no alarm condition. Clear the check box to display the hyperlink border.
8. Select how you want the alarm indication to display. The options are:
  - **Blinking** causes the hyperlink image to blink when an alarm event occurs.
  - **Custom Alarm Indication** allows you to select a color. The hyperlink border around the image changes to this color when an alarm event occurs.
    - Click the **Browse** button to display the Choose Alarm Color window. Select a color and click **OK**.
9. Select the **Launch New Window** check box if you want the associated site map to display in a new Graphics Viewer window.
  - If you want the associated site map to display in the same Graphics Viewer window, clear this check box.
10. Click **Save**.

## Working with Layers

Layers are defined as *single, transparent drawing surfaces that lay on top of one another*, much like pages in a notebook. Layers give you the ability to see each layer through the others above it, or see each layer individually. Layers allows you to move or edit objects on any layer without disturbing the objects on other layers.

A graphic display can be created with multiple layers to group access points, cameras, and inputs. When viewed using the Graphics Viewer, an operator can choose to view all the layers, or select a specific layer, such as only access doors. This improves visibility by hiding unnecessary details at a critical time.

Refer to the following topics for more information:

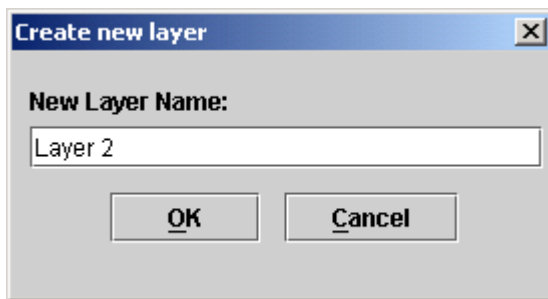
- [Creating a New Layer on page 323](#)
- [Selecting a Layer on page 324](#)
- [Renaming a Layer on page 325](#)
- [Removing a Layer on page 325](#)
- [Moving Objects Between Layers on page 326](#)

### Creating a New Layer

When the Graphics Editor opens, the drawing area that displays represents layer zero, or the background layer. Use this layer to display the building structure or site map. Create additional layers to display different objects, such as access points, camera, or inputs. Some site maps may not require multiple layers.

► **To create a new layer, follow these steps:**

1. From the **Layer** menu, select **Create New Layer** and the window shown in [Figure 196](#) displays with the layer number created when you selected this option.



**Figure 196.** Create New Layer window

2. Change the layer name to something more meaningful than Layer 2, such as Access Doors. Click **OK**.

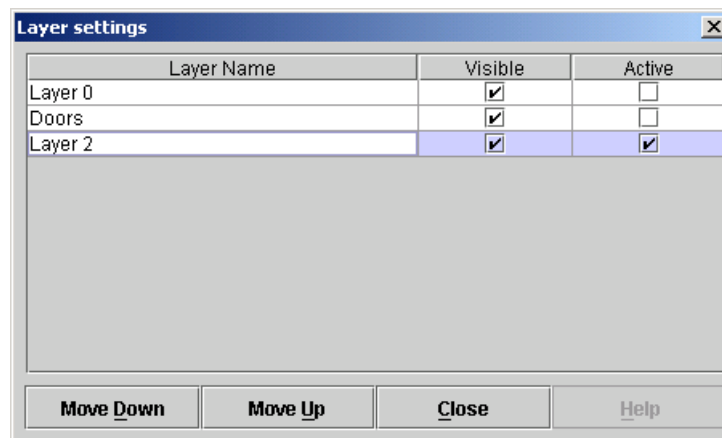
Refer to [Removing a Layer on page 325](#) for instructions on how to delete layers.

## Selecting a Layer

Use the layer setting feature to select one or all of the layers to display. When you are working with multiple layers, you will need to make a layer active before you can make changes to the layer. The layer setting feature also allows you to rearrange the layers by moving them up or down.

► **To select a layer, follow these steps:**

1. From the **Layer** menu, select **Layer Settings**. The window in [Figure 197](#) displays.



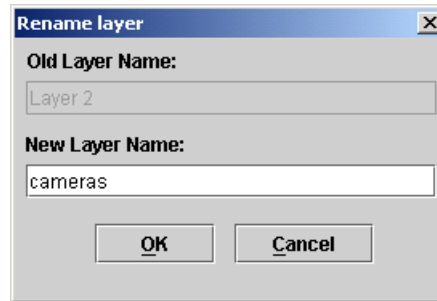
**Figure 197.** Layer settings window

2. To display a layer to view, select the appropriate **Visible** check boxes and the Graphics Editor displays the selected layers. To view all the layers, select all the check boxes.
3. To modify a layer, select the appropriate **Active** check box. The Graphics Editor displays the active layer. The remaining layers are visible while you make changes to the selected layer.
  - To view all the items on the active layer, select the **Edit** menu and then **Select All**. All the items on this layer are highlighted.
4. To rearrange the layers, click **Move Down** or **Move Up**.
5. Click **Close** when you are finished making changes.

## Renaming a Layer

➤ **To remove a layer, follow these steps:**

1. From the **Layer** menu, select **Rename Layer** and the window in [Figure 198](#) displays. The New Layer Name field displays the current layer name.



**Figure 198.** Rename Layer window

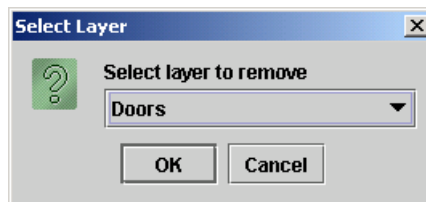
2. Type the new name in the **New Layer Name** field. Each layer name should be unique and no longer than 64 characters. If the name is longer, the extra characters will be truncated. The layer name is case sensitive.
  - Imported layers cannot be renamed.
3. Click **OK**.

## Removing a Layer

If you create too many layers or if you do not need all the layers in the graphic display, you can remove the extra layers. The last layer cannot be removed.

➤ **To remove a layer from your display, follow these steps:**

1. From the **Layer** menu, select **Remove Layer**. The Select Layer window in [Figure 199](#) displays with a drop-down list.



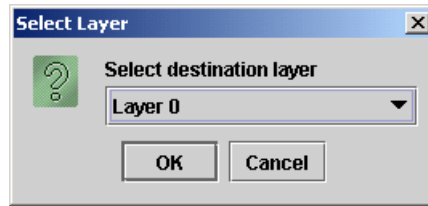
**Figure 199.** Select layer window

2. Use the drop-down list to select the layer you want to remove from the drawing.
3. Click **OK**.

## Moving Objects Between Layers

When you are working with multiple layers, you may want to rearrange the objects by moving them to another layer. *First, select the object you want to move and then follow these instructions.*

- **To move an object to a different layer, follow these steps:**
  1. From the **Layer** menu, select **Move Selected Objects**. The Select Layer window as shown in [Figure 200](#) displays.



**Figure 200.** Select Layer window

2. Use the drop-down list to select the correct destination layer. This is the location where the object will be moved.
3. Click **OK**.

## Managing Graphic Display Files

Graphic displays are stored on the local system until they are uploaded to the server system for centralized storage and backup. Once the files are uploaded they are available to use with the Graphics Viewer to view site maps and associated icons when an alarm event occurs.

When working with symbol schemes, use **Download** to make sure you are working with the most current scheme files.

Refer to the following sections for more information:

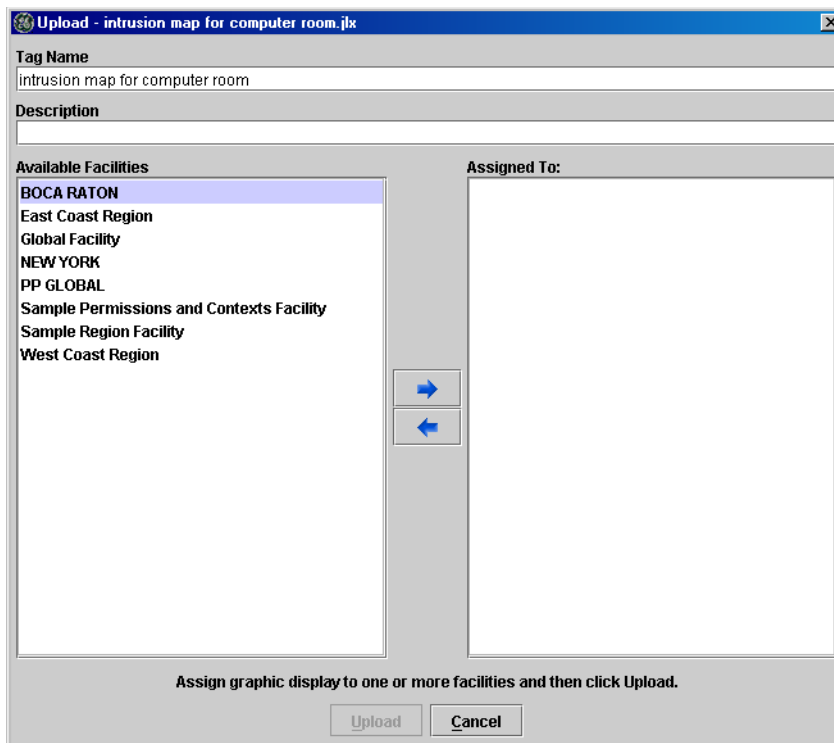
- [Uploading Graphic Displays](#)
- [Downloading Graphic Displays](#)
- [Deleting Unused Files on page 329](#)

## Uploading Graphic Displays

Graphic displays are stored on the local system, until they are uploaded to the server system. Once they are uploaded, they are available to use with the Graphics Viewer. The Graphics Editor automatically loads the most current symbol schemes from the server every time it opens.

- **To upload a site map to the server, follow these steps:**
  1. Display the site map you want to upload to the server. From the **File** menu, click **Open** and select the file you want to upload.

- From the **File** menu, click **Upload**. The Upload window as shown in Figure 201 displays. The graphic display file name appears in the title bar with a J LX extension.



**Figure 201.** Upload window

- Enter the information described in Table 131. The Upload window displays this message: **Assign graphic display to one or more facilities and then click Upload.**
- Use the arrow keys to add or remove facilities where this graphic display is assigned. Items can belong to more than one facility. Click **Upload**.
  - If the file exists already, this message displays: **This file already exists on the server, click Upload to overwrite.**

**Table 131.** Upload window fields and descriptions

Field Name	REQ	Description
<b>Tag Name</b>		Enter a unique name to identify this item. Use 2-36 characters. This is the name that displays in the navigation pane of the client applications.
<b>Description</b>		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
<b>Available Facilities</b>		Displays the list of facilities where this graphic display can be assigned. Facilities in this list depend on the operator's context and permissions.

**Table 131.** Upload window fields and descriptions (Continued)

Field Name	REQ	Description
Assigned To		Displays the list of facilities where this graphic display is assigned. Items can belong to more than one facility.

## Downloading Graphic Displays

Graphic displays should be downloaded from the server before they are edited to ensure you have the latest file.

► **To download a site map to your local system, follow these steps:**

1. Display the site map you want to upload to the server. From the **File** menu, click **Open** and select the file you want to upload.
2. From the **File** menu, select **Download** or select the **Download** icon from the toolbar. The Download window shown in [Figure 202 on page 328](#) displays.



**Figure 202.** Download window

3. Select the site map from the drop-down list and click **OK**. The selected site map displays in the Graphics Editor drawing window.

When you are finished making changes to the site map, upload the current file to the server so that it will be available to other Facility Commander client applications.



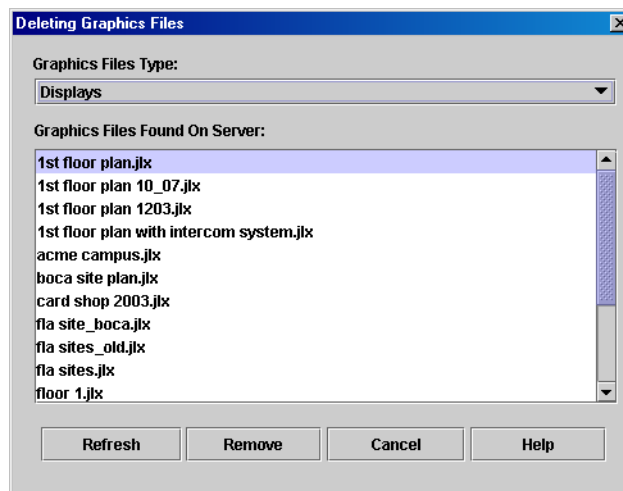
## Deleting Unused Files

The process of creating symbol schemes and graphic displays is an art, and during that process you may create some files that will not be used in your final product. The Graphics Editor provides the capability to remove unused files, which includes:

- **Displays** with JLN file extensions.
- **Images** with JPG, JPEG, or GIF file extensions.

➤ **To remove the files that are no longer needed, follow these steps:**

1. From the **File** menu, select **Deleting Graphics Files**. The Deleting Graphics Files window shown in [Figure 203](#) displays.



**Figure 203.** Deleting Graphics Files window

2. Select the Resource Type (Displays or Images) from the drop-down list. The site maps and images stored on the Facility Commander server display.
3. Highlight the entries you want to delete and click **Remove**.
  - Click **Refresh** to display an entries that may have changed on the server since this window displayed.
4. When you are finished removing the files, click **X** to close the window.

## Editing Graphic Display Records

When a graphic display is created with the Graphics Viewer, it may have a file name that is not exactly what should be displayed in the navigation pane of the client applications.

Using the Configure Graphic Displays page, you can assign a tag name and description, which are more meaningful. You can also use the Configure Graphic Displays page to change the facility membership.

Graphic displays, like other items, can be assigned to more than one facility. A facility is assigned when the graphic display is created and uploaded to the Facility Commander server. Later, it may be necessary to change the facility assignment by assigning additional facilities or assigning the display to a new facility.

► **To edit the graphic displays records, follow these steps:**

1. Select **System Administration**.
2. Select **Graphic Displays**. The Graphic Displays list page as shown in [Figure 204](#) displays.

Graphic Displays

[00051] Operation cancelled by the operator.

Instructions
















View or edit graphic displays.

Search:

◀ Page 1 of 2 ▶

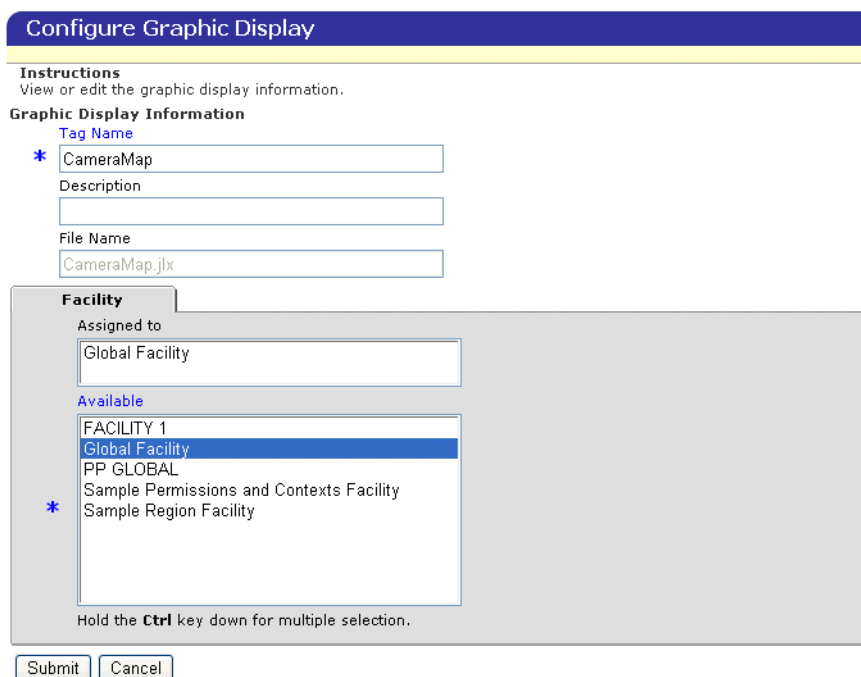
Go to

Items per Page 15 ▼

	Tag Name	Description	Location
	1st floor plan 10_07		1st floor plan 10_07.jlx
	1st floor plan		1st floor plan.jlx
	1st floor plan with intercom system		1st floor plan with intercom system.jlx
	acme campus		acme campus.jlx
	boca site plan		boca site plan.jlx
	card shop 2003		card shop 2003.jlx
	fla site_boca		fla site_boca.jlx
	fla sites		fla sites.jlx
	fla sites_old		fla sites_old.jlx
	floor 1		floor 1.jlx
	floor plan 10 08		floor plan 10 08.jlx
	main building w_computer room		main building w_computer room.jlx
	NY Floor 01		NY Floor 01.jlx
	NY Floor 02		NY Floor 02.jlx
	test		test.jlx

**Figure 204.** Graphic Displays page

3. Select the tag name to create or edit the tag name and description, or change the facilities where this graphic is assigned. The Configure Graphic Display page as shown in [Figure 205 on page 331](#) displays.



**Configure Graphic Display**

**Instructions**  
View or edit the graphic display information.

**Graphic Display Information**

**Tag Name** \*

CameraMap

**Description**

**File Name**

CameraMap.jlx

**Facility**

**Assigned to**

Global Facility

**Available**

FACILITY 1  
Global Facility  
PP GLOBAL  
Sample Permissions and Contexts Facility  
Sample Region Facility

Hold the **Ctrl** key down for multiple selection.

**Submit** **Cancel**

**Figure 205.** Configure Graphic Display page

4. Enter the information described in [Table 132](#). A check mark indicates a required field.
5. Click **Submit** to save the record.

**Table 132.** Configure Graphic Display fields and descriptions

Field Name	REQ	Description
<b>Tag Name</b>	✓	Displays the file name assigned to the graphic display. Enter a unique name to identify this item in the navigation pane of the client applications. This changes the file name on the Facility Commander server. Use 2-36 characters.
<b>Description</b>		Enter a description for this item. Use 1-100 characters. The description does not have to be unique.
<b>File Name</b>		Displays the file name with the J LX extension.

**Table 132.** Configure Graphic Display fields and descriptions

Field Name	REQ	Description
<b>Facility</b>		
<b>Assigned To</b>		Displays the name of facility where this graphic display is currently assigned. This is a read-only field.
<b>Available</b>	✓	<p>Use to assign or change the facility membership for this graphic display. The facilities that display in this list depend on the operator's context and permissions.</p> <p><b>Note:</b> When assigning this item to a facility listed in the Available list, press the <b>Ctrl</b> key before selecting the new facility assignment.</p> <ul style="list-style-type: none"><li>• To assign the graphic display to more than one facility, select the first facility and press the <b>Ctrl</b> key while selecting the other facilities. The selected facilities are highlighted. Click <b>Submit</b>.</li><li>• To assign the graphic display to all the listed facilities, select the first facility in the list, press the <b>Shift</b> key and select the last facility in the list. All the facilities are highlighted. Click <b>Submit</b>.</li></ul>

## Chapter 16. Viewing Graphic Displays

This chapter describes the how to use the Graphics Viewer to issue commands, such as locking and unlocking doors, enabling and disabling devices, and more. Readers should be familiar with using layers in the Graphic Editor client application.



---

### **In this chapter:**

[Overview on page 334](#)

[Navigating the Graphics Viewer on page 336](#)

[Issuing Commands on page 340](#)

[Customizing Window Name and Contents on page 347](#)

[Printing Graphic Displays on page 348](#)

## Overview

The Graphics Viewer is a client application that allows an operator to view graphic displays and issue commands. The Graphics Viewer can be launched from the Alarm Monitor, Event Monitor, or the Facility Commander Launcher window.

When an alarm event is generated, the symbol placed on the graphic display changes to reflect the alarm state. For example, a Door Forced alarm includes two conditions — set and reset. Each alarm state and condition is represented on the graphic display by a different symbol, such as the:

- initial state is represented by a gray door icon
- alarm condition is represented by a red door icon
- reset condition is represented by a green door icon

The graphic displays contain symbols, which represent:

- |                            |                        |
|----------------------------|------------------------|
| • Cameras                  | • Intercom Substations |
| • Door Access Points       | • Intrusion Areas      |
| • Digital Inputs           | • Intrusion DGPs       |
| • Logical Inputs           | • Intrusion Inputs     |
| • Digital Outputs          | • Intrusion Outputs    |
| • Intercom Exchanges       | • Intrusion Keypad     |
| • Intercom Master Stations | • Intrusion Panel      |

In addition, a globe icon displays on the Alarm Monitor and Event Monitor to represent a graphic display when an alarm event occurs. When you select the globe icon, the Graphics Viewer launches with the default graphic display, if configured to do so.

## Alarm States

An alarm can be in one of three states: Alarm, Tamper, and Reset. If different icons were defined for each of these states (using the Symbol Editor), then the appearance of the symbol reflects its current state. If you have multiple maps and link them in a hierarchical arrangement, the associated icons on each level displays the icon in its alarm state condition.

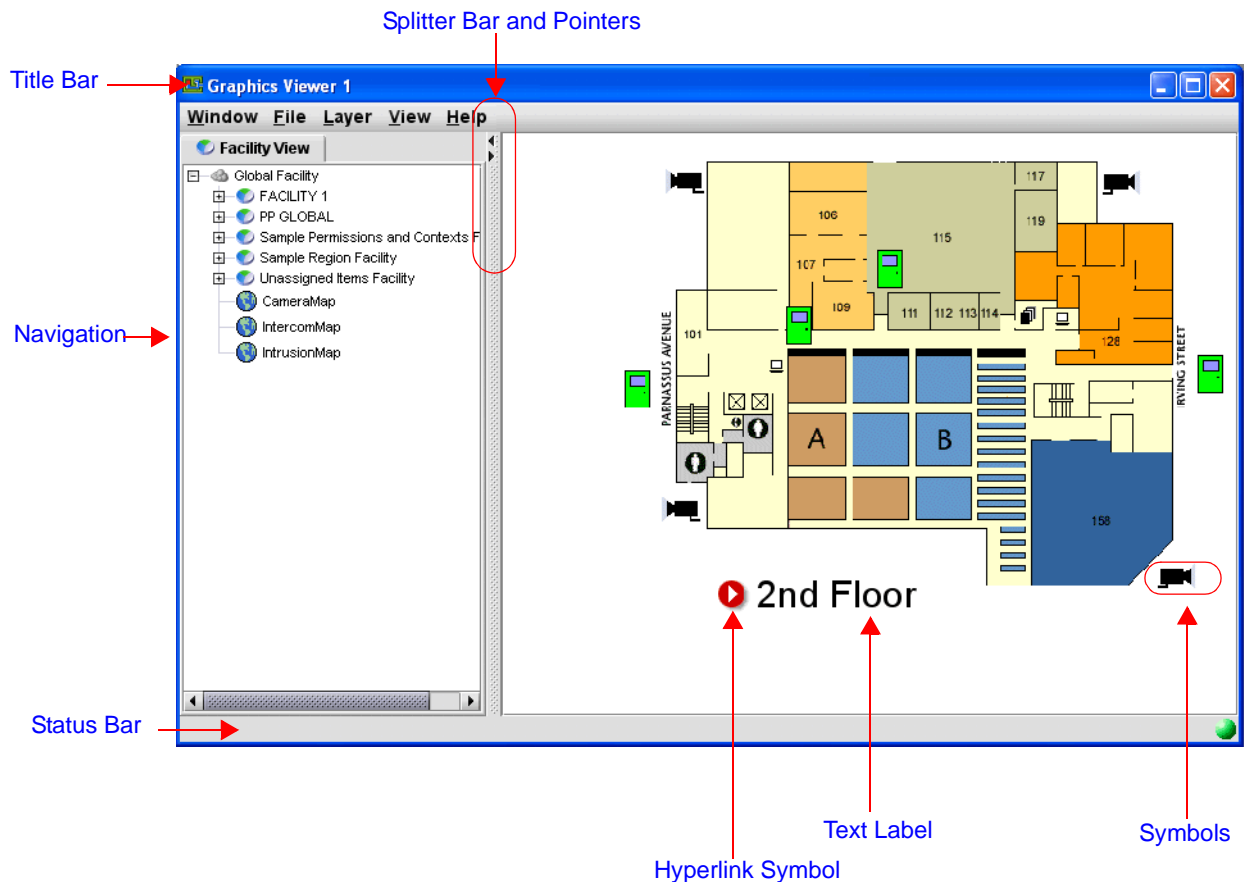
Also, a device such as an access point can have multiple alarms at the same time. When this happens, there are rules for determining the current appearance of the symbol.

- The icon representing the highest priority alarm displays.  
For example, if an access point has a Door Forced Alarm with priority 10 and a Lost Badge Alarm with priority 50, the symbol's appearance will reflect the Door Forced state attribute and condition.
- If all alarms for the device have the same priority, then the symbol's appearance will reflect the most recent alarm occurrence.  
For example, a Lost Badge and Suspended Badge Alarm both have a priority of 50. The Lost Badge alarm occurred at 10:15 and the Suspended Badge alarm occurred at 10:18. The symbol's appearance will reflect the Suspended Badge state attribute and condition.

## Navigating the Graphics Viewer

➤ To display the Graphics Viewer, follow these steps:

1. Open the **Facility Commander Launcher** window.
2. Select **Launch** and **Graphics Viewer**, or select the Graphics Viewer icon from the Viewers toolbar. The Graphics Viewer shown in [Figure 205](#) displays.



**Figure 205.** Graphics Viewer window

[Table 133](#) lists and describes the elements of the Graphics Viewer.

**Table 133.** Graphics Viewer window

Element	Description
Title Bar	<ul style="list-style-type: none"> <li>Displays Graphics Viewer and the window instance number. Refer to <a href="#">Managing Multiple Windows on page 20</a> for more information.</li> <li>Displays the file name and custom window title. Refer to <a href="#">Customizing Window Name and Contents on page 347</a> for more information.</li> </ul>



Table 133. Graphics Viewer window (Continued)

Element	Description
<b>Navigation Pane</b>	<p>Graphic displays are represented by a globe icon and are sorted in alphabetical order. Click the globe icon to change the display.</p> <p>The items that display in the navigation pane are determined by an operator's permission levels and context.</p>
<b>Splitter Bar and Pointers</b>	<p>The Graphics Viewer is divided by a split bar with split pointers, which can be used to change the size of the window.</p> <p>Panes can be resized by moving the location of the splitter bar displayed between the panes or using the split pointers.</p> <p>Click the split pointer to move the window left or right of its current position.</p>
<b>Symbols</b>	<p>Symbols represent devices, such as:</p> <ul style="list-style-type: none"> <li>• Cameras</li> <li>• Door Access Points</li> <li>• Digital Inputs</li> <li>• Logical Inputs</li> <li>• Digital Outputs</li> <li>• Intercom Devices</li> <li>• Intrusion Devices</li> </ul> <p>Refer to <a href="#">Issuing Commands on page 340</a> for more information.</p>
<b>Hyperlink Symbol</b>	<p>Displays the default hyperlink symbol. The hyperlink symbol can be customized and may display as a blinking icon. Click the symbol to view the associated map.</p>
<b>Text Label</b>	<p>Displays a text label, which may identify the building name, a link to another site map, or identify a symbol icon on the site map.</p>
<b>Status Bar</b>	<ul style="list-style-type: none"> <li>• Displays a window filter icon indicating the list of available Facility Commander facilities has changed. When the facilities have been reset, the icon no longer displays on the status bar. Refer to <a href="#">Customizing Window Name and Contents on page 347</a>.</li> <li>• Displays an icon indicating if the system with the Graphics Viewer is connected to the Facility Commander server. <ul style="list-style-type: none"> <li>- Green indicates the Graphics Viewer is communicating with the server.</li> <li>- Red indicates the system is no longer communicating with the server.</li> </ul> </li> </ul>

## Opening Graphic Displays

There are two methods to open a file — tag name or menu option. The navigation pane displays the tag name. Select the tag name in the navigation pane to open the graphics display.

► **To open the Graphics Viewer using the menu, follow these steps:**

1. From the **Facility Commander Launcher** window, select **Launch** and **Graphics Viewer** or select the Graphics Viewer icon from the Viewers toolbar. The Graphics Viewer shown in [Figure 205 on page 336](#) displays.
2. Select **File**, and then **Open**.
  - If a more recent copy of the site map exists on the Facility Commander server, the **Open** window shown in [Figure 206](#) displays.



**Figure 206.** Download window

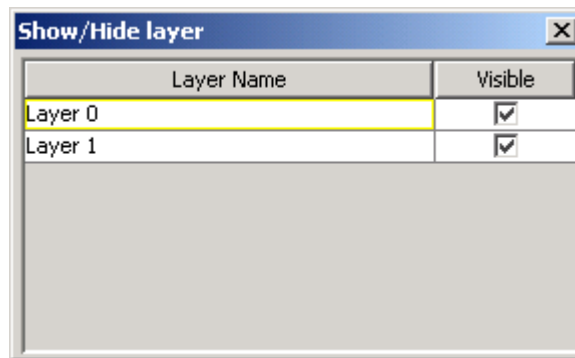
3. Use the drop-down list to select the graphic display you want to view. Click **OK**. The Graphics Viewer displays the selected site map.

## Selecting Layers

Graphic displays can be constructed of different layers with different items on each layer. Use this option to select the layers you want to view. One layer may contain only access points, while another layer may contain all the video devices. Hiding layers reduces the clutter when operators need to focus.

► **To display a different layer, follow these steps:**

1. Select **Layer** and **Show/Hide Layer**. The **Show/Hide Layer** window shown in [Figure 207](#) displays.



**Figure 207.** Show/Hide Layer window

2. The window displays the layer names (Layer 0, Layer 1, or the name assigned to the layer) with a check box to select individual layers. A check mark indicates the layer is visible.
  - Select the check box to display a layer. The **Show/Hide Layer** window remains open to allow you to move back and forth between layers.
  - Clear the check box to remove a layer from view. If you want to view only Layer 1, clear the Layer 0 check box.
3. Click **X** to exit from the **Show/Hide Layer** window.

## Issuing Commands

The Graphics Viewer allows operators to respond to alarm events and issue commands. Different menus with different actions display depending on the type of device and alarm state, such as:

- [Lock and Unlock Doors](#)
- [View Video from a Specific Camera on page 342](#)
- [View Video from Monitor Devices](#)
- [Enable or Disable Input Devices on page 344](#)
- [Connect and Disconnect Intercom Devices on page 345](#)
- [Arm or Disarm Intrusion Areas on page 346](#)

An action may be dimmed if the operation is not allowed. An action may not be allowed if the operator does not have permission to perform the action or the action is not supported by the product. [Table 134](#) lists the devices and the available actions for each device.

**Table 134.** Summary of devices and actions

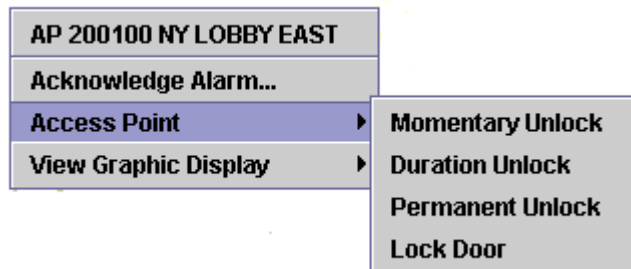
Device	Commands
<b>Access Points</b>	<ul style="list-style-type: none"> <li>• Momentary Unlock</li> <li>• Duration Unlock</li> <li>• Permanent Unlock</li> <li>• Lock Door</li> </ul>
<b>Cameras</b>	<ul style="list-style-type: none"> <li>• View Video Live</li> <li>• Display in CCTV Monitor</li> </ul>
<b>Input Devices</b>	<ul style="list-style-type: none"> <li>• Enable</li> <li>• Disable</li> </ul>
<b>Intercom Devices</b>	<ul style="list-style-type: none"> <li>• Connect</li> <li>• Disconnect</li> </ul>
<b>Intrusion Area</b>	<ul style="list-style-type: none"> <li>• Arm Area</li> <li>• Disarm Area</li> </ul>
<b>Intrusion DGP</b>	<ul style="list-style-type: none"> <li>• Bypass DGP</li> <li>• Unbypass DGP</li> <li>• Start DGP Battery Test</li> <li>• Cancel DGP Battery Test</li> </ul>
<b>Intrusion Input</b>	<ul style="list-style-type: none"> <li>• Bypass Input</li> <li>• Unbypass Input</li> <li>• Acknowledge Alarm</li> </ul>
<b>Intrusion Panel</b>	<ul style="list-style-type: none"> <li>• Set Panel Online</li> <li>• Set Panel Offline</li> </ul>
<b>Intrusion Keypad</b>	<ul style="list-style-type: none"> <li>• Bypass Keypad</li> <li>• Unbypass Keypad</li> </ul>

Refer to the appropriate sections for more information about using these features.

## Lock and Unlock Doors

➤ **To lock or unlock an access door, follow these steps:**

1. Select the appropriate graphic display. Refer to [Opening Graphic Displays on page 338](#).



**Figure 208.** Site map with action menu

2. Locate the symbol representing the device. If the device is in an alarm state:
  - Double-click the symbol to launch the Alarm Response window as shown in [Responding to Alarms on page 215](#).
  - Right-click the symbol to display the action menu. The window shown in [Figure 208](#) displays with the tag name and a list of actions available to the operator.

If the device is not in an alarm state:

- Double-click the symbol to perform the default action, which is Momentary Unlock.
- Right-click the symbol to display the action menu. The Control Toolbar displays when the device is not in an alarm state.

Refer to [Table 135](#) for a description of each action.

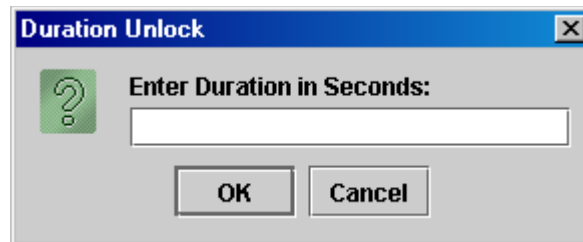
**Table 135.** Lock/Unlock options

Option	Description
<b>Momentary Unlock</b>	Unlocks the door for a time specified in the access control system.
<b>Permanent Unlock</b>	Unlocks the door permanently until changed by an operator.
<b>Duration Unlock</b>	Unlocks the door the number of seconds specified in the drop-down list. Refer to <a href="#">Unlock Door for Duration</a> for more information.
<b>Lock Door</b>	Locks the door until reset by an operator using the unlock command.

## Unlock Door for Duration

➤ **To unlock a door for a specified duration, follow these steps:**

3. Select **Duration Unlock**. The window shown in [Figure 209](#) displays.



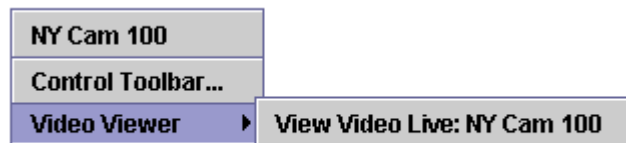
**Figure 209.** Lock and unlock door options

4. Enter the number of seconds in the **Enter Duration in Seconds** field.
5. Click **OK**.

## View Video from a Specific Camera

➤ **To view video from a camera device, follow these steps:**

1. Select the graphic display. Refer to [Opening Graphic Displays on page 338](#).



**Figure 210.** Graphic display with video devices

2. Locate the symbol representing the camera. If the camera is in an alarm state:
  - Double-click the symbol to launch the Alarm Response window as shown in [Responding to Alarms on page 215](#) displays.
  - Right-click the symbol to display the action menu. The window shown in [Figure 210](#) displays with the tag name and a list of actions available to the operator.

If the camera is not in an alarm state:

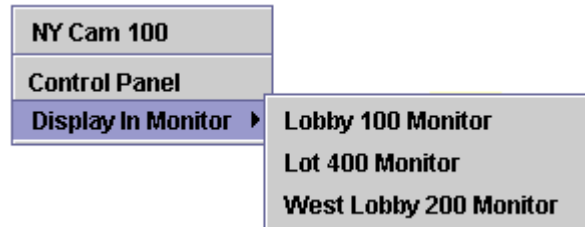
- Double-click the symbol to perform the default action, which is View Live Video. Or, drag the camera from the navigation pane to a Video Console pane and live video displays.
- Right-click the symbol to display the action menu. The Control Toolbar displays when the device is not in an alarm state.

## View Video from Monitor Devices

To use this feature, analog cameras must be connected to an analog CCTV switcher. Refer to [Configuring Video Devices on page 121](#) for more information.

► **To display video on a CCTV monitor, follow these steps:**

1. Select the graphic display. Refer to [Opening Graphic Displays on page 338](#).



**Figure 211.** Graphical display with monitors

2. Locate the symbol representing the camera. If the camera is in an alarm state:
    - Double-click the symbol to launch the Alarm Response window as shown in [Responding to Alarms on page 215](#) displays.
    - Right-click the symbol to display the action menu. The window shown in [Figure 211](#) displays with the tag name and a list of actions available to the operator.
- If the camera is not in an alarm state:
- Right-click the symbol to display the action menu. Select **Display in Monitor** and then select the monitor device to play the video. The Control Panel displays when the device is not in an alarm state.

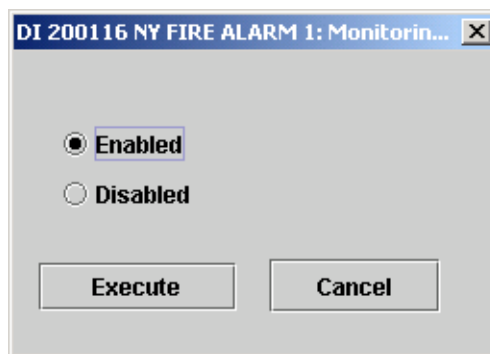
## Enable or Disable Input Devices

► To enable or disable input devices, follow these steps:

1. Select the graphic display. Refer to [Opening Graphic Displays on page 338](#).
2. Locate the symbol representing the device. If the device is in an alarm state:
  - Double-click the symbol to launch the Alarm Response window as shown in [Responding to Alarms on page 215](#) displays.
  - Right-click the symbol to display the action menu. The window shown in [Figure 212](#) displays with the tag name and a list of actions available to the operator.

If the device is not in an alarm state:

- Right-click the symbol to display the action menu. The Control Toolbar displays when the device is not in an alarm state.



**Figure 212.** Monitor window

3. Select the appropriate option button and click **Execute** to perform the selected action. The actions are described in [Table 136](#).

**Table 136.** Monitor window

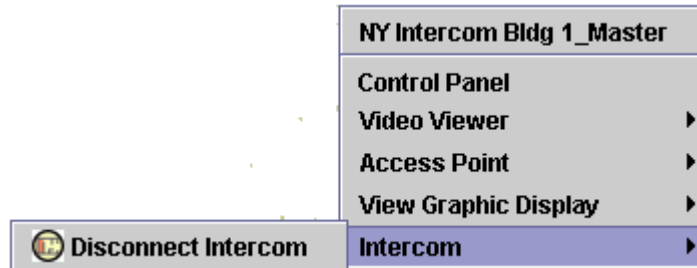
Option	Description
<b>Title Bar</b>	Displays DI-prefix to identify digital input and the tag name.
<b>Enabled</b>	Select to enable the device.
<b>Disabled</b>	Select to disable the device.



## Connect and Disconnect Intercom Devices

► **To connect an intercom device, follow these steps:**

1. Select the appropriate graphic display. Refer to [Opening Graphic Displays on page 338](#).



**Figure 213.** Graphic display with an intercom device

2. Locate the symbol representing the intercom device. If the device is in an alarm state:
  - Double-click the symbol to launch the Alarm Response window as shown in [Responding to Alarms on page 215](#) displays.
  - Right-click the symbol to display the action menu. The window shown in [Figure 213](#) displays with the tag name and a list of actions available to the operator.

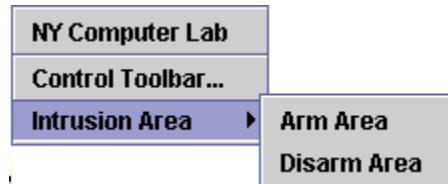
If the device is not in an alarm state:

- Double-click the symbol to perform the default action, which is Connect.
- Right-click the symbol to display the action menu. The Control Toolbar displays when the device is not in an alarm state.

## Arm or Disarm Intrusion Areas

► To arm or disarm an intrusion area, follow these steps:

1. Select the appropriate graphic display. Refer to [Opening Graphic Displays on page 338](#).



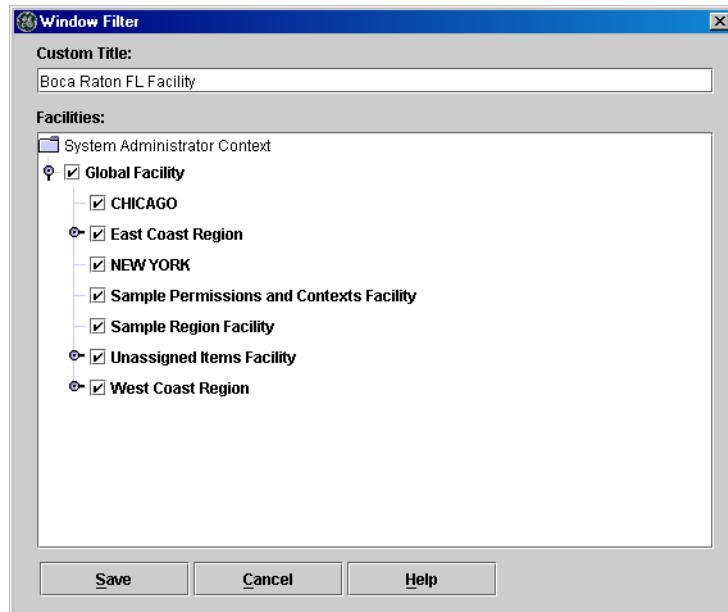
**Figure 214.** Graphic display with an intercom device

2. Locate the intrusion area. If the area is in an alarm state:
  - Right-click the symbol to display the action menu. The window shown in [Figure 213](#) displays with the tag name and a list of actions available to the operator.If the device is not in an alarm state:
  - Double-click the symbol to perform the default action, which is Arm.
  - Right-click the symbol to display the action menu. The Control Toolbar displays when the device is not in an alarm state.

## Customizing Window Name and Contents

➤ To filter the items, follow these steps:

1. From the **View** menu, select **Window Filter**. The Window Filter window in [Figure 215](#) displays.



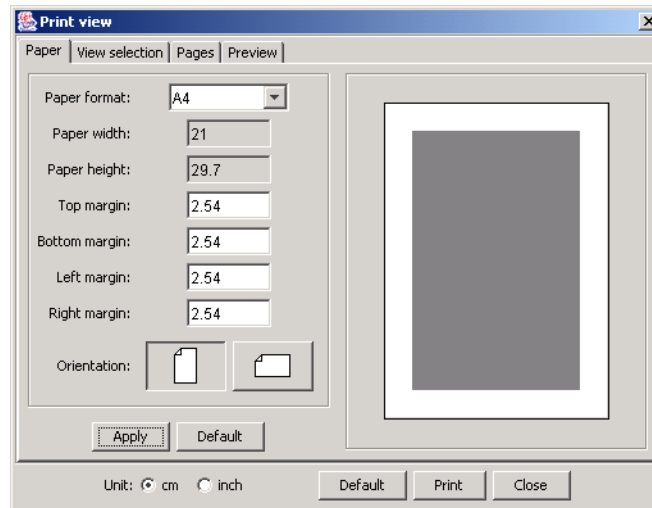
**Figure 215.** Window Filter

2. Use the **Custom Title** field to identify a title to display on the Graphics Viewer title bar. You can use up to 255 characters.
3. Select the check boxes to indicate the items you want to display on the Graphics Viewer. A check mark indicates the item is selected.
  - Clear the check boxes to remove the items from view.
4. Click **Save**. The Graphics Viewer displays a window filter icon in the status bar indicating the list of available Facility Commander facilities has changed.

## Printing Graphic Displays

➤ **To print a display, follow these steps:**

1. From the **File** menu, select **Print**. The Print View window shown in [Figure 216](#) displays.



**Figure 216.** Print View window

2. On the **Paper** tab, use the **Paper Format** drop-down list to select the correct paper size. The measurements and margins display for the selected paper format. The default setting is A4.
  - Select the unit of measurement to display. Click the appropriate option button to select centimeters or inches.
  - Select the paper orientation. Click the portrait icon or landscape icon to change the orientation.
  - If you select a custom paper format, enter the paper width and height, and margins for the graphic display. Click **Default** to discard the changes and return to the default settings.
3. On the **View Selection** tab, you can adjust the position of the graphic display on the page. Use the **Start X** and **Start Y** to change the position of the display. Click **Apply** when you are finished making adjustments.
4. On the **Pages** tab, you can adjust the position size, resolution, and indicate the number of pages to print the site map or graphic display.
5. On the **Preview** tab, you can preview the page before printing. Make the necessary changes and click **Print**.

# Chapter 17. Backup/Restore Informix Databases

This chapter describes the backup and restore procedures for Linux and AIX files; and Informix databases.



---

**In this chapter:**

[Overview on page 350](#)

[Requirements \(Tape Backups\) on page 351](#)

[Backing Up Database Records on page 352](#)

[Restore Procedures on page 357](#)

## Overview

Backups let you copy data to a disc or tape device. When you back up data to a tape, you must have a tape device connected to the computer. If a tape device is not available, you can back up the data to a disc and transfer the file to a safe place for storage.

It is a good practice to back up the data stored on the Facility Commander server at regular intervals. If the original data stored on the server's hard disk becomes inaccessible because of a system malfunction, you can use the backup data to restore the lost or damaged data.

This chapter describes how to back up selected files and folders; and restore the backed up files to the original hard disk or a new hard disk.

## Backup Modes

Facility Commander provides a backup utility for backing up files and database records to a tape device, which is the default setting. If you want to back up the files to disk, you will need to edit two configuration files to change the output destination to disk.

To edit the configuration files, refer to [Appendix A on page 401](#), which includes:

- [Editing the Informix Configuration File on page 403](#)
- [Scheduling the Backup Utility on page 404](#)

Use [Table 137](#) to select the appropriate mode and device to back up the Facility Commander database records.

- Back up the Informix database to a tape device or disk. To do this, you must edit the backup utility and Informix configuration files to redirect the output to disk.

*Once you edit the configuration file to change the output to disk, instead of tape, the backup utility will not be able write to tape because of the changes in the configuration file.*

**Table 137.** Databases and Backup Modes

Database	Mode	Backup Device
Informix	Interactive	Tape or disk
Informix	Scheduled (Cron)	Disk only

## Backup Types

There are two types of backups — full and incremental. A full backup includes the entire database contents. If you choose to backup to disk, a full backup is done.

Incremental backups, sometimes called differential backups, only record those portions of the system that have been modified since the last full backup.

It is recommended that you perform a full backup at regular intervals.

**AIX Only:** Change the **TAPEDEV** parameter to the actual tape device name. AIX does not accept symbolic links to a tape device. The tape device name in the new value may be different.

Parameter: **TAPEDEV**

Default value: `/dev/tape`

New value: `/dev/rmt0`

## Requirements (Tape Backups)

A minimum of two tapes is required to create a system backup. One tape is used to record the database backup, while the other is used to record the required support files for Informix and Facility Commander. Depending on the amount of data to be backed up, additional tapes are “spanned” to contain the information.

## Tape Labels

Backup tapes must be identified clearly. Record the following information:

- Type (Full or Incremental)
- Date
- Tape number and the number in the series, such as: 1 of 2 and 2 of 2.

During file backups, the log file name is displayed and contains both the backup type and date. Refer to [Figure 222 on page 356](#) for an example. In addition, include the referenced full backup log file.

For the database backups, each database may have information that is unique to the vendor and should also be recorded on the tape label.

The Informix backup program prints out the IDs of logical logs that are recorded to the tape backup. Record these IDs on the tape label as well. This information is useful during the process that includes restoring the archived logical logs.

## Backing Up Database Records

These instructions describe how to complete a full backup of the files and database records. There are small differences if you are doing an incremental backup, and those differences are noted.

The database and files are backed up using **BackupUtility**, which is a command line script. The script first backs up the database, verifies the backup, and then begins to back up the files.

► **To begin the back up process, follow these steps:**

1. Open a terminal window. If you are not logged into the system as “root”, you will be prompted for the root password. This is required to ensure access to all resources.
2. Start the backup utility and the window in [Figure 217](#) displays.
  - For Linux/Informix: Double-click the **Backup Utility** icon.
  - For AIX, type: `cd /usr/BackupUtility [Enter]`  
`sh BackupUtility [Enter]`



**Figure 217.** Backup Utility

3. Type the appropriate letter to select the backup type, such as:
  - **F** to complete a full backup
  - **I** to complete an incremental backup.This menu is also used to restore a backup or to exit this program.



## Informix Database

The Informix database is backed up using the **ontape** utility application. When the backup procedure is started, the window in [Figure 218](#) displays.



**Figure 218.** Starting a full-level database backup

➤ **To begin the tape backup process, follow these steps:**

1. Insert the tape in the tape drive, wait for computer system to recognize the tape, and press **Enter**. The window in [Figure 219](#) displays.

A message displays stating the type of backup. “Level 0” indicates a full backup, while “Level 1” indicates an incremental backup.

Record the IDs of the logical logs to the backup on the tape label. →

```

root@mlnserver:~ - Shell - Konsole
Commencing Level 0 backup of the database.

Please mount tape 1 on /dev/tape and press Return to continue ...
100 percent done.

Please label this tape as number 1 in the arc tape sequence.
This tape contains the following logical logs:
5
Program over.
Ejecting media...

```

Figure 219. Database backup complete

2. A message displays with the process of the backup. When the backup is complete, a message displays reporting which logical logs were recorded to the tape during the backup process. Record the identification of the logical logs written to the backup on the tape label.

Backup verification process →

```

root@mlnserver:~ - Shell - Konsole
100 percent done.

Please label this tape as number 1 in the arc tape sequence.
This tape contains the following logical logs:
5
Program over.
Ejecting media...done
Commencing backup verification.
Informix Dynamic Server 2000 Version 9.21.UC4
Program Name: archecker
Version: 4.7
Released: 11/30/00 09:32
Compiled: 11/30/00 09:34 on Linux 2.2.12-20smp #1 SMP Mon Sep 27 10:34:45
EDT 1999
AC_STORAGE /tmp
AC_MSGPATH /tmp/ac_msg.log
AC_VERBOSE on
AC_TAPEDEV /dev/tape
AC_TAPEBLOCK 16
Please put in tape number 1.
Type 1 <return> or 0 to end:

```

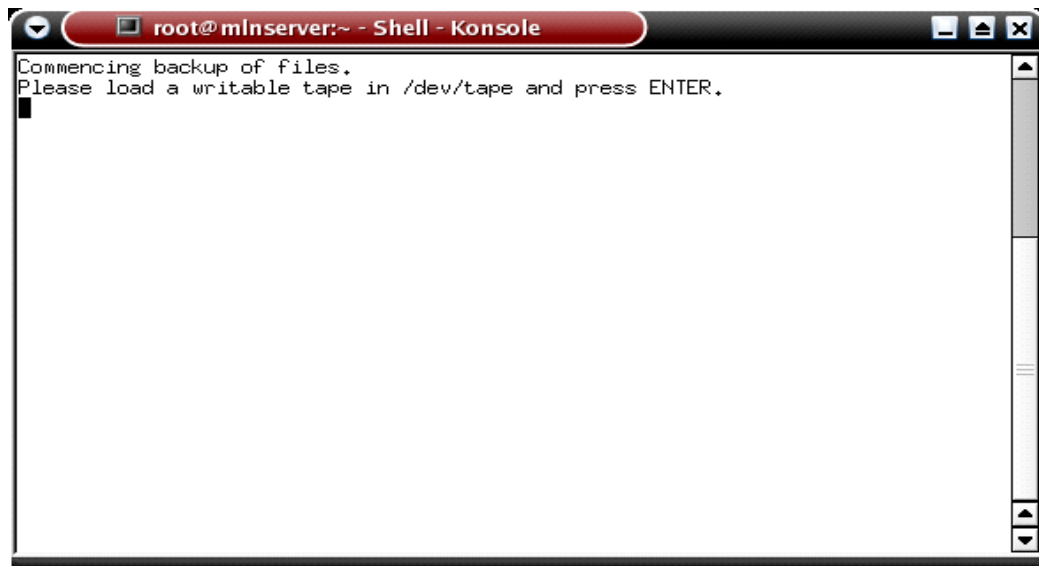
Figure 220. Backup verification

3. Insert tape number one when the verification is complete and type: **1** to continue. Press **Enter**.

As each tape is verified, a prompt displays to insert the next tape in the series. When the last tape in the series has been verified, or if you do not want to continue, type: **0**. Press **Enter**.

## Backing Up Files

After the database backup verification is complete, the process of backing up files begins. The window in [Figure 221](#) displays.



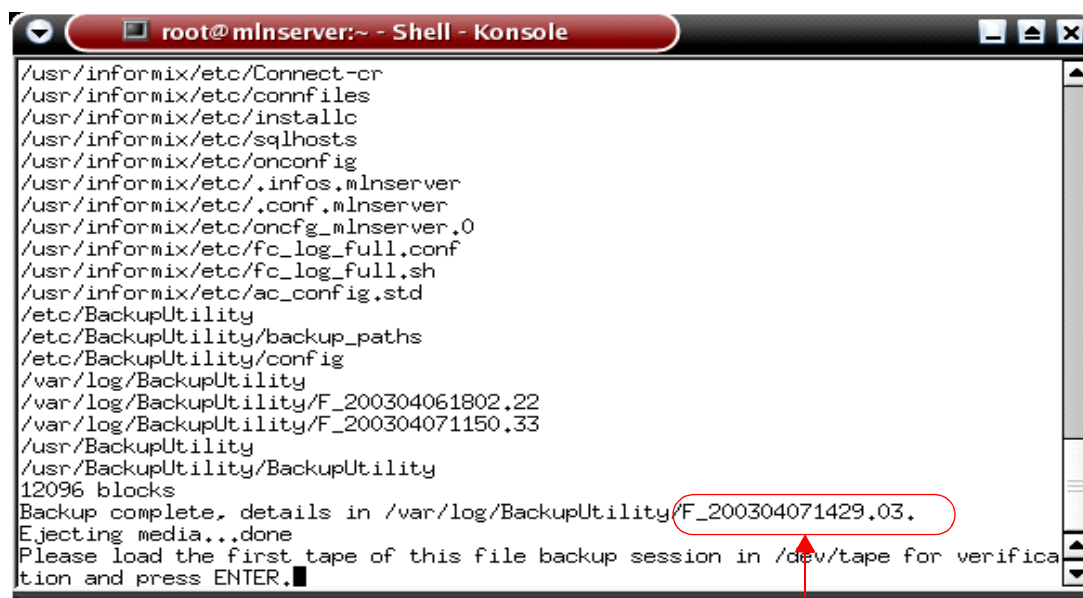
**Figure 221.** Start backup of files

► **To begin the back up process, follow these steps:**

1. Insert the tape in the tape drive, wait for computer system to recognize the tape, and press **Enter**. The window in [Figure 222](#) displays. The list of files being backed up scrolls as the files are written to the tape.

**Note:** On AIX systems, the backup process begins immediately when **Enter** is pressed. Failure to insert a tape, use a read-only tape, or pressing the **Enter** key too early will result in a program error.

2. If the number or size of the files is sufficiently large, the tape will become full and you will be prompted to replace the tape. This prompt is repeated each time a tape is filled to capacity. In many cases, one tape is sufficient and you will not see this message.

A terminal window titled 'root@mlnserver:~ - Shell - Konsole' displays the output of a backup process. The output lists various system files, followed by backup details: '12096 blocks', 'Backup complete, details in /var/log/BackupUtility/F\_200304071429.03.', 'Ejecting media...done', and a prompt to load the first tape for verification. A red circle highlights the log file path, with a red arrow pointing to it from the label 'Log file name' below the window.

```
root@mlnserver:~ - Shell - Konsole
/usr/informix/etc/Connect-cr
/usr/informix/etc/connfiles
/usr/informix/etc/installc
/usr/informix/etc/sqlhosts
/usr/informix/etc/onconfig
/usr/informix/etc/.infos.mlnserver
/usr/informix/etc/.conf.mlnserver
/usr/informix/etc/oncfg_mlnserver.0
/usr/informix/etc/fc_log_full.conf
/usr/informix/etc/fc_log_full.sh
/usr/informix/etc/ac_config.std
/etc/BackupUtility
/etc/BackupUtility/backup_paths
/etc/BackupUtility/config
/var/log/BackupUtility
/var/log/BackupUtility/F_200304061802.22
/var/log/BackupUtility/F_200304071150.33
/usr/BackupUtility
/usr/BackupUtility/BackupUtility
12096 blocks
Backup complete, details in /var/log/BackupUtility/F_200304071429.03.
Ejecting media...done
Please load the first tape of this file backup session in /dev/tape for verification and press ENTER.
```

Log file name

**Figure 222.** Waiting to start file backup verification

3. When the backup is complete, a message displays with the details of where the log is stored and the last tape is ejected. Record this information to view the logs at a later date.
4. Insert the first tape in the series to verify the backup and press **Enter**. This verification only tests the readability of the tape and not the contents of the tape. The window in [Figure 223 on page 357](#) displays next.

```

root@mlnserver:~ - Shell - Konsole
/usr/informix/etc/sqlhosts
/usr/informix/etc/onconfig
/usr/informix/etc/.infos.mlnserver
/usr/informix/etc/.conf.mlnserver
/usr/informix/etc/oncfg_mlnserver.0
/usr/informix/etc/fc_log_full.conf
/usr/informix/etc/fc_log_full.sh
/usr/informix/etc/ac_config.std
/etc/BackupUtility
/etc/BackupUtility/backup_paths
/etc/BackupUtility/config
/var/log/BackupUtility
/var/log/BackupUtility/F_200304061802.22
/var/log/BackupUtility/F_200304071150.33
/usr/BackupUtility
/usr/BackupUtility/BackupUtility
12096 blocks
Backup complete, details in /var/log/BackupUtility/F_200304071429.03.
Ejecting media...done
Please load the first tape of this file backup session in /dev/tape for verification and press ENTER.
Verifying backup...12096 blocks
PASSED
Ejecting media...

```

Verification passed message

**Figure 223.** Successful file backup verification

5. Remove the tape and store it according to your organization's policy.
  - If you are using an Imation™ Travan™ tape, it will not be ejected automatically. Remove the tape from the drive to prevent any problems with loading future tapes.

## Restore Procedures

This section describes the restore process as if the Facility Commander server disk drive fails. Previous to restoring the data, the system administrator should:

- Install the operating system
- Install the database
- Install Facility Commander software

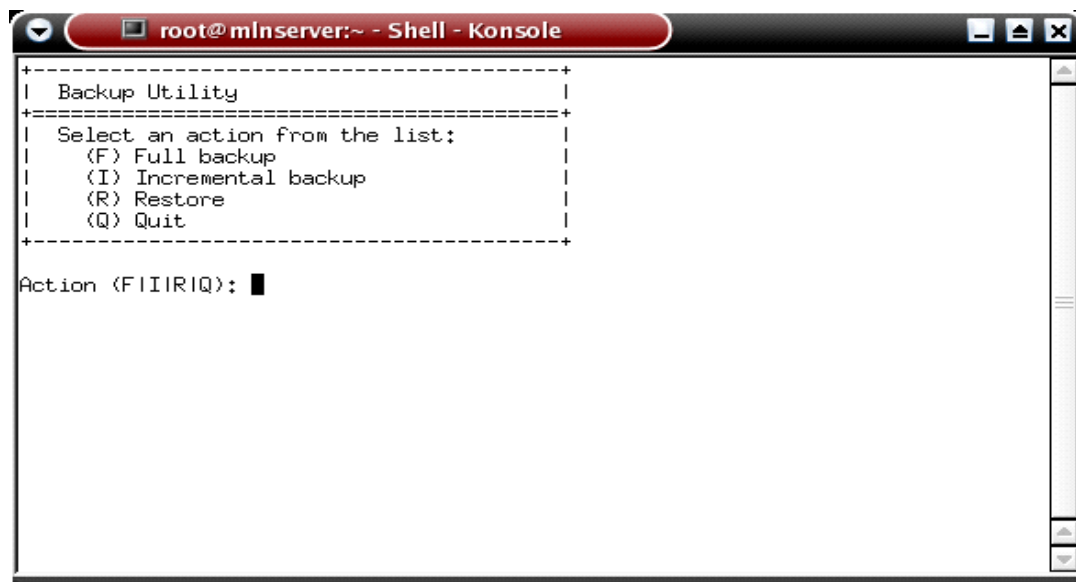
Also, install all patches or upgrades that are appropriate. The machine should have the same configuration as the original hardware when the backups were completed.

When the Restore action is selected, the program preforms a pre-restoration check to verify the system is in an appropriate state. These checks depend on the database.

*The Informix database must be shut down before it is restored. You will be unable to restore the Informix database before shutting it down. An error message displays. Use the command “service Informix stop” to shutdown the database.*

➤ **To begin the restore process, follow these steps:**

1. Insert the tape in the tape drive, wait for computer system to recognize the tape, and press **Enter**.
2. Open a terminal window. If you are not logged into the system as “root”, you will be prompted for the root password. This is required to ensure access to all resources.
3. Start the backup utility and the window in [Figure 224](#) displays.
  - For Linux/Informix: Double-click the **Backup Utility** icon.
  - For AIX, type: `cd /usr/backuputility [Enter]`  
`sh backuputility [Enter]`



**Figure 224.** Backup Utility

4. Type **R** to begin the restore process.

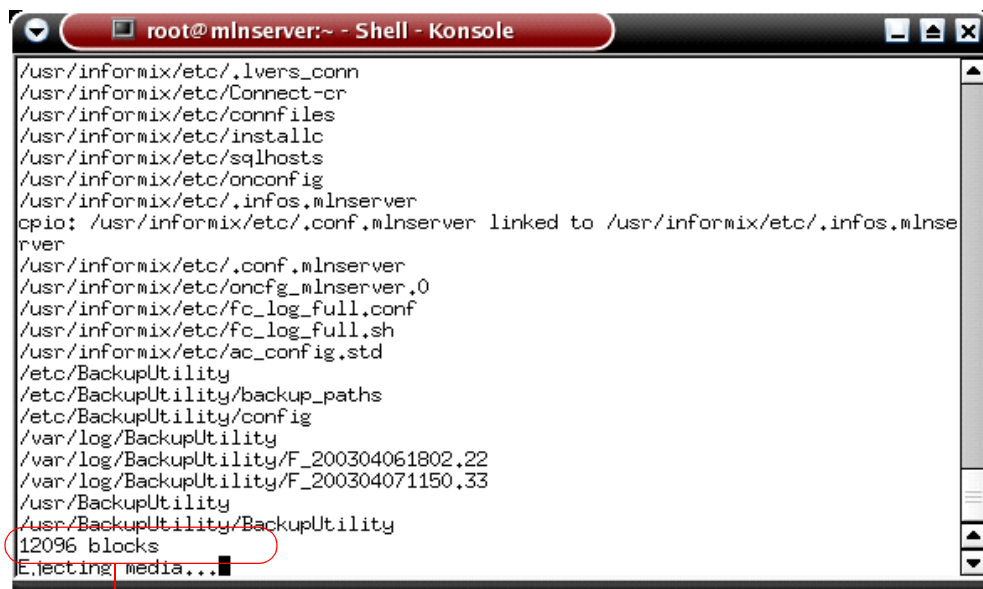


**Figure 225.** Start Restore process with tape in drive

5. Type: **Y** to indicate the tape is loaded and the program begins restoring the files from the tape. If you type **N** indicating the tape is not the first in the series, the program will eject the tape.

Failure to insert a tape, using a read-only tape, or pressing the **Enter** key too early will result in a program error and the process must be started over.

6. If the backup is comprised of multiple tapes, this message displays each time a tape is restored: **Found end of volume. Load next volume and press RETURN.**



```
root@mInserver:~ - Shell - Konsole
/usr/informix/etc/.lvers_conn
/usr/informix/etc/Connect-cr
/usr/informix/etc/connfiles
/usr/informix/etc/installc
/usr/informix/etc/sqlhosts
/usr/informix/etc/onconfig
/usr/informix/etc/.infos.mInserver
cpio: /usr/informix/etc/.conf.mInserver linked to /usr/informix/etc/.infos.mInserver
/usr/informix/etc/.conf.mInserver
/usr/informix/etc/oncfg.mInserver.0
/usr/informix/etc/fc_log_full.conf
/usr/informix/etc/fc_log_full.sh
/usr/informix/etc/ac_config.std
/etc/BackupUtility
/etc/BackupUtility/backup_paths
/etc/BackupUtility/config
/var/log/BackupUtility
/var/log/BackupUtility/F_200304061802.22
/var/log/BackupUtility/F_200304071150.33
/usr/BackupUtility
/usr/BackupUtility/BackupUtility
12096 blocks
Ejecting media...
```

Block count

**Figure 226.** File restoration complete

7. Remove the tape and store it according to your organization's policy.



## Restore Incremental Backups

After the files are restored, the incremental backups should be restored. The window in [Figure 227](#) displays next.



**Figure 227.** Restore incremental backups

- **To begin the restore process, follow these steps:**
  1. Type: **Y** to indicate an incremental backup will be restored. If you type **N** to indicate there are no incremental backups, the program continues to the next step, which is to restore the database.

## Restore Database

When the program begins to restore the Informix database, a long pause occurs. A window displays during this pause.

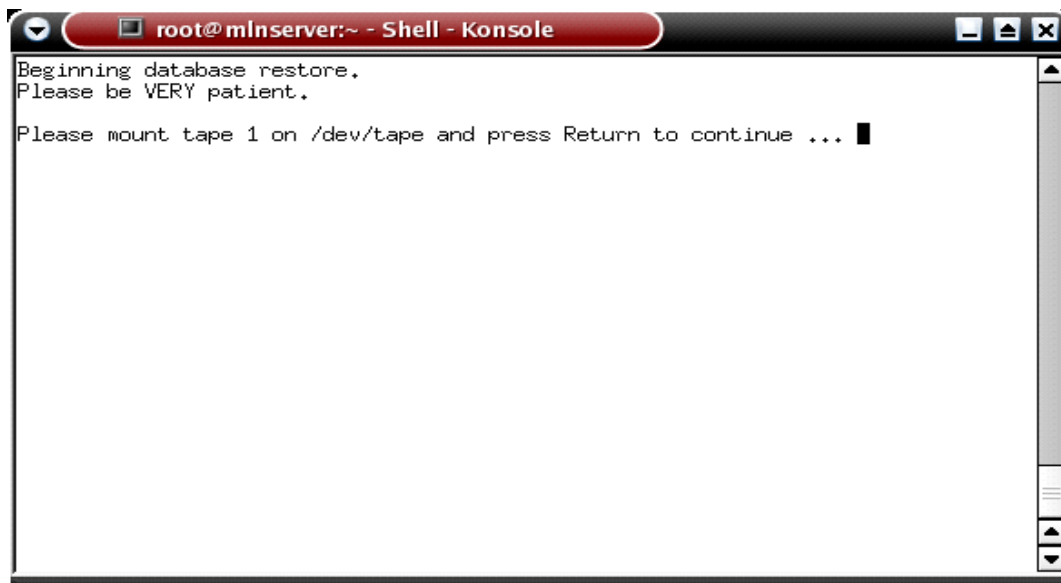


Figure 228. Wait for database tape to be loaded

► **To begin the restore process, follow these steps:**

1. Insert the tape in the tape drive, wait for computer system to recognize the tape, and press **Enter**. The program reads information from the tape and displays the details in the window as shown in [Figure 229](#).

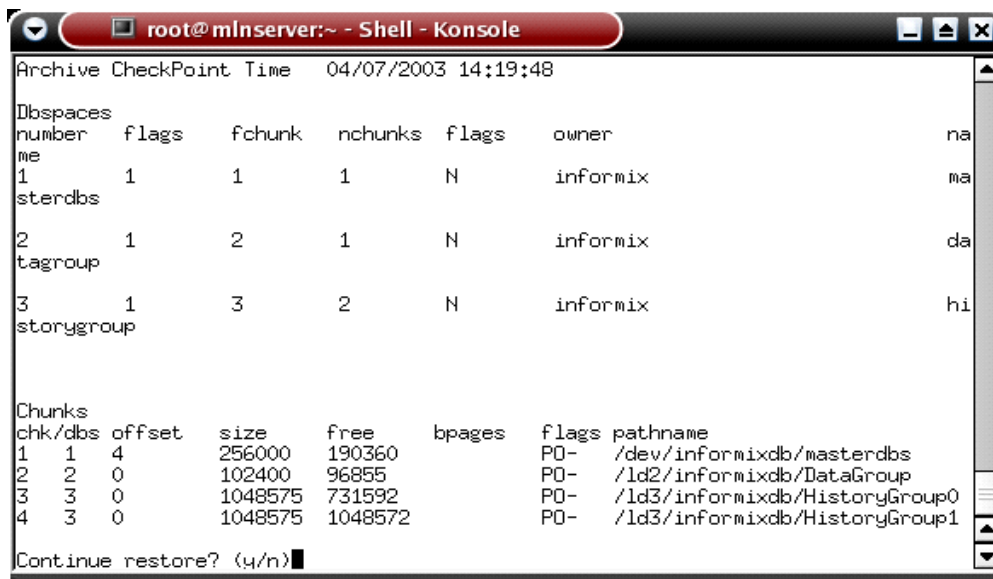


Figure 229. Restore details

2. Type: **Y** when this message displays: **Continue restore?**
3. Type: **Y** when this message displays: **Do you want to back up the logs?**

The logs contain details of the database transactions (database already residing on disk drive). If you have problems with your database, these logs may be used to recover transactions that have occurred since the last backup.

```

number  flags  fchunk  nchunks  flags  owner  na
me
1       1     1      1        N    informix  ma
sterdbs

2       1     2      1        N    informix  da
tagroup

3       1     3      2        N    informix  hi
storygroup

Chunks
chk/dbs offset  size    free    bpages  flags  pathname
1  1  4    256000  190360  1       PO-   /dev/informixdb/masterdbs
2  2  0    102400  96855   1       PO-   /ld2/informixdb/DataGroup
3  3  0    1048575 731592  1       PO-   /ld3/informixdb/HistoryGroup0
4  3  0    1048575 1048572 1       PO-   /ld3/informixdb/HistoryGroup1

Continue restore? (y/n)y
Do you want to back up the logs? (y/n)y
Please mount tape 1 on /var/LogicalLogs/Logs and press Return to continue ...

```

**Figure 230.** Prompt for salvaging logs

4. Insert the tape to store the logical log files. The device name listed is a file stored on the disk drive. Press **Enter** and the window in [Figure 231](#) displays.

```

root@mlnserver:~ - Shell - Konsole
3      1      3      2      N      informix      hi
storygroup

Chunks
chk/dbs offset    size    free    bpages  flags pathname
1  1  4      256000  190360      P0-   /dev/informixdb/masterdbs
2  2  0      102400   96855      P0-   /ld2/informixdb/DataGroup
3  3  0      1048575  731592      P0-   /ld3/informixdb/HistoryGroup0
4  3  0      1048575  1048572     P0-   /ld3/informixdb/HistoryGroup1

Continue restore? (y/n)y
Do you want to back up the logs? (y/n)y

Please mount tape 1 on /var/LogicalLogs/Logs and press Return to continue ...
Would you like to back up log 5? (y/n) y

Please label this tape as number 1 in the log tape sequence.

This tape contains the following logical logs:
    5
Log salvage is complete, continuing restore of archive.

```

Figure 231. Logical logs restored

- After the logical logs are restored, the process of restoring the database begins. The window displays messages to describe the process. When the database is restored, this message displays:

**Restore a level 1 archive?**

If you have incremental backup tapes that you want to restore, type: **Y**. The program repeats the process used to restore the database. The window in [Figure 232](#) displays next.

```

root@mlnserver:~ - Shell - Konsole
14:50:45 Loading Module <BUILTI>NNULL>
14:50:49 Informix Dynamic Server 2000 Version 9.21.UC4      Software Serial Numbe
er AAD#J245782
14:50:50 Informix Dynamic Server 2000 Initialized -- Shared Memory Initialized.

14:50:50 Dataskip is now OFF for all dbspaces
14:50:50 Recovery Mode
14:52:05 Physical Restore of masterdbs, datagroup, historygroup started.

14:52:10 Checkpoint Completed: duration was 0 seconds.
14:52:10 Checkpoint logunq 5, logpos 0x64b2b4

14:52:11 Checkpoint Completed: duration was 0 seconds.
14:52:11 Checkpoint logunq 5, logpos 0x64b2b4

14:52:13 Checkpoint Completed: duration was 0 seconds.
14:52:13 Checkpoint logunq 5, logpos 0x64b2b4

14:52:14 Physical Restore of masterdbs, datagroup, historygroup Completed.
14:52:14 Checkpoint Completed: duration was 0 seconds.
14:52:14 Checkpoint logunq 5, logpos 0x64b2b4

Restore a level 1 archive (y/n) n
Do you want to restore log tapes? (y/n)n

```

Figure 232. Restore log tapes

- Type: **N** to skip this step. Use the logical logs to recover transactions that have occurred since the last regular backup. It is

not recommended to use the logs unless you are familiar with this process, which is not described in this document.

The window in [Figure 233 on page 365](#) displays next.

```

root@mlnserver:~ - Shell - Konsole
Do you want to restore log tapes? (y/n)n
/usr/informix/bin/onmode -sy

Program over.
Ejecting media...done
Waiting for restore to complete.
14:53:33 Physical Recovery Started at Page(1:884).
14:53:33 Physical Recovery Complete: 0 Pages Examined 0 Pages Restored.

14:53:33 Logical Recovery Started.
14:53:33 10 recovery worker threads will be started.
14:53:36 Logical Recovery Complete.
0 Committed, 0 Rolled Back, 0 Open, 0 Bad Locks

14:53:37 Bringing system to Quiescent Mode with no Logical Restore.

Shutting down the database.
14:53:38 Quiescent Mode
14:53:38 Checkpoint Completed: duration was 0 seconds.
14:53:38 Checkpoint loguniq 5, logpos 0x64c018

14:53:39 Informix Dynamic Server 2000 Stopped.

Reboot system to start database? <[Y]/N>: █

```

**Figure 233.** Reboot system to start database

7. The program ends, the tape is ejected from the tape drive, and you are prompted to reboot the system to start the database.



# Chapter 18. Viewing Diagnostics

This chapter describes the different diagnostics used to troubleshoot the system. The system administrator should not change these settings unless instructed to do so by Customer Support.



---

**In this chapter:**

[Overview on page 368](#)  
[Changing Diagnostics Settings on page 369](#)  
[ATS Panel Intrusion on page 371](#)  
[Database Connection Pool on page 372](#)  
[Database Transactions Diagnostics on page 373](#)  
[Database Queries Diagnostics on page 374](#)  
[Facility Membership Cache on page 375](#)  
[JVM Statistics on page 376](#)  
[Media Diagnostics on page 377](#)  
[Service Framework Diagnostics on page 378](#)  
[System Status Diagnostics on page 379](#)  
[Thread Pool Manager Diagnostics on page 380](#)

## Overview

The Diagnostics page shown in [Figure 234 on page 369](#) keeps track of all the software components that generate diagnostic information.

Diagnostics provides statistics on the following components:

- ATS Panel Intrusion Proxy Host ATS Panel
- Database Connection Pool
- Database Queries
- Database Transactions
- Facility Membership Cache
- JVM Statistics
- Media Diagnostics
- Service Framework
- System Status
- Thread Pool Manager

Each server has a server-wide configuration for diagnostics, which can be:























- **Disabled.** The server is not receiving any diagnostic information. Disabled is the default setting.
- **Enabled.** The information is written to the database. When you reset the system, the information is not lost.

The system administrator should not change these settings unless instructed to do so by Customer Support. The performance of the system could be affected if any of these settings are enabled. If you have any questions concerning these settings, please contact Customer Support.



## Changing Diagnostics Settings

Use the **Diagnostics** list page shown in [Figure 234](#) to view the diagnostic settings. This page allows you to edit or view diagnostic settings.

Diagnostics			
Request was successful.			
<b>Instructions</b>			
View Diagnostics			
	Description		Diagnostics Mode
 	System Status		Enabled
 	Database Transactions		Enabled
 	Database Queries		Enabled
 	Database Connection Pool		Enabled
 	Facility Membership Cache		Enabled
 	Thread Pool Manager		Enabled
 	Service Framework		Enabled
 	ATS Panel Intrusion Proxy Host ATS Panel		Enabled
 	Media Diagnostics		Enabled
 	JVM Statistics		Enabled
 	Picture Perfect Proxy Host bctpicture1		Enabled

Edit  
Icon →

↑  
View Icon

**Figure 234.** Diagnostics page

## Editing the Diagnostics Settings

Selecting the **Edit** icon allows you to change the diagnostics mode and identify the log interval (how often the statistics are written to a log).

➤ **To change the settings, follow these steps:**

1. Select **System Diagnostics**.
2. Select **Diagnostics Statistics**. The Diagnostics list page shown in [Figure 234](#) displays.
3. Click the **Edit** icon next to the component you want to change. The Configure Diagnostics page shown in [Figure 235 on page 370](#) displays.

**Figure 235.** Diagnostics Edit page

4. Enter the information described in [Table 138](#) to change the diagnostic settings.
5. Click **Submit** to change the record.

[Table 138](#) lists and describes the fields on the Diagnostic Edit page.

**Table 138.** Diagnostic fields and descriptions

Field Name	Description
<b>Diagnostics Mode</b>	Use the drop-down list to select the appropriate mode — Disabled or Enabled. The default value is Disabled.
<b>Log Interval (in seconds)</b>	Enter the number of seconds to wait before new information is written to the log. The default value is 60 seconds.

## Resetting Diagnostics Statistics

- **To reset the statistics for any component, follow these steps:**
  1. Select **System Diagnostics**.
  2. Select **Diagnostics Statistics**. The Diagnostics list page as shown in [Figure 234 on page 369](#) displays.
  3. Click the **View** icon next to the component you want to change. The component's diagnostic page displays.
  4. Click **Reset Statistics**.
  5. Click **Back to Diagnostics Home Page**.

## ATS Panel Intrusion

Use the Component Diagnostics page shown in [Figure 236](#) to view the following statistics:

- Ping interval
- Reconnect interval
- Online
- Connection state
- Number of messages not acknowledged by panel
- Number of messages received
- Number of polling attempts sent
- Number of panel events published
- Number of input events published
- Number of invalid packets received

The Component Diagnostic displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostic list page.

Component Diagnostics

Instructions

View Diagnostics

Search:

[Back to Diagnostics Home Page](#)  
[Reset Statistics](#)

Statistics Creation Time Mon Jun 28 11:26:26 EDT 2004

ATS Tecom Panel Name ATS Panel

Address 123.123.11.1

Port 8400

Statistic	Value
Ping Interval	500
Reconnect Interval	15
Online	false
Connection State	UNKNOWN
Number of Messages not Acknowledged by Panel	0
Number of Messages Received	0
Number of Polling Attempts Sent	7
Number of Panel Events Published	1
Number of Area Events Published	0
Number of Input Events Published	0
Number of Invalid Packets Received	0

**Figure 236.** Component Diagnostics page

## Database Connection Pool

Use the Database Connection Pool page shown in [Figure 237](#) to view the following statistics:

- Connection pool size
- Highest connection used
- Number of leases obtained
- Average lease time
- Number of lease waits
- Average lease wait time

The Database Connection Pool page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

Database Connection Pool

**Instructions**  
View Database Connection Pool

Search:

[Back to Diagnostics Home Page](#)  
[Reset Statistics](#)  
Statistics Creation Time: Mon Jun 28 11:26:24 EDT 2004

Statistic	Value
Connection pool size	20
Highest Connection Used	3
Number of lease obtained	3386
Average Lease Time	16.0
Number of leases waits	0
Average lease wait time	0.0

**Figure 237.** Database Connection Pool page

## Database Transactions Diagnostics

Use the Database Transactions Diagnostics page shown in [Figure 238](#) to view the following statistics:

- Transactions
- Number
- Average (milliseconds)
- Minimum in (milliseconds)
- Maximum in (milliseconds)
- Commits
- Rollbacks

The Database Transactions Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

Database Transaction Diagnostics

Instructions

View Database Transaction Diagnostics

Search:

[Back to Diagnostics Home Page](#)  
[Reset Statistics](#)  

Statistics Creation Time: Mon Jun 28 11:26:24 EDT 2004

Transaction	Number	Average (milliseconds)	Minimum (milliseconds)	Maximum (milliseconds)	Commits	Rollbacks
All Transactions	1	60.0	60	60	1	0
net.casi.datalayer.transactions.OperatorHistoryTransactions.insert	1	60.0	60	60	1	0

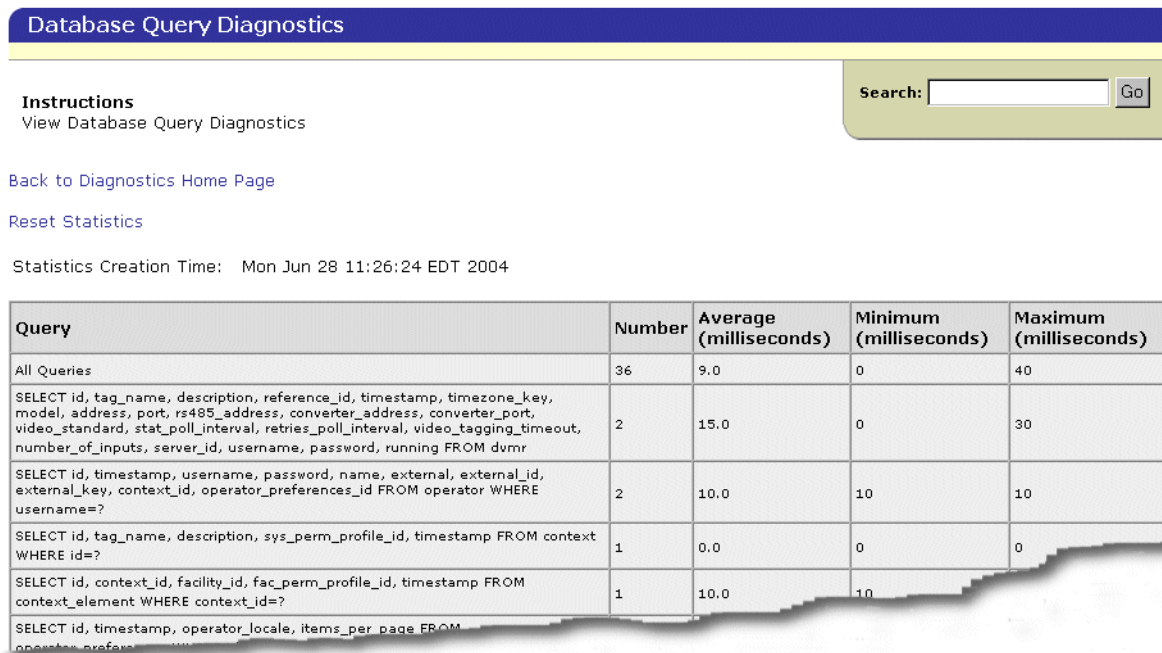
**Figure 238.** Database Transactions

## Database Queries Diagnostics

Use the Database Query Diagnostics page shown in [Figure 239](#) to view the following statistics:

- Query name
- Number
- Average (milliseconds)
- Minimum (milliseconds)
- Maximum (milliseconds)

The Database Query Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.



**Figure 239.** Database Queries page

## Facility Membership Cache

Use the Facility Membership Cache page shown in [Figure 240](#) to view the following statistics:

- maximum cache Size
- Current size
- Total misses
- Total hits
- Hit percent
- Cache purges

The Facility Membership Cache page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

Database Connection Pool

Instructions

View Database Connection Pool

Search:

[Back to Diagnostics Home Page](#)  
[Reset Statistics](#)  

Statistics Creation Time: Mon Jun 28 11:26:24 EDT 2004

Statistic	Value
Connection pool size	20
Highest Connection Used	3
Number of lease obtained	3386
Average Lease Time	16.0
Number of leases waits	0
Average lease wait time	0.0

**Figure 240.** Facility Membership Cache page

## JVM Statistics

Use the JVM Diagnostics page shown in [Figure 241](#) to view the following statistics:

- Maximum amount of memory available
- Total memory claimed
- Free memory available

The number of available processors is also listed on this page.

The JVM Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

JVM Diagnostics	
<b>Instructions</b> View JVM Diagnostics	
<a href="#">Back to Diagnostics Home Page</a>	
<a href="#">Reset Statistics</a>	
Available processors: 1	
Statistic	Value
Maximum amount of memory available:	65088K
Total memory claimed:	56892K
Free memory available:	14218K

**Figure 241.** JVM Diagnostics page



## Media Diagnostics

Use the Media Diagnostics page shown in [Figure 242](#) to view the following statistics:

- Total KB per second
- Percentage of 10 MB network
- Percentage of 100 MB network
- DVRs and workstation host names
- Current kilobytes per second
- Current Frames per second

The Media Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

**Media Diagnostics**

**Instructions**  
View Media Diagnostics

Search:  Go

[Back to Diagnostics Home Page](#)

[Reset Statistics](#)

Total KB Per Second: 0

Percentage Of 10 MB Network: 0.0

Percentage Of 100 MB Network: 0.0

Statistics Creation Time: Mon Jun 28 11:26:25 EDT 2004

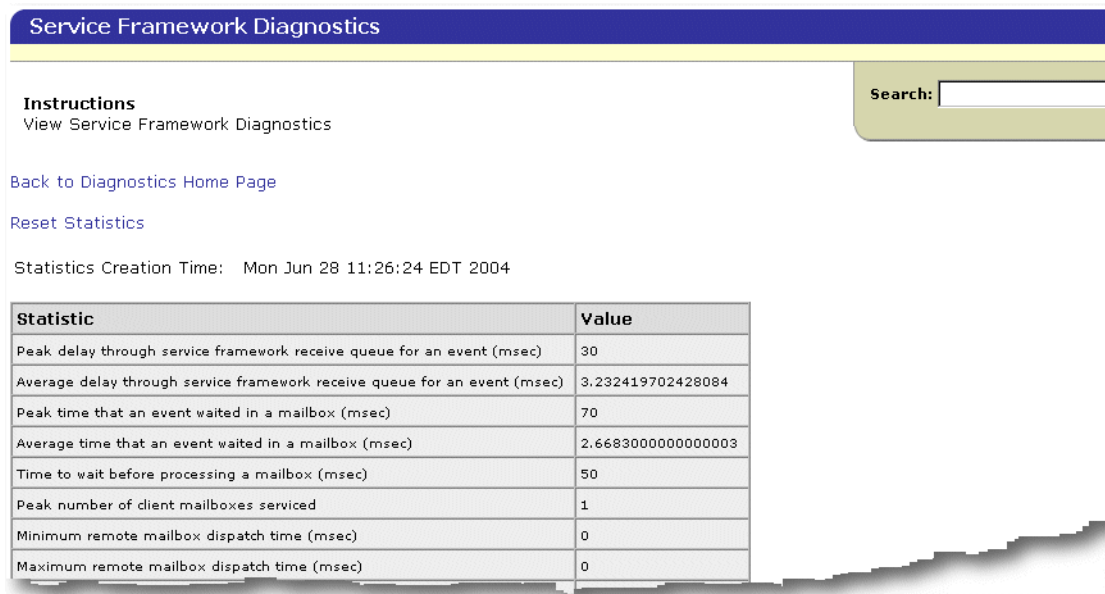
DVRs and Workstation Host Names	Current KiloBytes Per Second	Current Frames Per Second
---------------------------------	------------------------------	---------------------------

**Figure 242.** Media Diagnostics page

## Service Framework Diagnostics

The Service Framework Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

- Peak delay through service framework queue for an event (msec)
- Average delay through service framework queue for an event (msec)
- Peak time that an event waited in a mailbox (msec)
- Average time that an event waited in a mailbox (msec)
- Time to wait before processing a mailbox (msec)
- Peak number of client mailboxes serviced
- Minimum remote mailbox dispatch time (msec)
- Maximum remote mailbox dispatch time (msec)
- Maximum total remote mailbox dispatch time (msec)
- Current number of concurrent mailbox dispatch threads
- Peak number of concurrent mailbox threads
- Peak number of concurrent mailbox dispatch threads
- Average number of events sent per xml-rpc mailbox transactions
- Average time it took to filter an event (msec)
- Total number of dropped events
- Total number of events delivered
- Total number of xml-rpc requests/sec
- Max measured deadline timing error (msec)
- Max measured internal clock drift (msec)
- Max processing time to check all mailboxes (msec)



**Figure 243.** Service Framework Diagnostics page

## System Status Diagnostics

Use the System Status Diagnostics page shown in [Figure 244](#) to view the following statistics:

- Number of application servers
- Facility Commander server
- Number of remote media servers
- Number of DVMRs
- Number of client workstations
- Number of managed proxy components

System Status also identifies DVRs and client applications and reports the connectivity status.

The System Status Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.

System Status Diagnostics

Instructions

View System Status

Search:

[Back to Diagnostics Home Page](#)  
[Reset Statistics](#)  

Statistics Creation Time Wed Jul 07 08:34:22 EDT 2004

Statistic	Value
Number of Application Servers	1
FCServer	Connected
Number of Remote Media Servers	0
Number of DVMRS	1
DVR 100_10	Connected
Number of Client Workstations	2
FCClient	Connected
FCClient 200	Connected
Number of Managed Proxy Components	0

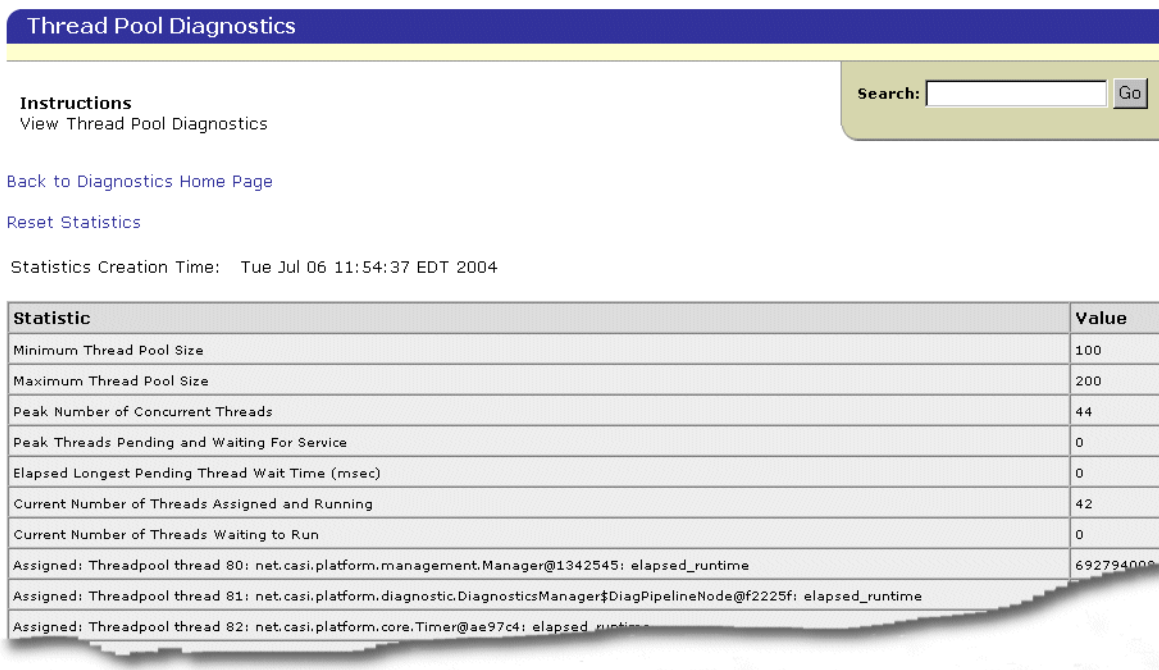
**Figure 244.** System Status Diagnostics page

## Thread Pool Manager Diagnostics

Use the Thread Pool Manager Diagnostics page shown in [Figure 245](#) to view the following statistics:

- Minimum and maximum thread pool size
- Peak number of concurrent threads
- Peak threads pending and waiting for service
- Elapsed longest pending thread wait time
- Current number of threads assigned and running
- Current number of threads waiting to run

The Thread Pool Manager Diagnostics page displays the date and time the last event was written to a log. Use this page to reset the statistics and to return to the Diagnostics list page.



**Figure 245.** Thread Pool Diagnostics

# Chapter 19. Advanced Configuration

This chapter describes how to customize the Facility Commander Launcher window, verify the server's host name, and change the host name.

Readers should be familiar with using a text editor application.



---

**In this chapter:**

[\*Customizing Launcher Window on page 382\*](#)

[\*Verifying Computer Host Name on page 384\*](#)

[\*Changing the Host Name or IP Address on page 385\*](#)

[\*Enabling SSL Encryption for Picture Perfect on page 388\*](#)

## Customizing Launcher Window

You can customize the Facility Commander Launcher window by changing the existing icons or by adding up to six additional applications, such as WaveReader or any other application you use often.

The Facility Commander Launcher on Window client systems is modified by changing to the client properties file, refer to:

- [Adding Custom Icons](#)
- [Adding External Applications on page 383](#)

### Adding Custom Icons

► **To add custom icons to the Launcher window, follow these steps:**

1. On the Facility Commander client system, open the `client.properties` file using a text editor such as Notepad. The client properties file is found in a directory similar to this:

`C:\Program Files\FacilityCommanderClient\lib\resources`

(The path may differ depending on where Facility Commander was installed on the system.)

2. Enter the text shown in [Table 139](#) for each icon you want to change.

**Table 139.** Add Custom Icons to Launcher window

Application	Add this text to client.properties file:
Alarm Monitor	<code>workspace.icon.alarmMonitor= c:/myPath/myIcon.gif</code>
Event Monitor	<code>workspace.icon.eventMonitor= c:/myPath/myIcon.gif</code>
Video Console	<code>workspace.icon.cctvMonitor= c:/myPath/myIcon.gif</code>
Graphic Viewer	<code>workspace.icon.graphicViewer= c:/myPath/myIcon.gif</code>
Main Viewer	<code>workspace.icon.mainViewer= c:/myPath/myIcon.gif</code>
Graphic Editor	<code>workspace.icon.graphicEditor= c:/myPath/myIcon.gif</code>
Symbol Editor	<code>workspace.icon.symbolEditor= c:/myPath/myIcon.gif</code>
Web Report Viewer	<code>workspace.icon.webReportViewer= c:/myPath/myIcon.gif</code>

## Adding External Applications

There are sample lines in the properties file are commented out so they are not used. Uncomment the lines in the file and edit them to add external applications to the Facility Commander Launcher window.



**Figure 246.** Notepad application added to Launcher window

► **To add external applications to the Launcher window, follow these steps:**

1. On the Facility Commander client system, open the `client.properties` file using a text editor such as Notepad.
2. Edit three lines to add the executable, icon, and tooltip for each application. The information includes:
  - directory path of application executable
  - directory path of icon graphic
  - tooltip text

This path must point to an existing and valid file. All path separators must use a forward slash "/" instead of a back slash "\".

The path includes a number (N), which indicates the icon position on the Applications toolbar.

Also, make sure the icon is the correct size to fit on the toolbar. The maximum size is 32 x 32 pixels.

The format is:

```
workspace.user_application.N.exe=
workspace.user_application.N.icon=
workspace.user_application.N.tooltip=
```

**Sample Entry:**

The text below represents what should be entered if you want to add an application such as Notepad to the Launcher window. (This change adds the Notepad icon to the first position on the Applications toolbar.)

```
launcher.user_application.1.exe=c:/winnt/system32/
notepad.exe
launcher.user_application.1.icon=c:/path/
wmplayer.gif
launcher.user_application.1.tooltip=Media Player
```

3. Save the changes and close the text editor when you are finished.

## Verifying Computer Host Name

Facility Commander servers, remote media servers, and client workstations all have host names, which are used to identify the system to the network.

### Windows

➤ **To verify the host name, follow these steps:**

1. Right-click **My Computer** on the desktop.
2. Select **Properties** from the shortcut menu.
3. Select the **Network Identification** tab. The computer host name is listed on this page.

### Linux/AIX/Windows

➤ **To verify the host name:**

1. Open a terminal window and type the host name command:

```
hostname
```



## Changing the Host Name or IP Address

If you are installing Facility Commander on a new system, or a system that is already configured in your network, the server's host name may need to be changed.

On a new system, only a change on the Facility Commander server is required. Refer to the following sections:

- *Linux Operating System*
- [AIX Operating System on page 386](#)
- [Windows Operating System on page 386](#)

On an existing system, changes are required on the following systems:

- *Facility Commander server*
- [Facility Commander Clients on page 386](#)
- [Picture Perfect Server on page 386](#)

Use the checklist in [Table 140](#) to change the host name:

**Table 140.** Change Host Name Checklist

Facility Commander Server	
✓	Disable client encryption. Refer to <a href="#">Changing the Client Encryption on page 387</a> for instructions to enable or disable encryption between the Facility Commander server and the client applications.
✓	Change the host name on the Facility Commander server. Refer to <a href="#">Changing the Host Name on Server Record on page 387</a> for more information.
✓	Change the operating system host name. Refer to the following sections for the appropriate operating system.
Linux Operating System	
✓	Run the <code>chhostlinux.sh</code> script located in the following directory: <code>/var/FacilityCommanderServer/server/webapps/Merlin/WEB-INF/classes/resources</code>
✓	Select the database you are using and enter the new host name and IP address. Enter the same IP address if it is not changing.

**Table 140.** Change Host Name Checklist (Continued)

AIX Operating System	
✓	Run the <code>chhostaix.sh</code> script located in the following directory: <code>/var/FacilityCommanderServer/server/webapps/Merlin/WEB-INF/classes/resources</code>
✓	Select the database you are using and enter the new host name and IP address. Enter the same IP address if it is not changing.
Windows Operating System	
✓	Edit the system configuration file. Refer to <a href="#">Advanced Configuration on page 381</a> for more information.
✓	Change computer name in System Properties. Refer to <a href="#">Changing the Computer Name on Server on page 390</a> for more information.
✓	Change server name in SQL Server. Refer to <a href="#">Changing the Server Name in SQL Server on page 391</a> for more information.
Facility Commander Clients	
✓	Edit the host file. This step is only necessary if the customer is <i>not</i> using domain name service (DNS) server. Refer to <a href="#">Editing the Host File on a Client System on page 387</a> for more information.
✓	Edit the client properties file. <a href="#">Editing the Client Properties File on a Client System on page 388</a> .
✓	Delete existing security certificates.
✓	Enable client encryption. Refer to <a href="#">Changing the Client Encryption on page 387</a> for instructions to enable encryption.
Picture Perfect Server	
✓	Edit the configuration file. Refer to <a href="#">Editing the Picture Perfect Configuration File on page 388</a> for more information.
✓	Recreate SSL certificates. Refer to <i>Picture Perfect External Interface Installation Guide</i> for more information.
✓	Restart the Picture Perfect system for the changes to take effect.

## Changing the Client Encryption

*This is required only if you have SSL enabled.*

➤ **To change the encryption settings, follow these steps:**

1. Using the web browser, select **System Administration**, and then **System Parameters**. The Configure System Parameters page displays.
  - To enable encryption, select the **Enable Encryption With Clients** check box.
  - To disable encryption, clear the **Enable Encryption With Clients** check box.
2. Click **Submit**.

## Changing the Host Name on Server Record

➤ **To change the host name, follow these steps:**

1. Select **System Administration**, and then **Facility Commander Servers**. The Configure Facility Commander Servers page displays.
2. Locate the Facility Commander server's tag name. Click the tag name to display the configuration information for the selected server.
3. Use the **Host Name** field to enter the new host name for this server. The host name is case sensitive.
4. Click **Submit**.

## Editing the Host File on a Client System

*Required only if the customer is not using domain name server (DNS).*

➤ **To change the host name, follow these steps:**

1. On the taskbar, click the **Start** button, and then select **Run**. The Run window displays.
2. Enter the following path:  
`\winnt\system32\drivers\etc`
3. Click **OK**.
4. Create a backup copy of the Host file.
5. Open the original file using a text editor, such as Notepad.
6. Locate the line of text with the host name. Replace the host name with the new host name.
7. Save the file and close the text editor.

## Editing the Client Properties File on a Client System

➤ **To edit the client properties, follow these steps:**

1. On the taskbar, click the **Start** button, and then select **Run**. The Run window displays.
2. Enter the following path:  
`\Program Files\FacilityCommanderClient\lib\resources`  
This is the default directory, unless a different directory was selected during the installation process.
3. Click **OK**.
4. Create a backup copy of the `client.properties` file.
5. Open the original file using a text editor, such as Notepad.
6. Locate the following line:  
`hostURL=http://host_name:8085/Merlin/servlet/  
net.casi.app.AppHttpServlet`
7. Replace "host\_name" with the host name you want to use.
8. Save the file and close the text editor.

## Editing the Picture Perfect Configuration File

➤ **To update the Facility Commander Server host name on the Picture Perfect system, follow these steps:**

1. Login as root and open a new terminal window.
2. Navigate to this directory:  
`/cas/db/text`
3. Create a backup copy of the `eifvmtmgr.cfg` file.
4. Open the original file using a text editor.
5. Locate the following line:  
`http://host_name/Merlin/servlet/  
net.casi.AppHttpServlet`
6. Change the host name to the new host name.
7. Save the file and close the text editor.

This completes the procedure for changing the host name.

## Enabling SSL Encryption for Picture Perfect

This section describes how to configure SSL support between the Picture Perfect server and the Facility Commander server. Using SSL enables a secure communication channel between these two systems.

The steps in this section are very technical and should only be performed by an IT Network Administrator who is knowledgeable about SSL.

The following commands apply to a Windows Facility Commander server and a Linux Picture Perfect server. Because your system configuration may be different., ask your Network Administrator who will know how to execute these commands on your system.

To enable SSL encryption, follow the steps listed in [Table 141](#):

**Table 141.** Overview of SSL Instructions for Picture Perfect

Procedures	
✓	Copy the Facility Commander Certificate to Picture Perfect. Refer to: <ul style="list-style-type: none"> <li>• <a href="#">Copying File from Facility Commander on page 389.</a></li> <li>• <a href="#">Linux and AIX on page 390.</a></li> <li>• <a href="#">FTP the File to Picture Perfect on page 390.</a></li> </ul>
✓	Move the Facility Commander Certificate to <code>/cas/db/text</code> . Refer to page 391.
✓	Generate Picture Perfect Key file. Refer to page 391.
✓	Generate the Picture Perfect Certificate Request from the Picture Perfect Key. Refer to page 392.
✓	Generate the Picture Perfect Signed Certificate. Refer to page 392.
✓	Generate the Picture Perfect PEM file. Refer to page 393.
✓	Update the EIF Event Manager Configuration file to enable SSL. Refer to page 393.
✓	Update the EIF Request Manager Configuration file. Refer to page 395
✓	Copy the certificate to the Facility Commander server. Refer to page 397.
✓	Add the Picture Perfect Certificate. Refer to page 398.
✓	Enable the SSL communication between Picture Perfect and Facility Commander. Refer to page 399.

The server certificate on the Facility Commander system is used by the Picture Perfect SSL library. The following commands use FTP to transfer the certificate, **server.cer**, in binary mode from a Windows server to Picture Perfect.

## Copying File from Facility Commander

The **server.cer** file is located in the certificates directory under the Facility Commander web application as shown below. These directories are the default installation paths, which may not be the same if a different path was chosen during Facility Commander installation.

- **Linux and AIX**

The file is located in the following directory:

`/var/FacilityCommanderServer/server/webapps/Merlin/  
WEB-INF/classes/resources/certificates`

- **FTP the File to Picture Perfect**

*Copy the server.cer file and follow these instructions to connect to the remote Picture Perfect system.*

```
c:> cd "\\Program  
Files\FacilityCommanderServer\server\webapps\Merlin\WEB-  
INF\classes\resources\certificates"  
  
c:> ftp pphost  
Connected to pphost.na.ilxi.net.  
220 pphost FTP server (Version wu-2.6.1-20) ready.  
Name (pphost:install): install  
Password: <install's password>  
230 User install logged in.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> bin  
200 Type set to I.  
ftp> put server.cer  
ftp> quit
```

## Moving File to Picture Perfect

Move the Facility Commander Certificate to `/cas/db/text`. These commands describe logging in to the Picture Perfect system as “install” and then becoming “root” to copy the file.

```
c:> telnet pphost

Trying ...

Connected to pphost.na.ilxi.net.

Escape character is '^]'.

Kernel 2.4.9-31 on an i686

login: install

Password: <install's password>

Last login: Wed Dec 18 15:06:20 from bctrenegade

$ su

Password: <root's password>

# cp server.cer /cas/db/text/
```

## Generating Picture Perfect Key File

Use these commands to produce a key file, which will be used to create the Picture Perfect certificate. You should be in the `/cas/db/text` directory when the `openssl` command is run. You are required to supply your own password (PEM pass phrase) for the key file. You will also use this password later in the configuration.

```
# cd /cas/db/text

# openssl genrsa -des3 -out picture.key 512/1024

Generating RSA private key, 512 bit long modulus
.....+++++++
.....+++++++

e is 65537 (0x10001)

Enter PEM pass phrase: <password>

Verifying password - Enter PEM pass phrase: <password>
```

## Generating Picture Perfect Certificate Request

The next step is to generate a Picture Perfect certificate request from the Picture Perfect key.

Use the `openssl` command to generate the certificate request used by the Facility Commander server. You are required to supply the password used from the previous `openssl` command. The command prompts for several fields from the certificate.

The important field during this activity is the `Common Name` field. This must be the host name of the Picture Perfect system. If this is not correct, then the Facility Commander will not be able to use the proper certificate when Picture Perfect attempts to communicate.

```
# openssl req -new -key picture.key -out picture.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase: <password>
You are about to be asked to enter information that
will be
incorporated into your certificate request.
What you are about to enter is what is called a
Distinguished
Name or a DN.
There are quite a few fields but you can leave some
blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
US
State or Province Name (full name) [Some-State]:FL
FL
Locality Name (eg, city) []:Boca
Boca
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:CASI
CASI
Organizational Unit Name (eg, section) []:eng
eng
Common Name (eg, your name or your server's hostname)
[]:pphost
pphost
Email Address []:fc@casi-rusco.com
casi-rusco.com
Please enter the following 'extra' attributes to be
sent with your
certificate request
A challenge password []:
An optional company name []:
```



## Generating Picture Perfect Signed Certificate

The following `openssl` command creates a signed certificate file. You will be prompted for the password used in the previous commands.

```
# openssl req -x509 -key picture.key -in picture.csr -  
out picture.crt
```

Using the configuration from `/usr/share/ssl/openssl.cnf`, enter PEM pass phrase: `<password>`

## Generating Picture Perfect PEM File

The following command creates the PEM file that will be used by the Facility Commander system.

```
# cat picture.key picture.crt > picture.pem
```

## Updating EIF Event Manager Configuration File

The following set of commands uses `vi` to modify the `EIFEVTmgr.cfg` file to configure Picture Perfect to use SSL with Facility Commander. You should make a copy of the configuration file in case you have to restore the previous version.

```
# cp EIFEVTmgr.cfg EIFEVTmgr.cfg.bak
```

The following properties need to be configured correctly to support SSL: URL, PORT, RANDOM, CERTIFICATE, SSL\_PASSWORD.

- The URL is modified to use the https protocol.
- The non-secure PORT, 8085, is commented out, and the secure PORT is uncommented to use 8443.
- The RANDOM and CERTIFICATE properties are not commented to use the values from the examples.
- The SSL\_PASSWORD is the same password used to generate the Picture Perfect keys. The following shows the original and the modified copy of the configuration file.

**Table 142.** EIF Event Manager Configuration File

Original File (SSL Enabled)	Modified File (SSL Enabled)
#	#
# Copyright (C) 2002 GE Interlogix	# Copyright (C) 2002 GE Interlogix
# All Rights Reserved.	# All Rights Reserved.
#	#
# eifevtmgr.cfg	# eifevtmgr.cfg
#	#
# @(#) eifevtmgr.cfg 1.0 12/12/02	# @(#) eifevtmgr.cfg 1.0 12/12/02
#	#
# Supported Property Examples	# Supported Property Examples
#	#
# URL=http://hostname/facilitycommander/servlet/ net.casi.app.AppHttpServlet	# URL=http://hostname/facilitycommander/servlet/ net.casi.app.AppHttpServlet
# PORT=8085	# PORT=8085
# Default SSL port	# Default SSL port
# PORT=8443	# PORT=8443
# KEEP_ALIVE=FALSE	# KEEP_ALIVE=FALSE
# MESSAGE_TRACE=TRUE	# MESSAGE_TRACE=TRUE
# RESEND_BUFFER_SIZE=256	# RESEND_BUFFER_SIZE=256
# RANDOM=/cas/db/text/random.pem	# RANDOM=/cas/db/text/random.pem
# CERTIFICATE=/cas/db/text/server.cer	# CERTIFICATE=/cas/db/text/server.cer
#	#
# URL=http://bctrenegade/FacilityCommander/servlet/ net.casi.app.AppHttpServlet	URL=https://bctrenegade/FacilityCommander/servlet/ net.casi.app.AppHttpServlet
# PORT=8085	#PORT=8085
# SSL Default Port	# SSL Default Port
# PORT=8443	PORT=8443
KEEP_ALIVE=TRUE	KEEP_ALIVE=TRUE
# KEEP_ALIVE=FALSE	# KEEP_ALIVE=FALSE
# RANDOM=/cas/db/text/random.pem	RANDOM=/cas/db/text/random.pem
# CERTIFICATE=/cas/db/text/server.cer	CERTIFICATE=/cas/db/text/server.cer
# MESSAGE_TRACE=TRUE	# MESSAGE_TRACE=TRUE
# RESEND_BUFFER_SIZE=256	# RESEND_BUFFER_SIZE=256
	SSL_PASSWORD=password

## Updating EIF Request Manager Configuration File

The following set of commands uses `vi` to modify the `elfreqmgr.cfg` file to configure Picture Perfect to use SSL with Facility Commander. You should make a copy of the configuration file in case you have to revert to the previous version.

```
# cp elfreqmgr.cfg elfreqmgr.cfg.bak
```

The following properties need to be configured correctly to support SSL: `PROTOCOL`, `RANDOM`, `KEYFILE`, `SSL_PASSWORD`.

- The non-secure protocol is commented out, and the secure protocol is uncommented to use HTTPS.
- The `SSL_PASSWORD` is the same password used to generate the Picture Perfect keys.
- The `RANDOM` and `KEYFILE` properties are uncommented to use the values from the examples.

Using the `cat` command, you can view the output of a modified configuration file.

**Table 143.** EIF Request Manager Configuration File

Original File (SSL Disabled)	Modified File (SSL Enabled)
#	#
# Copyright (C) 2002 GE Interlogix	# Copyright (C) 2002 GE Interlogix
# All Rights Reserved.	# All Rights Reserved.
#	#
# eifreqmgr.cfg	# eifreqmgr.cfg
#	#
# @(#) eifreqmgr.cfg 1.0 12/12/02	# @(#) eifreqmgr.cfg 1.0 12/12/02
#	#
# Supported Property Examples	# Supported Property Examples
#	#
# Non-SSL connection	# Non-SSL connection
# PROTOCOL=HTTP	# PROTOCOL=HTTP
# SSL connection	# SSL connection
# PROTOCOL=HTTPS	# PROTOCOL=HTTPS
# PORT=8088	# PORT=8088
# KEEP_ALIVE=TRUE	# KEEP_ALIVE=TRUE
# RANDOM=/cas/db/text/random.pem	# RANDOM=/cas/db/text/random.pem
# KEYFILE=/cas/db/text/picture.pem	# KEYFILE=/cas/db/text/picture.pem
# SESSION_TIMEOUT=10	# SESSION_TIMEOUT=10
# MESSAGE_TRACE=TRUE	# MESSAGE_TRACE=TRUE
#	#
PROTOCOL=HTTP	PROTOCOL=HTTPS
PORT=8088	PORT=8088
KEEP_ALIVE=TRUE	KEEP_ALIVE=TRUE
# RANDOM=/cas/db/text/random.pem	RANDOM=/cas/db/text/random.pem
# KEYFILE=/cas/db/text/picture.pem	KEYFILE=/cas/db/text/picture.pem
	SSL_PASSWORD=password

## Copying Certificate to Facility Commander Server

Once you have created and configured the necessary files, you should exit the telnet session to return to the Facility Commander system.

The commands are:

```
# exit
```

```
$ exit
```

```
Connection closed by foreign host.
```

On the Facility Commander system, navigate to the Facility Commander web applications directory, and then to the Certificates directory. Use the `hostname` command to verify the machine is the correct host system. Use the `pwd` command to verify the directory structure.

Use the `ftp` command to connect to the Picture Perfect system and to transfer the `picture.crt` file created in the previous steps. The file is transferred in binary mode.

```
c:> cd "/Program Files/Facility CommanderServer/
webapps/Merlin/WEB-INF/classes/resources/certificates"
c:> ftp pphost
Connected to pphost.na.ilxi.net.
220 pphost FTP server (Version wu-2.6.1-20) ready.
Name (pphost:install): install
Password: <install's password>
230 User install logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Type set to I.
ftp> cd /cas/db/text
ftp> get picture.crt
ftp> quit
```

## Adding Picture Perfect Certificate

The **keytool** command should be in the path. The **keytool** command adds the certificate created in Picture Perfect to the server's trusted keystore file.

You are asked to identify the **server.trust** file password, which is generated during the Facility Commander installation. The password can be found by viewing the contents of **ssl.bat** file (Windows) or the **ssl.sh** file (Linux/AIX).

Examine the contents of the file to locate the **-storepass** parameter, which is a randomly generated 10-character string (**-storepass TKXQWPLSRN**) and is also the password you need to provide at the keytool password prompt. You are prompted to trust the certificate.

```
c:> keytool -import -keystore server.trust -alias
picture -file picture.crt
Enter keystore password: <password>
Owner: EMAILADDRESS=fc@casi-rusco.com, CN=pphost,
OU=eng, O=CASI,
L=Boca, ST=FL, C=US
Issuer: EMAILADDRESS=fc@casi-rusco.com, CN=pphost,
OU=eng, O=CASI,
L=Boca, ST=FL, C=US
Serial number: 0
Valid from: Wed Dec 18 15:13:39 EST 2002 until: Fri Jan
17 15:13:39
EST 2003
Certificate fingerprints:
MD5: 8F:06:F8:3D:48:4C:59:EF:6D:2E:E5:04:6D:7B:DD:4C
SHA1:
E8:60:F8:C1:85:90:5F:CF:9B:B9:16:2B:72:53:E9:5D:81:A6:
97:70
Trust this certificate? [no]: yes
Certificate was added to keystore
```

## Enabling SSL Communication on Facility Commander

To enable SSL communication between the Picture Perfect and Facility Commander systems, open the web browser and log on to Facility Commander.

► **To enable SSL communication, follow these steps:**

1. Select **System Administration** and **Access Control Systems**. The Access Control Systems page displays.
2. Select the Picture Perfect system to edit. The Configure Access Control System page displays.
3. Select the **Advanced** tab.
4. Select the **Enable Encryption with Access Control System** check box.
5. Click **Submit**.
6. Restart the Picture Perfect system, which will allow the Picture Perfect system to communicate with Facility Commander using SSL encryption.





## Appendix A. Edit Configuration Files for Informix Backup to Disk

This section describes the steps needed to modify the configuration files, which allows you to backup the database to a disk file. Read [Backup/Restore Informix Databases on page 349](#) before proceeding.

*Once you edit these files to change the output to disk, the backup utility will not write to tape because the output destination has been changed from tape to disk.*

For instructions, refer to the following sections:

- [Editing the Informix Configuration File on page 403](#)
- [Scheduling the Backup Utility on page 404](#)

## Configuration Files

**Table 144.** Configuration files and default values

Configuration File	File Name and Parameters
<b>General Backup</b>	
<p>Edit the Facility Commander Backup Utility configuration file to change the parameters, which include the location of log files and the number of log files retained.</p> <p>For each parameter listed below, uncomment (remove the # sign) the command to enable the value assignment.</p>	File: <code>/etc/BackupUtility/config</code>
<ul style="list-style-type: none"> <li>Use to identify the location of log files. This parameter may be changed depending on operating system, disk space, and more.</li> </ul>	Parameter: <code>LOG_DIR</code> Default value: <code>/var/log/BackupUtility</code>
<ul style="list-style-type: none"> <li>Use to identify the tape device used for file backups. This is the default setting.</li> </ul>	Parameter: <code>BACKUP_DEVICE</code> Default value: <code>/dev/tape</code> New value: <code>/dev/disk</code>
<ul style="list-style-type: none"> <li>Use to identify the directory where backup files are stored. This is the default setting.</li> </ul>	Parameter: <code>BACKUP_DEVICE</code> Default value: <code>/bud</code>
<ul style="list-style-type: none"> <li>Use to minimize the number of log files. This parameter minimizes the impact on free space on the partition containing the file backup logs. The backup utility retains a limited number of each log file type (full or Incremental).</li> <li>The default value can be scaled up or down to balance more history or more free space.</li> </ul>	Parameter: <code>NUMBER_OF_LOGS_RETAINED</code> Default value: 7
<b>Database Backup:</b> Refer to <a href="#">Editing the Informix Configuration File on page 403</a> .	
<p>Edit the Informix configuration file when you want to back up to disk instead of tape.</p>	File: <code>/usr/informix/etc/onconfig</code>
<ul style="list-style-type: none"> <li>Defines the device file associated with the tape drive to use for database backups. The default value is a link to the device file.</li> </ul>	Parameter: <code>TAPEDEV</code> Default value: <code>/dev/tape</code> New value: <code>/bud/BackupUtility/db_backup.cpio</code>
<b>Database Support Files Backup</b>	
<p>Use to identify the list of directories to include in a file system backup.</p> <ul style="list-style-type: none"> <li>The file should contain one entry per line. The entry should be the path to a directory or file to back up.</li> <li>When an entry identifies a directory, the contents are recursively included in the backup.</li> <li>The path may be relative to the root directory or absolute.</li> </ul>	File: <code>/etc/BackupUtility/backup_paths</code>

## Editing the Informix Configuration File

➤ **To edit the Informix configuration file, follow these steps:**

Use the instructions in [Table 145](#) to edit the configuration file. The instructions use `vi` as the text editor, however, you can use any text editor installed on the system.

**Table 145.** Edit configuration file

Action	Type
Navigate to the directory.	<code>cd /usr/informix/etc [Enter]</code>
Open file with vi editor.	<code>vi onconfig [Enter]</code>
Locate parameter.	Parameter: <b>TAPEDEV</b>
- Move to this location.	<code>/dev/tape [Enter]</code>
- Delete each character in the old parameter value, by typing "x" nine times to remove the previous entry.	<code>xxxxxxxxx [Enter]</code>
- Change to an input mode.	<code>i</code>
- Add new entry.	<code>/bud/BackupUtility/ db_backup.cpio</code>
- Exit editor and save changes.	<code>[Esc]:x [Enter]</code>
View file to confirm changes.	<code>cat onconfig [Enter]</code>

## Scheduling the Backup Utility

The backup utility can be launched by setting the task to run on a regular schedule or by manually running the task.

### Create a Cron Task

► **To run the task on a schedule, follow these steps:**

1. Use the vi text editor to edit the configuration file. Type:  
`crontab -e [Enter]`
2. Type: `i` to enter the input mode of the text editor.
3. Use the arrow keys to position the cursor at the end of the last line displayed. Press: `[Enter]` to create a new line.
4. Type:  
`30 2 * * * /usr/BackupUtility/BackupUtility B`

This line represents the command used to schedule this task at 2:30 am each day. The variables are: minute, hour, day of month, month, day of week, and command. Use an asterisk (\*) to indicate all days or months.

Exit the editor and save the changes. Type:

`[Esc]:x [Enter]`

5. View the scheduled tasks. Type:  
`crontab -l [Enter]`

### Launch the Script Manually

► **To run the task manually, follow these steps:**

1. Type:  
`cd /usr/BackupUtility [Enter]`
2. Type:  
`sh BackupUtility [Enter]`

**-OR-**

1. Log into the system as the Root user.
2. Type:  
`sh /usr/BackupUtility/BackupUtility B`

# Appendix B.

## Troubleshooting Information

This section provides trouble-shooting information for problems that may be not be resolved by consulting the user interface error message table. The table will be updated from experience gained through debugging customer problems, mostly based on input received from Customer Support and the Facility Commander test team.

**Table 146.** List of Common Problems with Possible Causes and Solutions

Problem	Possible Causes and Solutions
<b>Product Installation and Removal</b>	
After product installation you cannot log in the first time as the default admin operator.	<p>There are several possible causes of this problem. After performing the checks indicated in the steps below it may be necessary to change the logger configuration file to include more detailed information in the log file to help determine the cause of the problem.</p> <ol style="list-style-type: none"> <li>1. Verify that you have created a valid license file (<b>license.xml</b>) and is has been placed in the correct location. The license file must specify the correct Operating System and Database product.</li> <li>2. Verify the contents of the <b>systemconfig.xml</b> file and ensure that the database specification is correct. Verify all fields in the specification and that the host computer is accessible across the network.</li> </ol>
After product removal some files still remain in the software directories	The removal procedure does not remove any files that were changed or added after the installation. This is standard for all Windows application removals. These files can be deleted if the product will not be reinstalled. If you are installing a later version of the product you may wish to save the license and database encryption key files.
<b>Data Import</b>	

**Table 146.** List of Common Problems with Possible Causes and Solutions

Problem	Possible Causes and Solutions
After importing data from a Picture Perfect system to a Facility Commander server using the Informix database, the system has poor performance.	<p>Performance problems, if they occur, will be observable when bringing up client applications with a navigation pane. The pane will take several seconds to populate. These problems typically only occur at the initial data import, where the database has few or no records. The database engine is using inaccurate table size information thereby causing poor query performance. You can observe query performance using the database query diagnostic screen.</p> <p>Note that the system automatically forces an update of the table size information once per day at 3:30 am. To manually force the update to achieve optimal performance immediately, follow the procedure below.</p> <p>For Informix:</p> <ol style="list-style-type: none"> <li>1. Log in as the root user</li> <li>2. Enter the command: <code>cd /usr/Informix/bin/update</code></li> <li>3. Enter the command: <code>sh update</code></li> </ol>
Importing data from a Picture Perfect system fails.	<ol style="list-style-type: none"> <li>1. Verify proper network communications between the Facility Commander and Picture Perfect servers. Remember to verify that the DNS (Domain Name Server) is providing correct translation of host names to IP addresses when dynamic IP addressing is used on the network. For Unix systems verify the host name entries in the <code>/etc/hosts</code> file.</li> <li>2. Verify that the Facility Commander license enables access to Picture Perfect systems and the database. Examine the log file to determine this.</li> <li>3. Verify that the Facility Commander database record defining the Picture Perfect system has the correct user name and password to successfully log into the Picture Perfect system. Examine the log file to determine this.</li> <li>4. Verify that the correct version of the eif (External Interface) package has been installed on the Picture Perfect system and that it has also been licensed on that system. Examine the log file on the Picture Perfect system to determine this.</li> <li>5. Examine the Facility Commander server log file to see if a warning message is present indicating that there is a mismatch between the versions of the Facility Commander and Picture Perfect software. If this is the case, contact Customer Support for assistance.</li> <li>6. If encryption has been enabled between the Facility Commander and Picture Perfect servers, verify that the SSL password settings are correct between the two systems.</li> </ol>

**Table 146.** List of Common Problems with Possible Causes and Solutions

Problem	Possible Causes and Solutions
<b>All Client Applications</b>	
Client applications do not remember their size and position correctly.	<p>This problem is usually caused by the ATI HydraVision™ software that has the “Application position memory” option turned on.</p> <p>Perform the steps below to turn this option off.</p> <ol style="list-style-type: none"> <li>1. Right click on the ATI icon in the Windows task bar area to activate the ATI HydraVision Utility menu.</li> <li>2. Select the “Desktop Manager Configuration” item from the “HydraVision” menu.</li> <li>3. Clear the “Application position memory” check box and click <b>OK</b> to save the change</li> </ol>
<b>Alarm and Event Monitors</b>	
Alarms and events from Picture Perfect are not received even though the data import was successful.	<ol style="list-style-type: none"> <li>1. On the Picture Perfect server, verify that the URL address of the Facility Commander server is correct in the <code>/cas/db/text/eifevtmgr.cfg</code> file. Picture Perfect (tps) will need to be restarted after this file is changed.</li> <li>2. Verify proper network communications between the Facility Commander and Picture Perfect servers. Remember to verify that the DNS (Domain Name Server) is providing correct translation of host names to IP addresses when dynamic IP addressing is used on the network. For Unix systems verify the host name entries in the <code>/etc/hosts</code> file.</li> </ol>
<b>Graphic Editor, Symbol Editor, and Graphic Viewer</b>	
Graphic displays do not display on the list of candidates for deletion even though they exist on the server.	A graphic display cannot be deleted if another display links to it.
Graphic symbols or images do not display on the list of candidates for deletion even though they exist on the server.	Graphic symbols or images cannot be deleted as long as there is a graphic display that references them.
When adding an image to a symbol scheme, the workstation becomes very slow and the Windows Task Manager indicates almost 100% CPU usage.	<p>There is a known problem in the Java Swing library with certain GIF file formats. If this problem occurs, the image file cannot be used. Choose or create another image file.</p> <p>The operator must log off and exit the Facility Commander application to correct the CPU usage problem.</p>
When viewing a graphic display, the workstation becomes very slow and the Windows Task Manager indicates almost 100% CPU usage.	<p>There is a known problem in the Java Swing library with certain GIF file formats. This problem usually occurs because a Graphic Display was created containing a GIF file with a format that is not supported, or it is using a Symbol that was created with a GIF file of a format that is not supported.</p> <p>The GIF image must be deleted from the Graphic Display or Symbol Editor. If this problem occurs, the image file cannot be used. Choose or create another image file.</p> <p>The operator must log off and exit the Facility Commander application to correct the CPU usage problem.</p>

**Table 146.** List of Common Problems with Possible Causes and Solutions

Problem	Possible Causes and Solutions
Images imported from a non-mapped network drive display as blank in the Graphics Editor.	This is a known problem with the JLOOX™ Graphics Engine. A workaround is to map a drive letter to the network location and access the image from the mapped drive.
<b>Video Console</b>	
Video cannot be received from a digital video recorder (DVR) device.	There are several possible causes of the problem. Examine the log file to obtain additional information. <ol style="list-style-type: none"> <li>1. Verify that the host name or IP address specified for the DVR are correct and that communications with the device is working through the network.</li> <li>2. Verify that the password you specified for the DVR is correct.</li> </ol>
<b>Languages and Translations</b>	
The user interface does not present data in the correct language as specified by the operator locale.	This usually indicates that the language files were not installed. For the web browser interface the language files must be installed on the server. For the client user interface the language files must be installed on both the server and client workstation.
<b>Administration Guide</b>	
After selecting the Administration Guide link, the window displays a white background and the document does not display in the window.	This can happen the first time you try to view a PDF file. The Acrobat Reader program requires the user to accept the terms of the license the first time the application is used. Unfortunately, the window to accept the license is presented behind other windows and is hidden from view. Minimize the other windows until you see the license agreement window. Accept the license and click <b>OK</b> . The document then will display.

## Contacting technical support

For assistance installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided. If you still have questions, you may contact technical support during normal business hours (Monday through Friday, excluding holidays, between 8 a.m. and 8 p.m. Eastern Time).

GE Security

United States: 1-888-GE SECURITY (1-888-437-3287)

Asia: 852-2907-8108

Australia: 61-3-9259-4700

Europe: 48-58-326-22-40

Latin America: 503-885-5700



## Appendix C. Error Messages

This section identifies error messages that may be displayed by the Facility Commander user interface. Error messages are identified by their 5-digit error number and include an explanation of possible causes and suggested solutions.

An integral component of the user interface is a standard web browser. Errors that may be encountered in accessing the server, or constructing a response screen to display, use the standard web browser reporting mechanism. They are first in the table and do not have error numbers associated with them. In some cases it may be necessary to examine the product log files to determine the cause of the failure.

If you are reading this document online, click on one of the error messages in the list below to view the causes and actions.

**Table 147.** Error messages, numbers, and page number

Error #	Messages	Page #
	<a href="#">The page cannot be displayed</a>	<a href="#">page 414</a>
	<a href="#">Internal server error</a>	<a href="#">page 415</a>
00001	<a href="#">Exceeded licensed quantity: capacity is &lt;number&gt;, &lt;number&gt; in use, desired change is &lt;number&gt;.</a>	<a href="#">page 415</a>
00002	<a href="#">Cannot release license resource: capacity is &lt;number&gt;, &lt;number&gt; in use, desired change is &lt;number&gt;.</a>	<a href="#">page 415</a>
00003	<a href="#">Licensing exception. No details specified.</a>	<a href="#">page 415</a>
00004	<a href="#">License has expired.</a>	<a href="#">page 416</a>
00005	<a href="#">Subsystem &lt;name&gt; is not a licensed resource.</a>	<a href="#">page 416</a>
00006	<a href="#">Invalid parameter specified in license request: subsystem is &lt;name&gt;, quantity is &lt;number&gt;.</a>	<a href="#">page 416</a>
00007	<a href="#">No license for subsystem &lt;name&gt;.</a>	<a href="#">page 416</a>
00008	<a href="#">Invalid license code.</a>	<a href="#">page 416</a>
00009	<a href="#">Error creating video player. Cause: &lt;text&gt;.</a>	<a href="#">page 417</a>
00010	<a href="#">Video clip not found.</a>	<a href="#">page 417</a>
00011	<a href="#">Video source not available.</a>	<a href="#">page 417</a>
00012	<a href="#">Digital recorder not available. Cause: &lt;text&gt;.</a>	<a href="#">page 417</a>
00013	<a href="#">Connection failed. Cause: &lt;text&gt;.</a>	<a href="#">page 417</a>
00014	<a href="#">Recorder initialization failed.</a>	<a href="#">page 417</a>

**Table 147.** Error messages, numbers, and page number (Continued)

Error #	Messages	Page #
00015	Requested operation not supported.	page 417
00016	Duplicate tag name, please try another.	page 418
00017	Error performing database operation.	page 418
00018	Invalid value for parameter.	page 418
00019	Error accessing the database, please try again.	page 418
00020	Deletion of predefined data not permitted.	page 419
00021	Requested data not found. Data may have been deleted by another operator.	page 419
00022	Attempt to save data failed.	page 419
00023	Attempt to update data failed. Data may have been updated or deleted by another operator.	page 420
00024	Attempt to delete data failed. Data may have been updated or deleted by another operator.	page 420
00025	Database read failed, number of columns incorrect.	page 420
00026	Database read failed, column data not of correct type.	page 421
00027	Database connection error.	page 421
00028	No database configured.	page 421
00029	Input value to validator is not correct type.	page 421
00030	Incorrect number of criteria provided to validator.	page 421
00031	Criterion value is not correct type.	page 421
00032	Enter value for required field.	page 422
00033	Duplicate user name, please try another.	page 422
00034	Text entered must be at least <number> characters.	page 422
00035	Text entered exceeds <number> characters.	page 422
00036	Enter a number from <number> to <number>.	page 422
00037	Enter true or false.	page 422
00038	Enter a number.	page 422
00039	Enter a valid URL such as http:// www.someDomain.com.	page 422

**Table 147.** Error messages, numbers, and page number (Continued)

Error #	Messages	Page #
00040	Enter a valid host name such as server3@domain.com.	page 423
00041	Enter a valid IP address such as 10.20.30.40.	page 423
00042	Enter a valid host name or IP address such as server3@domain.com or 10.20.30.40.	page 423
00043	Value must be blank for this option.	page 423
00044	Value must be entered for this option.	page 423
00045	Minimum value must be less than maximum value.	page 423
00046	Camera linking or unlinking failed. Camera assigned to another DVR input or DVR deleted by another operator.	page 424
00047	Preset number in use, please try another.	page 424
00048	Everything is imported for the facilities enabled in the window filter.	page 424
00049	Errors occurred. Move mouse pointer over X for details.	page 425
00050	Screen definition error. Request could not be performed.	page 425
00051	Operation cancelled by the operator.	page 425
00052	Operation not permitted.	page 425
00053	Duplicate browser error.	page 425
00054	Login timed out, please log in again.	page 425
00055	Login failed, server not available.	page 426
00056	Login not supported from unknown terminal.	page 426
00057	Specified user name not valid.	page 426
00058	Context information not available for specified user name.	page 427
00059	All workstation licenses in use.	page 427
00060	Login failed, workstation not specified or not defined.	page 427
00061	Password and confirmation password must match.	page 427
00062	Invalid user name or password, please try again.	page 428

**Table 147.** Error messages, numbers, and page number (Continued)

Error #	Messages	Page #
00063	Number of items per page not valid.	page 428
00064	Page number not valid.	page 428
00065	Page request not valid.	page 428
00066	This client is currently offline, request cannot be executed.	page 428
00067	Attempt to update facility membership failed.	page 429
00068	The window filter contains no facilities.	page 429
00069	The update to the window filter failed.	page 429
00070	Only one instance of <name> can be started at a time.	page 430
00071	Port number <number> specified in the client.properties file is already in use.	page 430
00072	Error in recording clip, no video available.	page 430
00073	Alarm instructions currently unavailable.	page 430
00074	No hyperlink location defined.	page 431
00075	Error in saving display.	page 431
00076	Error in getting display from server.	page 431
00077	Error in getting symbol schemes from server.	page 431
00078	Error in getting palettes from server.	page 432
00079	Display not found in server.	page 432
00080	file name cannot contain any of the following characters: \:*?\"<>.	page 432
00081	Error in uploading display.	page 433
00082	Error in uploading symbol scheme.	page 433
00083	Uploading aborted! Files used in display not found.	page 433
00084	Error in removing resource.	page 434
00085	No domains found in system.	page 434
00086	Record delete failed due to dependency.	page 434
00087	Camera information not available. The camera may have been deleted by another operator.	page 435

**Table 147.** Error messages, numbers, and page number (Continued)

Error #	Messages	Page #
00088	Missing initial state icon.	page 435
00089	License key does not exist or is invalid.	page 435
00090	Selected DXF file name does not match the original name. Operation aborted!	page 436
00091	Error importing AutoCad DXF drawings. Operation aborted!	page 436
00092	Duplicate layer name {0} found. Operation aborted!	page 436
00093	AutoCad DXF layer name {0} cannot be renamed.	page 436
00094	Value is not within the range {0, number, integer} to {1, number, integer}.	page 436
00095	Enter a valid numeric range such as: 1-100 or 1-20;25;30-50.	page 436
00096	Range numbers must be in numeric sequence such as 1;5-50;60-70.	page 436
00097	Value must contain only numeric digits.	page 437
00098	Intercom extension or exchange number is already assigned to {0}.	page 437
00099	Camera and preset information has been refreshed on the Monitoring tab.	page 437
00100	Camera is not linked to a DVR.	page 437
00101	Intercom extension or exchange number length must not exceed {0, number, integer} digits.	page 437
00102	Selected alarms require response information.	page 437
00103	Alarm requires response information.	page 437
00104	Other field values are inconsistent with this value.	page 437
00105	Tag name may be in use or invalid. Please specify a different tag name.	page 438
00106	Switcher configuration file syntax error or model type incorrect.	page 438
00107	The input number is already in use for this area.	page 438
00108	The area number is already in use for this panel.	page 438
00109	Switcher configuration has already been imported.	page 439

**Table 147.** Error messages, numbers, and page number (Continued)

Error #	Messages	Page #
00110	Items cannot be imported. Name already exists.	page 439
00111	The bus address is already in use for this DVR. Please select another.	page 440
00112	Client version (<client-version>) not compatible with server version (<server-version>).	page 440

**Table 148.** List of error numbers, messages, causes, and actions

#	Message	Causes	Actions
	The page cannot be displayed	<p>This message and the associated detailed information indicate that communications with the server were not successful or the operation timed out.</p> <p>Unsuccessful communications may be due to the server being down, a network communications problem or that the URL address for the server is not correct. Successful communication between the workstation and server requires the use of static IP addresses or an accessible DNS (domain name server) to perform the translation of host name to IP address.</p> <p>For Unix systems the <i>/etc/hosts</i> table may be used to provide the translation.</p>	<p>If this error occurred when attempting to log in, contact the System Administrator to ensure that the server is up, that communications from your workstation to the server are functioning properly, and that the URL address for the server is correct.</p> <p>Retry the login operation. If the error occurred while already logged in, click the <b>Back</b> button on the browser to return to the last valid screen and try another operation. If the problem persists, contact the System Administrator for assistance. The system log file should be examined for evidence of network failures or a software problem. If necessary, contact Customer Support for assistance.</p>

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
	Internal server error	This message indicates a software problem has occurred or that the request made through the web browser interface is not synchronized with the current state of the operator's session. The latter problem can occur if the operator attempts to bypass the normal operations of the user interface or may indicate an attempted security breach.	Click the <b>Back</b> button on the browser to return to the last valid screen and try another operation. If the problem persists, contact the System Administrator for assistance. The system log file should be examined for evidence of an attempted security breach, operator bypassing of normal operations of the user interface or a software problem. If necessary contact Customer Support for assistance.
00001	Exceeded licensed quantity: capacity is <number>, <number> in use, desired change is <number>.	The operation requested by the operator required a license resource that was not available at the current time. The license resource required, how many license units are currently in use and how many license units were requested are shown in the message.	Reduce the number of active operator windows using the resource or increase the license capacity of the system.
00002	Cannot release license resource: capacity is <number>, <number> in use, desired change is <number>.	The operation requested by the operator attempted to release license resources not held by the operator's session. This could indicate a software problem or an attempted security breach.	The requested operation by the operator to release the license resources not held by the operator's session. This could indicate a software problem or an attempted security breach.
00003	Licensing exception. No details specified.	Indicates a software problem or an attempted security breach.	Examine the system log file to determine if any unauthorized network activity is present. If there is evidence of a software problem send the error message and corresponding information from the log file to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00004</b>	License has expired.	<p>The operator's session was expired due to inactivity and the license required for the requested operation was released.</p> <p>The session timeout period is a system parameter with a default of 30 minutes but is changeable by the System Administrator.</p>	The operator must log in again.
<b>00005</b>	Subsystem <name> is not a licensed resource.	Indicates a software problem or an attempted security breach.	Examine the system log file to determine if any unauthorized network activity is present. If there is evidence of a software problem send the error message and corresponding information from the log file to Customer Support for assistance.
<b>00006</b>	Invalid parameter specified in license request: subsystem is <name>, quantity is <number>.	Indicates a software problem or an attempted security breach.	Examine the system log file to determine if any unauthorized network activity is present. If there is evidence of a software problem send the error message and corresponding information from the log file to Customer Support for assistance.
<b>00007</b>	No license for subsystem <name>.	Indicates a software problem or an attempted security breach.	Examine the system log file to determine if any unauthorized network activity is present. If there is evidence of a software problem send the error message and corresponding information from the log file to Customer Support for assistance.
<b>00008</b>	Invalid license code.	Indicates a software problem or an attempted security breach.	Examine the system log file to determine if any unauthorized network activity is present. If there is evidence of a software problem send the error message and corresponding information from the log file to Customer Support for assistance.



**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00009</b>	Error creating video player. Cause: <text>.	The DVR could not be connected to. Also the video player data source classes for the specified protocol are not available.	Check that the DVR is turned on and recording. Verify on the DVR configuration screen that the correct model was selected. Also make sure that no other applications are connected to the DVR. Verify that the drivers for the requested protocol are installed on the client.
<b>00010</b>	Video clip not found.	The video token stored in the database was not found on the DVR. It's possible the video token was erased from the DVR or writing the token to the DVR failed.	If the video token was just written to the DVR it might not be available for playback yet, so retry playing the clip. Make sure the DVR is recording.
<b>00011</b>	Video source not available.	The camera was configured but not physically installed on DVR. Also see error message 00009.	Verify the camera configuration on the DVR.
<b>00012</b>	Digital recorder not available. Cause: <text>.	The DVR connection was not available.	The connection to the DVR was lost. Verify if the connection was lost. The System Administrator should determine if the DVR could be accessed across the network. Contact the network administrator for assistance.
<b>00013</b>	Connection failed. Cause: <text>.	A connection to the DVR could not be established.	Verify that the DVR configuration is correct. Also check that no other applications are connected to the DVR.
<b>00014</b>	Recorder initialization failed.	A connection to the DVR could not be established.	Verify that the DVR configuration is correct. Also check that no other applications are connected to the DVR.
<b>00015</b>	Requested operation not supported.	The software was requested to perform an operation that is not permitted. This message can be the result of an attempted security breach or a software problem.	Examine the system log file for evidence of an attempted security breach or a software problem and send the information to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00016</b>	Duplicate tag name, please try another.	The tag name specified by the operator is already in use for another item defined on the system. This error can also occur if a manual (command line) deletion of an item is made from a database table (strongly discouraged) but the corresponding entry in the tag_name table was not deleted.	The operator should specify a different tag name. When a manual deletion was performed, the system administrator should be contacted to delete the entry in the tag_name table.
<b>00017</b>	Error performing database operation.	The database operation requested by the operator failed, possibly due to a network problem that made the database inaccessible or a software problem.	The operator should try the operation again. If the problem persists, examine the log file for evidence of a network or a software problem and send the relevant information to Customer Support for assistance.
<b>00018</b>	Invalid value for parameter.	The database operation requested by the operator failed, possibly due to an inconsistency in the database or a software problem.	The operator should try the operation again. If the problem persists, examine the log file for evidence of a database inconsistency or a software problem and send the relevant information to Customer Support for assistance.
<b>00019</b>	Error accessing the database, please try again.	The database operation requested by the operator failed, most likely due to a network problem that made the database inaccessible or a software problem.	The operator should try the operation again. If the problem persists, examine the log file for evidence of a network or a software problem and send the relevant information to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00020</b>	Deletion of predefined data not permitted.	The operator attempted to delete an item from the database that cannot be deleted. The Facility Commander user interfaces prevent such deletion attempts so this error message may indicate an attempted security breach, an attempt to bypass normal operations of the user interface or a software problem.	The operator should not attempt to delete data where the delete icon has been disabled. If this message continues to occur, examine the log file for evidence of an attempted security breach or a software problem and send the relevant information to Customer Support for assistance.
<b>00021</b>	Requested data not found. Data may have been deleted by another operator.	The requested read operation failed, most likely due to a situation where another operator deleted an item that was required for the requested operation. This problem can occur when multiple operators with configuration delete permission are altering the system configuration in an uncoordinated manner. An example of this is where one operator is linking a camera to a DVR device while another operator is deleting the same camera.	Revisit the current screen to verify that the requested operation is still available. If on a list screen, use the appropriate entry in the navigation menu to refresh the list screen. You may observe that the record you were attempting to delete is no longer present. If on the DVR Link Camera screen, click on the Digital Video Recorders menu item, then click on the Link Cameras link of the specific DVR. You may observe that the camera you were attempting to link is no longer available. If this message continues to occur, examine the log file for evidence of uncoordinated changes to the system configuration or a software problem and send the relevant information to Customer Support for assistance.
<b>00022</b>	Attempt to save data failed.	The database save operation requested by the operator failed, possibly due to a network problem that made the database inaccessible, an inconsistency in the database or a software problem.	The operator should try the operation again. If the problem persists, examine the log file for evidence of a network problem, database inconsistency, or a software problem and send the relevant information to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00023</b>	Attempt to update data failed. Data may have been updated or deleted by another operator.	The requested updated operation failed, most likely due to a situation where another operator updated or deleted the same record. This problem can occur if two operators attempt to update the same item at the same time. The first update attempt will succeed and the second will fail with this error message. This error can also indicate a database inconsistency or a software problem.	<p>Revisit the current screen to verify that the requested operation is still available after noting the changes that you had intended to make. If on a list screen, use the appropriate entry in the navigation menu to refresh the list screen. You may observe that the item you were attempting to edit is no longer present.</p> <p>If on an edit screen, click the <b>Cancel</b> button to return to the list screen.</p> <p>If the item is still present, you can select its tag name or description to re-edit it. You may observe another operator changed one or more of the values. Some of your intended changes may no longer be relevant.</p> <p>If the problem persists, examine the log file for evidence of a database inconsistency or a software problem and send the relevant information to Customer Support for assistance.</p>
<b>00024</b>	Attempt to delete data failed. Data may have been updated or deleted by another operator.	<p>The requested updated operation failed, most likely due to a situation where another operator deleted the same record.</p> <p>This problem can occur if two operators attempt to delete the same item at the same time. The first delete attempt will succeed and the second will fail with this error message. This error can also indicate a database inconsistency or a software problem.</p>	<p>Revisit the current list screen by clicking on the appropriate entry in the navigation menu to determine if the item you were attempting to delete still exists. If so, repeat the delete operation. If the problem persists, examine the log file for evidence of a database inconsistency or a software problem and send the relevant information to Customer Support for assistance.</p>
<b>00025</b>	Database read failed, number of columns incorrect.	Indicates an inconsistency between a database table and the software, possibly due to a database corruption or software problem.	Provide this error message and the relevant information from the system log file to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00026</b>	Database read failed, column data not of correct type.	Indicates an inconsistency between a database table and the software, possibly due to a database corruption or software problem.	Provide this error message and the relevant information from the system log file to Customer Support for assistance.
<b>00027</b>	Database connection error.	The Facility Commander server could not connect to the database specified by the DatabaseServer element in the SystemConfig.xml file. The database name or URL address may be invalid or the database host may not be accessible through the network. The host containing the database may be down, disconnected from the network or the name server may not be providing translation of the host name to a valid IP address. For Unix systems verify that entries in the <code>/etc/hosts</code> file are correct.	The System Administrator should verify that the database URL is correct and the specified location is accessible through the network. Contact the local network Administrator for assistance.
<b>00028</b>	No database configured.	The systemConfig.xml file that defines the database location could not be found or did not have the correct format.	The System Administrator should verify the location and content of the file and correct as required and restore it from a backup if needed.
<b>00029</b>	Input value to validator is not correct type.	Indicates a software problem.	Provide this error message and the relevant information from the system log file to Customer Support for assistance.
<b>00030</b>	Incorrect number of criteria provided to validator.	Indicates a software problem.	Provide this error message and the relevant information from the system log file to Customer Support for assistance.
<b>00031</b>	Criterion value is not correct type.	Indicates a software problem.	Provide this error message and the relevant information from the system log file to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00032</b>	Enter value for required field.	When configuring a new or existing item the operator did not provide a value for a field where a value was required. This error message can also occur where a value of one field is dependent upon the value of another field.	The operator should specify a value for the field.
<b>00033</b>	Duplicate user name, please try another.	When in the process of creating a new or updating an existing operator record, a user name that is already in use by another operator record was entered.	The operator should enter a different user name.
<b>00034</b>	Text entered must be at least <number> characters.	The operator entered a value for the field that was too short in length (had too few characters). The minimum length required is provided in the error message.	Enter a value that has sufficient length.
<b>00035</b>	Text entered exceeds <number> characters.	The operator entered a value for the field that was too long in length (had too many characters). The maximum length permitted is provided in the error message.	Enter a value that does not exceed the maximum length.
<b>00036</b>	Enter a number from <number> to <number>.	The operator entered a value for a numeric quantity that was not valid. The error message specifies the range of valid values.	Enter a value within the specified range of valid values.
<b>00037</b>	Enter true or false.	The operator did not enter a value of true or false where one was required.	Enter the true or false.
<b>00038</b>	Enter a number.	The operator entered a non-numeric value where a numeric value was required.	Enter a numeric value.
<b>00039</b>	Enter a valid URL such as http://www.someDomain.com.	The operator did not enter a valid URL (Uniform Resource Locator) address. A URL is a full path specification to an object on the network.	Enter a valid URL address. Contact the System Administrator for assistance in specifying an appropriate value.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00040</b>	Enter a valid host name such as server3@domain.com.	The operator did not enter a valid host name for a device on the network.	Enter a valid host name. The host name is case-sensitive. Contact the System Administrator for assistance in specifying an appropriate value.
<b>00041</b>	Enter a valid IP address such as 10.20.30.40.	The operator did not enter a valid IP (Internet Protocol) address for a device on the network.	Enter a valid IP address. Contact the System Administrator for assistance in specifying an appropriate value.
<b>00042</b>	Enter a valid host name or IP address such as server3@domain.com or 10.20.30.40.	The operator did not enter a valid host name or IP (Internet Protocol) address for a device on the network.	Enter a valid host name or IP address. The host name is case-sensitive. Contact the System Administrator for assistance in specifying an appropriate value.
<b>00043</b>	Value must be blank for this option.	The operator specified a value for a field that must be blank (empty) based on the value specified for another field. Both fields are flagged with an error indicator and this error message.	Set the value for the field to blank or change the value of the other field.
<b>00044</b>	Value must be entered for this option.	The operator did not specify a value for a field where one was required, based on the value specified for another field. Both fields are flagged with an error indicator and this error message.	Enter a value for the field or change the value of the other field.
<b>00045</b>	Minimum value must be less than maximum value.	Indicates one or more incorrect entries in the configuration files that specify minimum and maximum values for data entered by the operator.	The minimum value specified for a field must be less than or equal to the maximum value specified. Examine the entries in the configuration files fieldValidations.xml and eventActionCommandValidations.xml and contact Customer Support for assistance if necessary. Customers and business partners should not alter these files without specific instructions from Customer Support.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00046</b>	Camera linking or unlinking failed. Camera assigned to another DVR input or DVR deleted by another operator.	The system was unable to link the specified camera to the specified DVR. The most likely causes are that the camera was linked to another DVR, another operator deleted the DVR, multiple operators with configuration delete permission are making system configuration changes in an uncoordinated manner or the database has inconsistent data.	Click on the Digital Video Recorders menu item and observe if the DVR you are trying to link cameras to still exists. If it does, click on the Link Cameras link for the DVR and determine if the camera you were attempting to link is still available. If it is, retry the attempt to link the camera to the DVR. If this message continues to occur, examine the log file for evidence of uncoordinated changes to the system configuration, inconsistent data in the database or a software problem and send the relevant information to Customer Support for assistance.
<b>00047</b>	Preset number in use, please try another.	When configuring a new or updating an existing preset for a camera, the operator specified a preset number that is already in use by another preset defined for the camera.	Specify a preset number not in use for the camera. If necessary, click on the Cancel button to return you to the list screen where the currently defined preset numbers for the camera are shown.
<b>00048</b>	Everything is imported for the facilities enabled in the window filter.	No data was available for import when the operator clicked the Import button. The cause of the unavailability, if known, is displayed in the error message line. The most likely causes and actions to take are listed below.	<ol style="list-style-type: none"> <li>1. All data was imported already - no further action is required.</li> <li>2. Window filter had disabled facilities - enable the other facilities and retry the import operation.</li> <li>3. Communications (network) error - retry the import operation.</li> <li>4. License expired - log in again and retry the import operation.</li> </ol>



**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00049</b>	Errors occurred. Move mouse pointer over X for details.	There were two or more values entered by the operator that were not valid. This message is displayed in the error message line. The specific error messages are shown for each field in error.	Correct each error and retry the operation.
<b>00050</b>	Screen definition error. Request could not be performed.	The configuration file specifying the screen contents was not in the correct format.	Restore the listScreens.xml and editScreens.xml screen definition files from a backup. Customers and business partners should not alter these files without specific instructions from Customer Support.
<b>00051</b>	Operation cancelled by the operator.	The operator clicked the Cancel button to abort the edit operation.	None required. This is a routine message acknowledging the request.
<b>00052</b>	Operation not permitted.	An operation was attempted for which the operator does not have permission. The Facility Commander user interfaces do not offer operations that are not permitted. This message can occur if an operator attempts to circumvent normal operation of the user interfaces, or from an attempted security breach or from a software problem.	Examine the system log for evidence of operator attempts to circumvent normal operation of the user interfaces, an attempted security breach or a software problem and send the relevant information to Customer Support for assistance.
<b>00053</b>	Duplicate browser error.	The operator opened a second browser window using the New Window entry of the File menu. Secondary browser windows from the same log in are not supported.	Close the second browser window. To perform operations through two browser windows, launch a new instance of the browser and log in to establish an independent session. Note that this will use another web client license.
<b>00054</b>	Login timed out, please log in again.	The operator's session was expired due to inactivity and the client license was released. The session timeout period is a system parameter with a default of 30 minutes, which is changeable by the System Administrator.	The operator must log in again.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00055</b>	Login failed, server not available.	The client software could not communicate with the Facility Commander server. The server may be down or a network problem may be preventing communication. The name server used by the client workstation may not be providing translation of the server host name to a valid IP address. For Unix systems verify that entries in the <code>/etc/hosts</code> file are correct. Also, the operator may be attempting to log into a Facility Commander 2.0 server using a client application that is an earlier version.	The System Administrator should verify that the server host name specified by the <code>hostURL</code> parameter in the <code>client.properties</code> file specifies the correct server host name. Verify the server is up and the server host is accessible through the network. Also, use the client log file to view the details of the error message. Contact the local network administrator for assistance.
<b>00056</b>	Login not supported from unknown terminal.	The operator attempted to log in from a non-workstation device. The system could not determine that the log in was attempted from a web browser or from the client Workspace application. This message could indicate that an operator is attempting log in from a non-qualified device or that a security breach is being attempted.	Attempt to contact the operator to verify that the device being logged in from is qualified for use. Examine the system log file to determine if log in attempts are being made from unauthorized sources indicating that a security breach is being attempted. If necessary, contact Customer Support for assistance.
<b>00057</b>	Specified user name not valid.	The user name entered by the operator has not been defined on the server. The operator may have mistyped the user name or a security breach may have been attempted.	Re-enter the user name and try to log in. Examine the system log file to determine if log in attempts are being made from unauthorized sources indicating that a security breach is being attempted. If necessary, contact Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00058</b>	Context information not available for specified user name.	Indicates a database inconsistency or a software problem. An operator record was located for the operator that is attempting to log in, but the context specified in the operator record could not be located in the database.	Verify the presence of the context record in the database that is specified in the operator record. Try to recreate the context if it is missing. Examine the system log for evidence of database consistency error messages. If the problem persists send the relevant information to Customer Support for assistance.
<b>00059</b>	All workstation licenses in use.	All concurrent log-ins permitted by the license are in use.	Wait a few minutes and try to log in again. Idle log-ins will be terminated after their idle expiration period, freeing their licenses. Reduce the number of concurrent log-ins by asking operators to log off of workstations that they are not actively using. Increase concurrent login licenses.
<b>00060</b>	Login failed, workstation not specified or not defined.	The operator attempted to run the Java client user interface from a workstation that was not defined to the Facility Commander server. Workstations that may be used to run the Java client user interface must be defined on the Facility Commander server. The host name of the workstation where the Java client user interface was trying to log in from does not match the host name for any workstation defined on the Facility Commander server.	Notify the operator of which workstations may be used to run the Java client user interface software or define the workstation on the Facility Commander server. If dynamic IP addressing is being used on the network, the System Administrator should verify that the DNS (domain name server) is correctly translating the workstation host name. For Unix systems verify the host name translation entry in the <code>/etc/hosts</code> file.
<b>00061</b>	Password and confirmation password must match.	When configuring a new or updating an existing item, the value entered for the password confirmation did not match the value entered for the password. These values must match to ensure that the password entered is what the operator intended.	Re-enter the value for the password confirmation and click on the Submit button to save the changes.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00062</b>	Invalid user name or password, please try again.	The specified user name and password did not match the information for any operators defined on the server.	Re-enter the user name or password in case you had mistyped the previous information and try to log in again. If the problem persists contact the System Administrator for assistance.
<b>00063</b>	Number of items per page not valid.	The number of items specified to be shown on list screens was not a valid value. The Facility Commander user interfaces limit the values that may be selected to a range of valid values. This error may indicate an attempt to bypass the normal user interface mechanisms, could be indicative of an attempted security breach or a software problem.	The operator should select the number of items per page from the select list provided on the list screen. If the problem persists, the System Administrator should examine the system log file for evidence of an attempted security breach or software problem and send the relevant information to Customer Support for assistance.
<b>00064</b>	Page number not valid.	The value entered in the box to the left of the Go button was not a number.	The operator should enter a valid numeric value within the range of the page numbers shown on the screen. If the problem persists, contact Customer Support for assistance.
<b>00065</b>	Page request not valid.	The value entered in the box to the left of the Go button was not within range of the available page numbers as shown on the screen.	The operator should enter a valid numeric value within the range of the page numbers shown on the screen. If the problem persists, contact Customer Support for assistance.
<b>00066</b>	This client is currently offline, request cannot be executed.	The Facility Commander client software cannot currently communicate with the server. The operator tried to perform an action that requires communication with the server. This can be caused either by the server being down, or due to a lost connection with the client PC.	If the color of the connection indicator in the lower right corner of the client application is red, this indicates a communication problem. First verify with the System Administrator that the server is up and running. If it is, then the problem may be with the client PC's network connection, or due to an incorrect hostURL entry in the client.properties file.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00067</b>	Attempt to update facility membership failed.	The operator request to change the membership of a facility was not totally successful most likely due to a problem accessing the database or an inconsistency between database tables. Some of the requested changes may have been made but at least one change failed. The screen will be refreshed to show the current membership of the facility. The operator should examine the information to determine what changes did not occur.	Attempt to make the membership changes that previously failed. If the problem persists, contact the System Administrator to examine the system log file for evidence of database inconsistency or a software problem and send the relevant information to Customer Support for assistance.
<b>00068</b>	The window filter contains no facilities.	This message indicates that the context assigned to the operator does not include any facilities. This message will be displayed if an operator assigned a context without facilities views the window filter by clicking on the Window Filter entry of the navigation menu.	No action is required unless the operator believes that the context should contain access to one or more facilities. In this case the System Administrator should be contacted to verify the context assigned to the operator. If the context does include facilities then there may be a software problem or a database inconsistency. Examine the system log file for evidence of these problems and send the relevant information to Customer Support for assistance.
<b>00069</b>	The update to the window filter failed.	This message indicates that the operator request to change the facilities that are enabled in the window filter was not successful. This error message should not occur and is indicative of a software problem.	Examine the system log file for evidence of a software problem and send the relevant information to Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00070</b>	Only one instance of <name> can be started at a time.	The operator tried to launch the Facility Commander client, but it is already running. This can also occur if the previous instance of the Facility Commander client aborted unexpectedly, leaving the network communication port allocated. A third possible cause is that another program running on the workstation is using the port number configured for the Facility Commander client.	Determine if an instance of the Facility Commander client is already running (check the Windows task bar to see if it is minimized) on the workstation. If the previous instance of client aborted unexpectedly, reboot the workstation to free up the port. If the problem persists, contact the System Administrator to change the value of the workspace.port_number parameter in the client.properties file to a port that is not in use by another program running on the workstation.
<b>00071</b>	Port number <number> specified in the client.properties file is already in use.	This message always appears together with message 00070 if the Facility Commander client can determine that the network port number is being used by another program.	Contact the System Administrator to change the value of the workspace.port_number parameter in the client.properties file to a port that is not in use another program running on the workstation.
<b>00072</b>	Error in recording clip, no video available.	The DVR was not in record mode or the connection was lost.	Verify that the DVR is recording and that a valid connection exists.
<b>00073</b>	Alarm instructions currently unavailable.	This message appears on the Alarm Response dialog in the Instructions field if the External Access Control System that is the source of the alarm (e.g. Picture Perfect) is currently offline.	Verify that the alarm has an Offline indicator displayed (a red "X"). This indicates that the external system that is the source for this alarm is currently offline. When the external system comes back online (when the red X is no longer displayed), bringing up the Alarm Response window again to display the alarm instructions.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00074</b>	No hyperlink location defined.	This message may occur with the Graphic Viewer when a hyperlink symbol was added to the graphic display but was not linked to another graphic.	Notify the System Administrator that the graphic display contains a link that was not set. The System Administrator should run the Graphic Editor to set the hyperlink to an existing graphic display or should delete the hyperlink symbol.
<b>00075</b>	Error in saving display.	The file name may contain invalid characters.	Examine the client log file to determine which file names were invalid. Correct the file names and retry the save operation.
<b>00076</b>	Error in getting display from server.	The attempt to retrieve the specified graphic display file from the Facility Commander server failed. The server may be down or there may be network communication problems.	Contact the System Administrator to determine if the server is down or there are network communication problems. Retry the operation when the server is up and network communications have been restored. If the problem persists the System Administrator should examine the server log file and if necessary, contact Customer Support for assistance.
<b>00077</b>	Error in getting symbol schemes from server.	The attempt to retrieve the symbol files associated with the specified graphic display from the Facility Commander server failed. The server may be down or there may be network communication problems.	Contact the System Administrator to determine if the server is down or there are network communication problems. Retry the operation when the server is up and network communications have been restored. If the problem persists the System Administrator should examine the server log file and if necessary, contact Customer Support for assistance.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00078</b>	Error in getting palettes from server.	The attempt to retrieve the symbol palette files associated with the specified graphic display from the Facility Commander server failed. The server may be down or there may be network communication problems.	Contact the System Administrator to determine if the server is down or there are network communication problems. Retry the operation when the server is up and network communications have been restored. If the problem persists the System Administrator should examine the server log file and if necessary, contact Customer Support for assistance.
<b>00079</b>	Display not found in server.	The attempt to retrieve the specified graphic display file from the Facility Commander server failed. This problem usually occurs when an operator logs in and the restored workspace preferences specify a graphic display that no longer exists on the Facility Commander server.	Contact the System Administrator to determine if the graphic display was deleted from the server. If it was, resave the workspace to remove the reference or ask the System Administrator to restore the graphic display on the server. If not, log out and log in again to see if the problem persists. If the problem reoccurs, the System Administrator should examine the server log file to seek other causes such as network communications problems.
<b>00080</b>	file name cannot contain any of the following characters: \ : * ? " < > .	When saving a graphic display the operator entered one or more characters (of \ : * ? " < > .) that are invalid for file names.	Attempt the save operation again after entering a name that does not contain any of the invalid characters.



**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
00081	Error in uploading display.	This error can occur from many different causes as listed in the actions below. Examine the client or server log files as appropriate to determine the cause of the failure.	<p>Retry the operation to see if the problem persists.</p> <ol style="list-style-type: none"> <li>1. Files referenced by the graphic display are missing on the client. This can occur especially if graphics files such as images were referenced across a network and they are not accessible when the save operation is in progress. Files may also have been deleted manually from the workstation after the graphic display was created but before it was uploaded.</li> </ol> <p>- Examine the client log file to determine which files were missing or inaccessible and correct as appropriate.</p> <ol style="list-style-type: none"> <li>2. Network communications error, Facility Commander server error, database error - Examine the system log file to determine which of these problems is the cause of the failure and correct as appropriate.</li> </ol>
00082	Error in uploading symbol scheme.	This message indicates that network communications problem occurred when uploading a symbol file referenced by a graphic display that is being uploaded to the server.	Retry the operation. If the problem persists contact the System Administrator to examine the client and server log files to determine the problem.
00083	Uploading aborted! Files used in display not found.	Images or symbol files that are referenced by the graphic display were not found. This can occur if these files were referenced across the network and are not accessible at the current time or if referenced files on the workstation were manually deleted after the graphic display was created.	Examine the client log file to determine which files are missing or are not accessible. Restore the missing files and retry the operation.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00084</b>	Error in removing resource.	This error can occur during a request to delete a symbol, image or graphic display from the server if the specified file cannot be deleted. The file may have been deleted by another operator, may have been manually set to read-only, or may be locked because it is in use by another program.	Determine if the file still exists on the server. If so, retry the operation. If the problem persists contact the System Administrator to determine why the file cannot be deleted.
<b>00085</b>	No domains found in system.	This message is displayed when in attempting to associate an item to a symbol on a graphic display, no items of the appropriate type are found using the current window filter. The window filter may specify a restricted set of facilities that do not contain any items of the appropriate type or no items of that type may exist in the database.	Examine the window filter and enable additional facilities to locate items of the appropriate type and retry the association operation. If the operator believes that items of the appropriate type do exist but are not being shown, it may indicate a database inconsistency or software problem. In this case the System Administrator should examine the server log file to determine the cause.
<b>00086</b>	Record delete failed due to dependency.	The operator request to delete an item could not be performed because other items are referencing the item to be deleted. The tag names of the referencing items are displayed when the mouse is placed over the X.	The operator must remove these references before the original item can be deleted.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
00087	Camera information not available. The camera may have been deleted by another operator.	This message may occur when linking cameras to a DVR device through the Link Cameras screen. It will also occur if the same camera is linked to more than one input of the DVR. The screen will be redisplayed and the camera inputs where the link failed will be flagged with an X. The reason for the link failure is shown when the mouse is placed over the X.	Examine the list of available cameras and observe if the camera you tried to link is still available. The camera may have been deleted from the system or may have been assigned to another DVR device. If the camera is still available try the link operation again. If the problem persists it may indicate a database inconsistency or a software problem. Examine the system log file for evidence of a software problem and send the relevant information to Customer Support for assistance.
00088	Missing initial state icon.	The symbol file that the operator requested to upload to the server references an image file to display for the initial state of an item that could not be found. The image file for the initial state of an item is a required component of a symbol. This can occur if the image file was referenced across the network and is not accessible at the current time or if the image file was located on the workstation but was manually deleted after the symbol was created.	Restore the missing image file and retry the operation. If the problem persists contact the System Administrator to examine the client and server log files to determine the problem.
00089	License key does not exist or is invalid.	The license key file license.xml is not present in the correct location or was generated using a machine code from a different computer.	Verify that the license.xml file is present in the correct location (the installation path plus <code>/server/resources</code> ). Verify that the license key was generated using the correct machine code for the computer where the server software was installed. You should call Customer Support, provide the server machine code, and have them verify that the license code is correct.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00090</b>	Selected DXF file name does not match the original name. Operation aborted!	Selected re-imported DXF file does not match the original DXF file name.	Select the same DXF file name to re-import.
<b>00091</b>	Error importing AutoCad DXF drawings. Operation aborted!	The DXF file may not be saved in version 12 format, or the DXF file is corrupted or not in DXF format.	Make sure the DXF file is in DXF file format with version 12.
<b>00092</b>	Duplicate layer name {0} found. Operation aborted!	Duplicate layer name is found when merging DXF layers.	Change the duplicate layer name from the layer setting dialog and re-import again. If that layer name is a DXF layer, you need to change the original layer name in AutoCad and delete the object to re-import it again.
<b>00093</b>	AutoCad DXF layer name {0} cannot be renamed.	DXF layer name cannot be changed for later updating and merging purpose.	You have to rename the layer in the AutoCad and re-import in again in order to change the layer name.
<b>00094</b>	Value is not within the range {0, number, integer} to {1, number, integer}.	The operator entered a value that was not within the specified range of numbers.	Enter a number within the specified range.
<b>00095</b>	Enter a valid numeric range such as: 1-100 or 1-20;25;30-50.	The operator entered an invalid numeric range specification.	<p>The range specification entered by the operator may not be valid for a number of reasons. The information entered must follow these rules:</p> <ul style="list-style-type: none"> <li>• No spaces are allowed when entering a range of numbers.</li> <li>• Semicolons (;) must be used to separate number range specifications.</li> <li>• The number range specifications must be in increasing numerical order.</li> </ul>
<b>00096</b>	Range numbers must be in numeric sequence such as 1;5-50;60-70.	The numeric range entered by the operator was not in an increasing numeric sequence.	Each number or range must be greater than the previous number or range. The entire sequence of numbers and ranges must be in increasing numerical order.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00097</b>	Value must contain only numeric digits.	The operator entered a sequence of characters that contained digits other than 0 through 9.	Enter characters that consist only of the digits 0 through 9.
<b>00098</b>	Intercom extension or exchange number is already assigned to {0}.	The intercom extension or exchange number entered by the operator is already assigned to another intercom station or exchange.	Specify a different extension or exchange number. The extension and exchange number must be unique for an intercom exchange and all of the stations connected to it. Note that the intercom stations connected to different exchanges can have the same extension number.
<b>00099</b>	Camera and preset information has been refreshed on the Monitoring tab.	This informational message alerts the operator that Facility Commander has changed camera and preset information on the Monitoring tab of the Configure Intercom Station page.	Return to the Monitoring tab to specify a preset for the camera before submitting the record.
<b>00100</b>	Camera is not linked to a DVR.	The operator selected a camera in the Video Console navigation pane that is not linked to a DVR in the database.	Using the browser client, go to the DVR list page and click Link Cameras. Link the camera to the proper input on that page.
<b>00101</b>	Intercom extension or exchange number length must not exceed {0, number, integer} digits.	The operator entered an intercom extension or exchange number that was too large.	Enter a value whose length does not exceed the specified value.
<b>00102</b>	Selected alarms require response information.	One of the selected alarms requires response text before it can be removed.	Enter the response text into the response text window.
<b>00103</b>	Alarm requires response information.	The alarm requires response text before it can be removed.	Enter the response text into the response text window.
<b>00104</b>	Other field values are inconsistent with this value.	The operator entered values for other fields that are inconsistent with the value for this field. The other fields will be flagged with their own error indicators and those error messages will indicate the type of inconsistency.	Review all the fields marked with an error indicator and determine a consistent set of values for those fields. After making the changes, click the <b>Submit</b> button to save the data.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
<b>00105</b>	Tag name may be in use or invalid. Please specify a different tag name.	The tag name entered for the graphic display is not valid. The tag name may be in use by another item or may be too long.	Enter a different tag name and click <b>Upload</b> to save the graphic display. Tag names must be at least two characters.
<b>00106</b>	Switcher configuration file syntax error or model type incorrect.	An error occurred when attempting to read the information in the specified analog switcher configuration file. The syntax of the file may be incorrect or the model specified in the file may not be the same model of the switcher record you are attempting to import the data for.	Verify that the model of the switcher record you are attempting to import the data for matches the model in the file. Verify the syntax of the file.
<b>00107</b>	The input number is already in use for this area.	The operator entered an input number on the intrusion input configuration screen that has already been used by another intrusion input assigned to the same intrusion area.	Choose a different input number not already in use by existing intrusion inputs for the specified intrusion area.
<b>00108</b>	The area number is already in use for this panel.	The operator entered an area number on the intrusion configuration screen that has already been used by another intrusion area assigned to the same intrusion panel.	Choose a different area number not already in use by existing intrusion areas for the specified intrusion panel.

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
00109	Switcher configuration has already been imported.	<p>This message can occur when you attempt to import an analog switcher configuration file.</p> <p>The operator already imported this switcher configuration with the option to automatically create cameras and monitors and is now attempting to perform this operation a second time for the same analog switcher. The created cameras and monitors have their tag names constructed based on the tag name of the analog switcher.</p> <p>If these items have already been created, trying to create them a second time is not permitted because duplicate tag names are not allowed.</p> <p>If the operator deletes that analog switcher with exactly the same tag name as the one that was deleted and attempts to import a configuration file, the same situation occurs and the cameras and monitors cannot be created because they already exist.</p>	<p>The operator can manually select the appropriate cameras and monitors on the analog switcher inputs and outputs page because they already exist.</p> <p>The operator can delete the cameras and monitors and retry the import operation.</p>
00110	Items cannot be imported. Name already exists.	<p>When importing items such as facilities from an external access control system, one or more of those facilities had a description that matches an existing item in Facility Commander.</p> <p>The description of an imported item becomes the tag name of the corresponding Facility Commander item.</p> <p>Facility Commander items have a unique tag name (not case-sensitive). All name conflicts will be shown on the import page.</p>	<p>The operator can continue with the import operation to import the items that do not have a name conflict. Change the description of the item on the external access control system so that it does not conflict with an existing item on the Facility Commander system and perform the import operation again.</p>

**Table 148.** List of error numbers, messages, causes, and actions (Continued)

#	Message	Causes	Actions
00111	The bus address is already in use for this DVR. Please select another.	On the camera configuration page, the operator specified a bus address for a PTZ camera that is already in use by another PTZ camera on the specified PTZ controller.	Select a different bus address for the PTZ camera.
00112	Client version (<client-version>) not compatible with server version (<server-version>).	The operator is running a Facility Commander client application that is not at the same version level as the server. This can happen if a version 1.x client is used with a version 2.x server or vice versa.	The Facility Commander client application must be at the same version level as the server. Either log into a different server that is at the same version level or upgrade the client to a later version.



## Appendix D. Facility Permissions

Use facility permissions to grant or deny permissions to monitor and control items, such as locking and unlocking door access points or control PTZ cameras, view live or recorded video, acknowledge alarms and more.

There are two types of permissions granted — enabled or not enabled, and none, view, update, create, and delete permissions.

- The ability to lock and unlock and access points is either enabled or not enabled.
- The second type grants permission based on which category is selected. For example, if an operator is granted permission to create new records, then permission is also granted to view and update records, but not delete records.

Refer to [Facility Permissions on page 102](#) for more information about configuring permissions. To review the specific permissions granted when using the predefined permissions, refer to the following sections:

Permission Level	Refer to:
All Facility Permissions	<a href="#">Table 149 on page 441</a>
Entry Level Guard Facility Permissions	<a href="#">Table 150 on page 444</a>
Guard Supervisor Facility Permissions	<a href="#">Table 151 on page 446</a>
Intermediate Guard Facility Permissions	<a href="#">Table 152 on page 448</a>
Update Configuration Facility Permissions	<a href="#">Table 153 on page 450</a>
View Configuration Facility Permissions	<a href="#">Table 154 on page 452</a>

If you are reading this document online, click one of the links above to navigate directly to the page.

### All Facility Permissions

**Table 149.** All Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Controls</b>						
<b>Lock/Unlock Access Points</b>	Yes					
<b>Activate/Reset Digital Outputs</b>	Yes					

**Table 149.** All Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Control PTZ Cameras</b>	Yes					
<b>Enable/Disable Digital Input Monitoring</b>	Yes					
<b>Enable/Disable Logical Input Monitoring</b>	Yes					
<b>Monitors</b>						
<b>Purge Alarms</b>	Yes					
<b>Acknowledge/Remove Alarms</b>	Yes					
<b>View Live Video</b>	Yes					
<b>View Recorded Video</b>	Yes					
<b>Setup</b>						
<b>Operators</b>		—	Yes	Yes	Yes	Yes
<b>Contexts</b>		—	Yes	Yes	Yes	Yes
<b>System Permissions</b>		—	Yes	Yes	Yes	Yes
<b>Facility Permissions</b>		—	Yes	Yes	Yes	Yes
<b>Facilities</b>		—	Yes	Yes	Yes	Yes
<b>Facility Commander Servers</b>		—	Yes	Yes	Yes	Yes
<b>Workstations</b>		—	Yes	Yes	Yes	Yes
<b>Access Control Systems</b>		—	Yes	Yes	Yes	Yes
<b>Devices</b>						
<b>Access Points</b>		—	Yes	Yes	Yes	Yes
<b>Digital Inputs</b>		—	Yes	Yes	Yes	Yes
<b>Logical Inputs</b>		—	Yes	Yes	Yes	Yes
<b>Digital Inputs</b>		—	Yes	Yes	Yes	Yes
<b>Digital Video Recorders</b>		—	Yes	Yes	Yes	Yes
<b>Cameras</b>		—	Yes	Yes	Yes	Yes
<b>Intercom Exchanges</b>		—	Yes	Yes	Yes	Yes

**Table 149.** All Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Intercom Stations</b>		—	Yes	Yes	Yes	Yes
<b>Analog Video Switcher</b>		—	Yes	Yes	Yes	Yes
<b>Intrusion Panels</b>		—	Yes	Yes	Yes	Yes
<b>Intrusion Areas</b>		—	Yes	Yes	Yes	Yes
<b>Intrusion Inputs</b>		—	Yes	Yes	Yes	Yes

## Entry Level Guard Facility Permissions

Table 150. Entry Level Guard Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Controls</b>						
<b>Lock/Unlock Access Points</b>	Yes					
<b>Activate/Reset Digital Outputs</b>	No					
<b>Control PTZ Cameras</b>	Yes					
<b>Enable/Disable Digital Input Monitoring</b>	No					
<b>Enable/Disable Logical Input Monitoring</b>	No					
<b>Monitors</b>						
<b>Purge Alarms</b>	No					
<b>Acknowledge/Remove Alarms</b>	Yes					
<b>View Live Video</b>	Yes					
<b>View Recorded Video</b>	Yes					
<b>Setup</b>						
<b>Operators</b>		Yes	No	No	No	No
<b>Contexts</b>		Yes	No	No	No	No
<b>System Permissions</b>		Yes	No	No	No	No
<b>Facility Permissions</b>		Yes	No	No	No	No
<b>Facilities</b>		Yes	No	No	No	No
<b>Facility Commander Servers</b>		Yes	No	No	No	No
<b>Workstations</b>		Yes	No	No	No	No
<b>Access Control Systems</b>		Yes	No	No	No	No

**Table 150.** Entry Level Guard Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Devices</b>						
<b>Access Points</b>		Yes	No	No	No	No
<b>Digital Inputs</b>		Yes	No	No	No	No
<b>Logical Inputs</b>		Yes	No	No	No	No
<b>Digital Video Recorders</b>		Yes	No	No	No	No
<b>Cameras</b>		Yes	No	No	No	No
<b>Intercom Exchanges</b>		Yes	No	No	No	No
<b>Intercom Stations</b>		Yes	No	No	No	No
<b>Analog Video Switcher</b>		Yes	No	No	No	No
<b>Intrusion Panels</b>		Yes	No	No	No	No
<b>Intrusion Areas</b>		Yes	No	No	No	No
<b>Intrusion Inputs</b>		Yes	No	No	No	No

## Guard Supervisor Facility Permissions

Table 151. Guard Supervisor Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Controls</b>						
<b>Lock/Unlock Access Points</b>	Yes					
<b>Activate/Reset Digital Outputs</b>	Yes					
<b>Control PTZ Cameras</b>	Yes					
<b>Enable/Disable Digital Input Monitoring</b>	Yes					
<b>Enable/Disable Logical Input Monitoring</b>	Yes					
<b>Monitors</b>						
<b>Purge Alarms</b>	Yes					
<b>Remove Alarms</b>	Yes					
<b>Acknowledge Alarms</b>	Yes					
<b>View Live Video</b>	Yes					
<b>View Recorded Video</b>	Yes					
<b>Setup</b>						
<b>Operators</b>	—	No	No	No	No	No
<b>Contexts</b>	—	No	No	No	No	No
<b>System Permissions</b>	—	No	No	No	No	No
<b>Facility Permissions</b>	—	No	No	No	No	No
<b>Facilities</b>	—	No	No	No	No	No
<b>Facility Commander Servers</b>	—	No	No	No	No	No
<b>Workstations</b>	—	No	No	No	No	No
<b>Access Control Systems</b>	—	No	No	No	No	No

**Table 151.** Guard Supervisor Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Devices</b>						
<b>Access Points</b>		No	No	No	No	No
<b>Digital Inputs</b>		No	No	No	No	No
<b>Logical Inputs</b>		No	No	No	No	No
<b>Digital Video Recorders</b>		No	No	No	No	No
<b>Cameras</b>		No	No	No	No	No
<b>Intercom Exchanges</b>		No	No	No	No	No
<b>Intercom Stations</b>		No	No	No	No	No
<b>Analog Video Switcher</b>		No	No	No	No	No
<b>Intrusion Panels</b>		No	No	No	No	No
<b>Intrusion Areas</b>		No	No	No	No	No
<b>Intrusion Inputs</b>		No	No	No	No	No

## Intermediate Guard Facility Permissions

Table 152. Intermediate Guard Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Controls</b>						
<b>Lock/Unlock Access Points</b>	Yes					
<b>Activate/Reset Digital Outputs</b>	Yes					
<b>Control PTZ Cameras</b>	Yes					
<b>Enable/Disable Digital Input Monitoring</b>	No					
<b>Enable/Disable Logical Input Monitoring</b>	No					
<b>Monitors</b>						
<b>Purge Alarms</b>	No					
<b>Remove Alarms</b>	Yes					
<b>Acknowledge Alarms</b>	Yes					
<b>View Live Video</b>	Yes					
<b>View Recorded Video</b>	Yes					
<b>Setup</b>						
<b>Operators</b>		Yes	No	No	No	No
<b>Contexts</b>		Yes	No	No	No	No
<b>System Permissions</b>		Yes	No	No	No	No
<b>Facility Permissions</b>		Yes	No	No	No	No
<b>Facilities</b>		Yes	No	No	No	No
<b>Facility Commander Servers</b>		Yes	No	No	No	No
<b>Workstations</b>		Yes	No	No	No	No
<b>Access Control Systems</b>		Yes	No	No	No	No



**Table 152.** Intermediate Guard Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Devices</b>						
<b>Access Points</b>		Yes	No	No	No	No
<b>Digital Inputs</b>		Yes	No	No	No	No
<b>Logical Inputs</b>		Yes	No	No	No	No
<b>Digital Video Recorders</b>		Yes	No	No	No	No
<b>Cameras</b>		Yes	No	No	No	No
<b>Intercom Exchanges</b>		Yes	No	No	No	No
<b>Intercom Stations</b>		Yes	No	No	No	No
<b>Analog Video Switcher</b>		Yes	No	No	No	No
<b>Intrusion Panels</b>		Yes	No	No	No	No
<b>Intrusion Areas</b>		Yes	No	No	No	No
<b>Intrusion Inputs</b>		Yes	No	No	No	No

## Update Configuration Facility Permissions

Table 153. Update Configuration Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Controls</b>						
<b>Lock/Unlock Access Points</b>	No					
<b>Activate/Reset Digital Outputs</b>	No					
<b>Control PTZ Cameras</b>	No					
<b>Enable/Disable Digital Input Monitoring</b>	No					
<b>Enable/Disable Logical Input Monitoring</b>	No					
<b>Monitors</b>						
<b>Purge Alarms</b>	No					
<b>Remove Alarms</b>	No					
<b>Acknowledge Alarms</b>	No					
<b>View Live Video</b>	No					
<b>View Recorded Video</b>	No					
<b>Setup</b>						
<b>Operators</b>		No	Yes	Yes	No	No
<b>Contexts</b>		No	Yes	Yes	No	No
<b>System Permissions</b>		No	Yes	Yes	No	No
<b>Facility Permissions</b>		No	Yes	Yes	No	No
<b>Facilities</b>		No	Yes	Yes	No	No
<b>Facility Commander Servers</b>		No	Yes	Yes	No	No
<b>Workstations</b>		No	Yes	Yes	No	No
<b>Access Control Systems</b>		No	Yes	Yes	No	No

**Table 153.** Update Configuration Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Devices</b>						
<b>Access Points</b>		No	Yes	Yes	No	No
<b>Digital Inputs</b>		No	Yes	Yes	No	No
<b>Logical Inputs</b>		No	Yes	Yes	No	No
<b>Digital Video Recorders</b>		No	Yes	Yes	No	No
<b>Cameras</b>		No	Yes	Yes	No	No
<b>Intercom Exchanges</b>		No	Yes	Yes	No	No
<b>Intercom Stations</b>		No	Yes	Yes	No	No
<b>Analog Video Switcher</b>		No	Yes	Yes	No	No
<b>Intrusion Panels</b>		No	Yes	Yes	No	No
<b>Intrusion Areas</b>		No	Yes	Yes	No	No
<b>Intrusion Inputs</b>		No	Yes	Yes	No	No

## View Configuration Facility Permissions

Table 154. View Configuration Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Controls</b>						
<b>Lock/Unlock Access Points</b>	No					
<b>Activate/Reset Digital Outputs</b>	No					
<b>Control PTZ Cameras</b>	No					
<b>Enable/Disable Digital Input Monitoring</b>	No					
<b>Enable/Disable Logical Input Monitoring</b>	No					
<b>Monitors</b>						
<b>Purge Alarms</b>	No					
<b>Remove Alarms</b>	No					
<b>Acknowledge Alarms</b>	No					
<b>View Live Video</b>	No					
<b>View Recorded Video</b>	No					
<b>Setup</b>						
<b>Operators</b>		—	Yes	No	No	No
<b>Contexts</b>		—	Yes	No	No	No
<b>System Permissions</b>		—	Yes	No	No	No
<b>Facility Permissions</b>		—	Yes	No	No	No
<b>Facilities</b>		—	Yes	No	No	No
<b>Facility Commander Servers</b>		—	Yes	No	No	No
<b>Workstations</b>		—	Yes	No	No	No
<b>Access Control Systems</b>		—	Yes	No	No	No

**Table 154.** View Configuration Facility Permissions

	Enabled	None	View	Update	Create	Delete
<b>Devices</b>						
<b>Access Points</b>		—	Yes	No	No	No
<b>Digital Inputs</b>		—	Yes	No	No	No
<b>Logical Inputs</b>		—	Yes	No	No	No
<b>Digital Video Recorders</b>		—	Yes	No	No	No
<b>Cameras</b>		—	Yes	No	No	No
<b>Intercom Exchanges</b>		—	Yes	No	No	No
<b>Intercom Stations</b>		—	Yes	No	No	No
<b>Analog Video Switcher</b>		—	Yes	No	No	No
<b>Intrusion Panels</b>		—	Yes	No	No	No
<b>Intrusion Areas</b>		—	Yes	No	No	No
<b>Intrusion Inputs</b>		—	Yes	No	No	No



## Appendix E. System Permissions

Use system permissions to grant or deny permissions to system applications, such as the Alarm Monitor, or access points to item that are not assigned to facilities. Examples of items that are not in facilities include: alarm colors, alarm instructions, and alarm profiles.

Refer to [System Permissions on page 108](#) for more information about configuring permissions. To review the specific permissions granted when using the predefined permissions, refer to the following sections:

Permission Level	Refer to:
All System Permissions	<a href="#">Table 155 on page 455</a>
Entry Level Guard System Permissions	<a href="#">Table 156 on page 457</a>
Guard Supervisor System Permissions	<a href="#">Table 157 on page 458</a>
Intermediate Guard System Permissions	<a href="#">Table 158 on page 459</a>

If you are reading this document online, click one of the links above to navigate directly to the page.

### All System Permissions

Grants all permissions including view, update, create, and delete for system level items. This also grants permission to use applications, such as the Alarm Monitor or permission to configure event action mapping definitions.

**Table 155.** All System Permissions

	Enabled	None	View	Update	Create	Delete
<b>Applications</b>						
<b>Alarm Monitor</b>	Yes					
<b>Event Monitor</b>	Yes					
<b>Video Console</b>	Yes					
<b>Graphic Viewer</b>	Yes					
<b>Editors</b>						

**Table 155.** All System Permissions

	Enabled	None	View	Update	Create	Delete
<b>Event Action Mappings</b>		—	Yes	Yes	Yes	Yes
<b>Alarm Instructions</b>		—	Yes	Yes	Yes	Yes
<b>Alarm Profiles</b>		—	Yes	Yes	Yes	Yes
<b>Graphic Editor</b>		—	Yes	Yes	Yes	Yes
<b>Symbol Editor</b>		—	Yes	Yes	Yes	Yes
<b>Operations</b>						
<b>Change Window Filter</b>	Yes					
<b>Change Locale</b>	Yes					
<b>Change Video Popup Options</b>	Yes					
<b>Shutdown System</b>	Yes					
<b>Run/Configure Diagnostics</b>	Yes					
<b>Alarm Colors</b>	Yes					
<b>System Parameters</b>	Yes					



## Entry Level Guard System Permissions

**Table 156.** Entry Level Guard System Permissions

	Enabled	None	View	Update	Create	Delete
Applications						
Alarm Monitor	Yes					
Event Monitor	Yes					
Video Console	Yes					
Graphic Viewer	Yes					
Editors						
Event Action Mappings		Yes	No	No	No	No
Alarm Instructions		Yes	No	No	No	No
Alarm Profiles		Yes	No	No	No	No
Graphic Editor		Yes	No	No	No	No
Symbol Editor		Yes	No	No	No	No
Operations						
Change Window Filter	No					
Change Locale	No					
Shutdown System	No					
Run/Configure Diagnostics	No					
Alarm Colors	No					
System Parameters	No					

## Guard Supervisor System Permissions

**Table 157.** Guard Supervisor System Permissions

	Enabled	None	View	Update	Create	Delete
<b>Applications</b>						
<b>Alarm Monitor</b>	Yes					
<b>Event Monitor</b>	Yes					
<b>Video Console</b>	Yes					
<b>Graphic Viewer</b>	Yes					
<b>Editors</b>						
<b>Event Action Mappings</b>		Yes	No	No	No	No
<b>Alarm Instructions</b>		Yes	No	No	No	No
<b>Alarm Profiles</b>		Yes	No	No	No	No
<b>Graphic Editor</b>		Yes	No	No	No	No
<b>Symbol Editor</b>		Yes	No	No	No	No
<b>Operations</b>						
<b>Change Window Filter</b>	Yes					
<b>Change Locale</b>	Yes					
<b>Shutdown System</b>	No					
<b>Run/Configure Diagnostics</b>	No					
<b>Alarm Colors</b>	No					
<b>System Parameters</b>	No					

## Intermediate Guard System Permissions

**Table 158.** Intermediate Guard System Permissions

	Enabled	None	View	Update	Create	Delete
<b>Applications</b>						
Alarm Monitor	Yes					
Event Monitor	Yes					
Video Console	Yes					
Graphic Viewer	Yes					
<b>Editors</b>						
Event Action Mappings		Yes	No	No	No	No
Alarm Instructions		Yes	No	No	No	No
Alarm Profiles		Yes	No	No	No	No
Graphic Editor		Yes	No	No	No	No
Symbol Editor		Yes	No	No	No	No
<b>Operations</b>						
Change Window Filter	Yes					
Change Locale	Yes					
Shutdown System	No					
Run/Configure Diagnostics	No					
Alarm Colors	No					
System Parameters	No					

