Administering Cisco Physical Security Operations Manager

Version 5.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24230-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Administering Cisco Physical Security Operations Manager
© 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Overview ix

Organization ix

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1 **Getting Started with PSOM** 1-1

About PSOM 1-1

Understanding the deployment architecture 1-2

Learning about PSOM Services 1-2

Overview of the Operation Console 1-3

Configuring PSOM 1-6

Getting familiar with the Administration Console 1-10

Docking and Undocking the Navigation Pane 1-13

Logging On or Off 1-13

Viewing and Updating Your License Key 1-14

Setting Preferences 1-17

Setting Homeland Security or MARSEC levels for the Operation Console 1-17

Setting Alert Preferences for the Operation Console 1-19

Setting Alert Preferences for the Alert Management Console 1-21

Setting Alert Preferences for the Alert Details Window 1-22

Setting the Order of the Monitoring Hierarchy 1-23

Stopping Video Alert Messages for Consoles without Video Support 1-24

Starting and Stopping Services 1-25

CHAPTER 2 **Defining Users and Managing User Groups** 2-1

Managing Users 2-1

Types of User Roles 2-1

Planning a PSOM User Deployment 2-2

Setting Up User Accounts 2-2

Changing a User Password or Security Role 2-5

Changing the Name Assigned to a User 2-6

Viewing the Groups to which a User Belongs 2-6

Viewing Users by Role 2-8

Managing User Groups 2-12
Creating a User Group 2-12
Editing a User Group 2-15
Managing the Members of a User Group 2-17
Deleting a User Group 2-19
Permissions Within PSOM 2-20
Enforcing Strong Passwords in PSOM 2-22
Single Sign On and User Management 2-25
Enabling PSOM Web Service to use SSO 2-25
Logging Into PSOM with SSO 2-26
Adding Users from Active Directory 2-26
Identity Management in PSOM 2-27

CHAPTER 3 **Configuring Video Services** 3-1
Enabling Video Integration with PSOM 3-1
Configuring Access to Video Servers for Monitoring 3-1
Adding New Sensors for Video Cameras 3-3
Controlling User Access to Video 3-3
Performing Batch Imports for Video Camera Sensors 3-4
Managing Video Matrix Views and Guard Tours 3-6

CHAPTER 4 **Defining Locations** 4-1
Planning Locations for your Environment 4-1
Adding Locations to PSOM 4-2
Editing Locations 4-3
Deleting Locations 4-5
Importing or Exporting Location Names 4-6

CHAPTER 5 **Managing Monitoring Areas and Zones** 5-1
Understanding Monitoring Areas and Zones 5-1
Planning Monitoring Areas and Zones 5-2
Adding Monitoring Areas to PSOM 5-2
Adding Monitoring Zones to PSOM 5-6
Setting up the Monitoring Tree Hierarchy 5-10
Adding Monitoring Zones to the Monitoring Tree 5-10
Adding Multiple Levels of Monitoring Zones to the Monitoring Tree 5-13
Adding Monitoring Areas to the Monitoring Tree 5-14

Removing Nodes from the Monitoring Tree 5-16
Viewing Properties for Monitoring Tree Nodes 5-17
Adding Maps to Monitoring Areas and Zones 5-19
Editing or Deleting Monitoring Areas 5-20
Editing or Deleting Monitoring Zones 5-23
Importing or Exporting Monitoring Areas 5-26

CHAPTER 6 **Managing Sensors** 6-1
Types of Sensors and Connectors 6-1
Planning Sensor Integration 6-2
Adding New Sensors for Access Control Devices 6-2
Adding new Sensors for Video Cameras 6-7
Setting Up PTZ Preset Positions 6-12
Adding New Sensors for Other Types of Devices 6-16
Editing Sensors 6-20
Grouping Sensors 6-24
Types of Sensor Groups 6-24
Adding a Sensor Group 6-24
Editing a Sensor Group 6-27
Deleting a Sensor Group 6-29
Managing Intercom Device Groups 6-30
Adding an Intercom Device Group 6-30
Editing an Intercom Device Group 6-33
Deleting an Intercom Device Group 6-35
Importing and Exporting Sensors, Sensor Groups, and Intercom Groups with PSOM 6-36
Updating Sensors with a Web Service Call 6-41
Structure of XML for Sensor Definitions 6-41
Structure of XML for Sensor Group Definitions 6-42
Return Values 6-42

CHAPTER 7 **Designing Maps** 7-1
Entering Map Design Mode 7-1
Adding Background Map Images 7-5
Configuring Origin and Scale for a Map 7-6
Configuring Coordinates using GPS 7-8
Setting Display Options for a Map 7-14
Drawing a Monitoring Zone or Area on a Map 7-16

Adding Sensors to a Map 7-21
Adding Navigation to Maps 7-24
Adding URL Links to Maps 7-27
Editing and Deleting Items from the Map 7-29
Setting the Sort Order of the Monitoring Hierarchy 7-30
Integrating GIS Maps with PSOM 7-31

CHAPTER 8 **Managing Response Task Items and Response Workflow Rules** 8-1
Response Tasks within the Operation Console 8-1
Managing Response Task Items 8-2
Adding a New Response Task Item 8-3
Modifying a Response Task Item 8-7
Deleting a Response Task Item 8-8
Managing Response Workflow Rules 8-9
Adding a New Response Workflow Rule 8-9
Modifying a Response Workflow Rule 8-14
Deleting a Response Workflow Rule 8-15
Applying a Response Workflow Rule to an Alert Type 8-15
Enforcing Task Completion in the Operation Console 8-19

CHAPTER 9 **Managing Alert Collapsing Rules** 9-1
Collapsing Similar Alerts Under a Single Listing 9-1
Adding an Alert Collapsing Rule 9-2
Applying an Alert Collapsing Rule 9-5

CHAPTER 10 **Customizing Reports** 10-1
Types of Default Reports 10-1
Customizing a Report 10-2
Modifying a Custom Report 10-8
Deleting a Custom Report 10-9
Setting a Default Directory for Incident Packages 10-10

CHAPTER 11 **Integrating Sensors with External Systems, Registering Third-Party Alarm Types, and Configuring Integration Modules** 11-1
Overview of Sensor Mappings 11-1
Mapping a Sensor 11-2
Editing or Deleting a Sensor Mapping 11-5

Registering Third-Party Alarms 11-6
Editing or Deleting a Registered Alert Type 11-10
Creating a Custom Alert Type 11-12
Creating a System Alert Type 11-15
Configuring Integration Modules for External Systems Integration 11-16

CHAPTER 12 **Setting Up EZ-Track** 12-1
How Operators use EZ-Track 12-1
Configuring PSOM for EZ-Track 12-3
Taking 'Field of View' Snapshot Images for Camera Sensors 12-3
Configuring the View Settings for Camera Sensors 12-6
Displaying the Sensor Name and Range in the Map View 12-7
Configuring the EZ-Track Camera Topology 12-11
Displaying Camera Positions and Names on the Map 12-16
Viewing Live Video for a Camera Sensor 12-16
Editing a Link to an Adjacent Camera 12-17
Deleting a Link to an Adjacent Camera 12-17
Making an Adjacent Camera the New "Base" Camera 12-18
Viewing Other Region Links to an Adjacent Camera 12-18
Testing the EZ-Track Configuration 12-18
Enabling EZ-Track (Backward) 12-19
Configuring EZ-Track in Batch with XML Configuration File 12-20
Defining the EZ-Track Configuration in XML 12-20
Uploading the XML Configuration File for EZ-Track 12-21
Exporting Your EZ-Track Configuration 12-22

CHAPTER 13 **Managing Tracking Devices and Resources** 13-1
Viewing Security Resources 13-1
Activating or Deactivating a Resource 13-3
Understanding Tracking Devices 13-5
Viewing Tracking Devices in PSOM 13-5
Activating or Deactivating a Tracking Device 13-7

CHAPTER 14 **Managing Business Logic** 14-1
Managing Business Logic using Templates 14-1
Creating an Event Business Logic Template Based on the Default Template 14-2
Applying Event Monitoring Business Logic in your Environment 14-12
Restricting Event Monitoring Business Logic to Monitoring Areas or Zones 14-13

Restricting Event Monitoring Business Logic to a Schedule 14-14
Taking Actions Before and After Alert Creation 14-15
Creating an Alert Business Logic Template Based on the Default Template 14-16
Creating a Schedule Business Logic Template Based on the Default Template 14-20
Creating an On-Demand Business Logic Template Based on the Default Template 14-24
Controlling Permissions to On-Demand Business Logic 14-30
Creating an Alert Status Business Logic Template Based on the Default Template 14-31
Designing Business Logic in the Business Logic Designer 14-36
Testing Business Logic Templates in the Business Logic Designer 14-43
Debugging Business Logic Templates that Include CorrelateCondition Components 14-43
Debugging Business Logic Templates that Include Delay Loops 14-46
Applying Business Logic Policies 14-46
Importing and Exporting Business Logic Templates 14-50
Using Global System Variables in Business Logic 14-51
Storing PowerShell Scripts for Business Logic 14-51
Adding Parameters to Define PowerShell Scripts 14-54
Adding Scripts to the Script Area 14-56
Setting Up PowerShell Scripts 14-56
PowerShell Script Format 14-57
Passing Objects in PowerShell Scripts Using Script Variables 14-58
Understanding Activity Contexts 14-60
Performing Health Checks Using PowerShell Scripts 14-62
Ping Test 14-62
Service Test 14-63
HTTP Test 14-64

CHAPTER 15 **Business Logic Component Reference** 15-1
Understanding Business Logic Components 15-2
Configuring Delay Properties 15-7
Configuring Call Child Logic Properties 15-8
Configuring Call Everbridge Properties 15-9
Configuring Call External Method Properties 15-11
Configuring Call Web Service Properties 15-15
Configuring Create Admin Alert Properties 15-16
Configuring Create Alert Properties 15-17
Configuring Create Report Properties 15-18
Configuring DOS Command Properties 15-21
Configuring HTTP Send Properties 15-22

Configuring IPICS Dispatch Alert Properties 15-23
Configuring IPICS Notify Alert Properties 15-24
Configuring ODBC Action Properties 15-25
Configuring PowerShell Action Properties 15-26
PowerShell Action Examples 15-28
Configuring PTZ Control Properties 15-29
Configuring Send Email Properties 15-31
Configuring Set Alert Context Properties 15-33
Configuring Set Alert Severity Properties 15-34
Configuring Set Alert Status Properties 15-35
Configuring Alert Condition Properties 15-35
Configuring Geo-Location Properties 15-37
Configuring Monitor Hierarchy Properties 15-38
Configuring Schedule Condition Properties 15-39
Configuring Threat Level Properties 15-41
Configuring Simulate Alert Properties 15-42
Configuring Simulate Contexts Properties 15-43
Configuring Simulate Event Properties 15-45
Configuring Correlate Condition Properties 15-46
Configuring Event Map Filter Properties 15-51
Using Event Map Filter in Event Monitoring Business Logic 15-54
Configuring Escalate Condition Properties 15-56
Configuring ODBC Condition Properties 15-57
Configuring PowerShell Decision Properties 15-58
PowerShell Decision Examples 15-61
Example 1: Creating User Alerts when a Process is Not Running 15-61
Example 2: Creating User Alerts when a Machine Becomes Unreachable 15-62
Configuring RSS Alerts Properties 15-63
Configuring Lock Door Properties 15-66
Configuring Open Door Properties 15-68
Configuring Open Door Momentarily Properties 15-70

CHAPTER 16 **Diagnosing System Tasks and Alerts** 16-1
Diagnosing Administrative Alerts 16-1
Diagnosing Monitoring Alerts 16-3
Producing an Audit Trail of all Activity in PSOM 16-6

Setting How Long Audit Records are Stored by PSOM 16-9

APPENDIX A **Planning Worksheets** A-1

Access Control System Integration Planning A-2
User Deployment Planning A-3
Locations Planning A-4
Video Camera Planning A-5
Monitoring Zone Planning A-6
Monitoring Areas Planning A-7
Task Items Planning A-8
Response Workflow Planning A-9
EZ-Track Planning A-10

APPENDIX B **Backup and Restore PSOM Database** B-1

Scheduled Back-up of the PSOM Database B-1
Manually Backing up the PSOM Database B-3
Restoring the PSOM Database B-5
Grooming the PSOM Database B-7

APPENDIX C **Reconfiguring PSOM Services** C-1

Reconfiguring Settings for PSOM Services C-1
Specifying Custom Parsing C-13
Changing the Configuration of the PSOM Web Service C-16
Changing the Configuration of the Connector Web Service C-19
Reconfiguring Settings for PSOM User Services C-22

GLOSSARY

INDEX

Preface

Overview

This manual provides information about administering Cisco Physical Security Operations Manager (PSOM).

Organization

This manual is organized as follows:

Chapter 1, “Getting Started with PSOM”	What operators do with the Operation Console, what must be configured so the Operation Console can be used, and how you must proceed to set up the PSOM system
Chapter 2, “Defining Users and Managing User Groups”	Describes how to set up user accounts and assign them to user groups so that operators can access the Operation Console, Administration Console, Alert Management Console, Video Management Console, or Business Logic Designer
Chapter 3, “Configuring Video Services”	Covers the basic steps to enable video streaming in the Operation Console
Chapter 4, “Defining Locations”	Explains how to establish the *locations,* or physical spaces, within your environment that will be monitored by PSOM
Chapter 5, “Managing Monitoring Areas and Zones”	Provides information about monitoring areas and monitoring zones, including how to add a monitoring area, how to add a monitoring, and how to establish a hierarchical navigation tree for traversing the security environment from the Navigation Pane
Chapter 6, “Managing Sensors”	Provides information about using sensors in a PSOM environment
Chapter 7, “Designing Maps”	Describes how to use the Map Design Mode to perform a variety of activities with maps
Chapter 8, “Managing Response Task Items and Response Workflow Rules”	Provides detailed information about response tasks and response workflow rules

Chapter 9, "Managing Alert Collapsing Rules"	Describes how to collapse similar alerts under a single listing in the Operation Console
Chapter 10, "Customizing Reports"	Describes the default reports that PSOM provides and how to customize a default report
Chapter 11, "Integrating Sensors with External Systems, Registering Third-Party Alarm Types, and Configuring Integration Modules"	Provides information about synchronize information between external intrusion detection systems and PSOM, managing sensor mappings, registering third-party alarm types, and creating custom alert types
Chapter 12, "Setting Up EZ-Track"	This chapter explains how to prepare video camera sensors for EZ-Track, configure EZ-Track navigation for camera sensors, import an EZ-Track configuration from an XML file, and enable backward tracking with EZ-Track
Chapter 13, "Managing Tracking Devices and Resources"	Provides information about tracking devices and security resources
Chapter 14, "Managing Business Logic"	Provides information about business logic and related activities
Chapter 15, "Business Logic Component Reference"	Provides detailed information about the components that can be used to build business logic templates
Chapter 16, "Diagnosing System Tasks and Alerts"	Provides information about diagnosing administrative alerts and monitoring alerts, and explains how to produce an audit trail about PSOM activity
Appendix A, "Planning Worksheets"	Provides worksheets you can use for planning your PSOM environment
Appendix B, "Backup and Restore PSOM Database"	Explains how to back up and restore PSOM database
Appendix C, "Reconfiguring PSOM Services"	Explains how to reconfigure PSOM Services, PSOM Web Service, and PSOM Connector Web Service after an initial deployment
Glossary	Defines various terms

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. That document also lists new and revised Cisco technical documentation. It is available at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Getting Started with PSOM

As the administrator, you are responsible for setting up and managing all components of Cisco Physical Security Operations Manager (PSOM) that are used by operators in the Operation Console. In this chapter, you'll learn:

- What operators do with the Operation Console
- What must be configured so the Operation Console can be used
- How you must proceed to set up the PSOM system

This chapter includes these topics:

- About PSOM, page 1-1
- Understanding the deployment architecture, page 1-2
- Learning about PSOM Services, page 1-2
- Overview of the Operation Console, page 1-3
- Configuring PSOM, page 1-6
- Getting familiar with the Administration Console, page 1-10
- Logging On or Off, page 1-13
- Viewing and Updating Your License Key, page 1-14
- Setting Preferences, page 1-17
- Starting and Stopping Services, page 1-25

About PSOM

PSOM is a Physical Security Information Management (PSIM) solution that provides situational awareness across the organization and delivers the insight required to protect people, assets and infrastructure. PSOM is a unified management platform that connects physical security systems (access control, analytics, sensors, video surveillance, etc.) with logical ones to enable security teams to better manage security events.

Understanding the deployment architecture

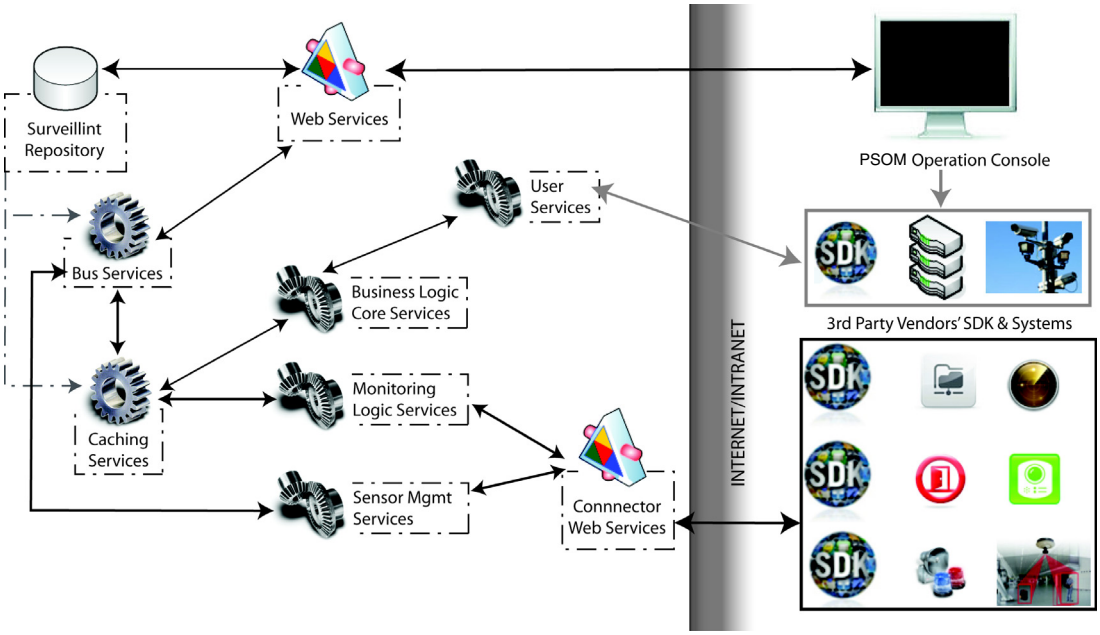
PSOM has these major components:

- PSOM Services—Collect information from various sensors within a security environment, and process this data for analysis of alert conditions. Specifically, the PSOM Services integrate with video, access control, and intrusion detection systems to collect sensor alerts and live and recorded video. Multiple network interface cards (NICs) enable PSOM Services to access the IP networks for the subsystems which may be on different networks.
- PSOM Consoles—Includes the Administration Console, Operation Console, Alert Management Console, Video Management Console, and Business Logic Designer. The Operation Console enables operators to detect and respond to alerts, view live and recorded video, and report on alert conditions. The Administration Console enables administrators to configure and manage the elements of PSOM used by the Operation Console.
- PSOM Repository—Stores all environment configurations and data collected by PSOM in a standard Microsoft SQL Server 2008 database.

Learning about PSOM Services

Each of the PSOM Services must be running for PSOM to function correctly.

- Bus Services (BUS)—Dispatches and routes rules, alerts, schedules, and commands to various services. Dynamically discovers Integration Modules and monitors services for abnormalities (e.g., a service becomes unreachable).
- Caching Services (CS)—Speeds up business logic execution by caching monitoring hierarchy and sensor map information.
- Business Logic Core Services (BL CORE)—Runs business logic policies such as Alert Business Logic, Scheduled Business Logic, and so forth; the BL CORE does not handle event monitoring logic.
- Monitoring Logic Services (MS)—Detects new and updated events from sensors via Integration Modules and creates alerts in PSOM.
- Sensor Management Services (SM)—Automatically discovers sensors via Integration Modules and synchronizes them with PSOM. Supports customized parsing of device semantics, and can automatically create the monitoring hierarchy with correct areas, zones and sensor locations.
- Web Services (WS)—Handles communication between PSOM Services and PSOM Consoles, and enables integration with external alarm systems.
- User Services (US)—Runs reports on data collected by PSOM and controls video management systems and cameras. This service is optional.
- Connector Web Services (CWS)—Handles communication with third-party vendor systems via Integration Modules. This service is optional if only video is being used.



PSOM uses a scalable Service Oriented Architecture (SOA) based on .NET, and is comprised of a series of web services which means PSOM enables easy integration with existing technology infrastructures.

Instead of being a monolithic application requiring significant development to add or modify functionality, PSOM uses a modern modular design that separates application components into discrete modules. The modular approach enables easy modifications with minimal impact and allows new functional modules to be added at any time. PSOM integration modules with physical security subsystems leverage this approach for quick development and deployment.

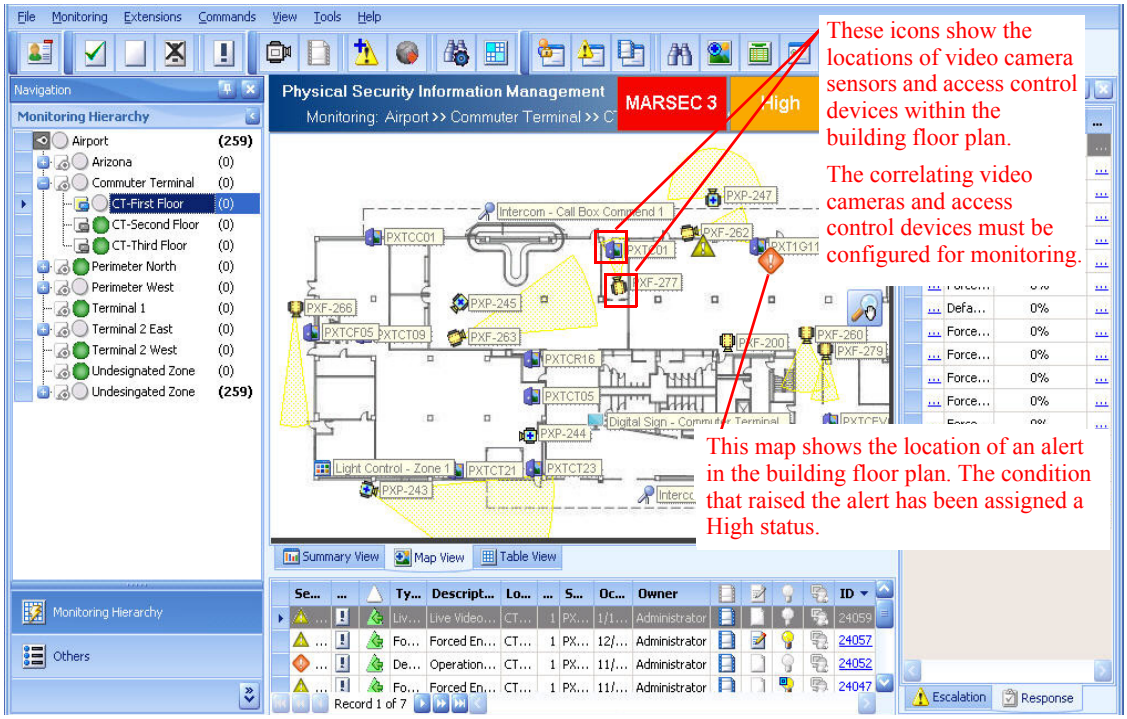
All data collected by PSOM is stored in a standard Microsoft SQL Server 2005 or SQL Server 2008 database. The use of a commonly deployed database platform simplifies regular database administration tasks and allows easy access to data in case there are unique reporting requirements not met by PSOM reporting capabilities. In addition to simplified management and reporting, PSOM can also leverage some of SQL Server's more advanced features such as clustering and replication.

All communication between PSOM components is based on the global standard TCP/IP protocol. This communication uses standard port definitions such as HTTP or HTTPS which means firewalls and other networking equipment require minimal configuration modifications. The message format used for communication is based on another industry standard, Extensible Markup Language, commonly known as XML. A significant benefit of using XML as a data interchange is that third party products based on SOA and XML can be quickly and easily integrated with PSOM.

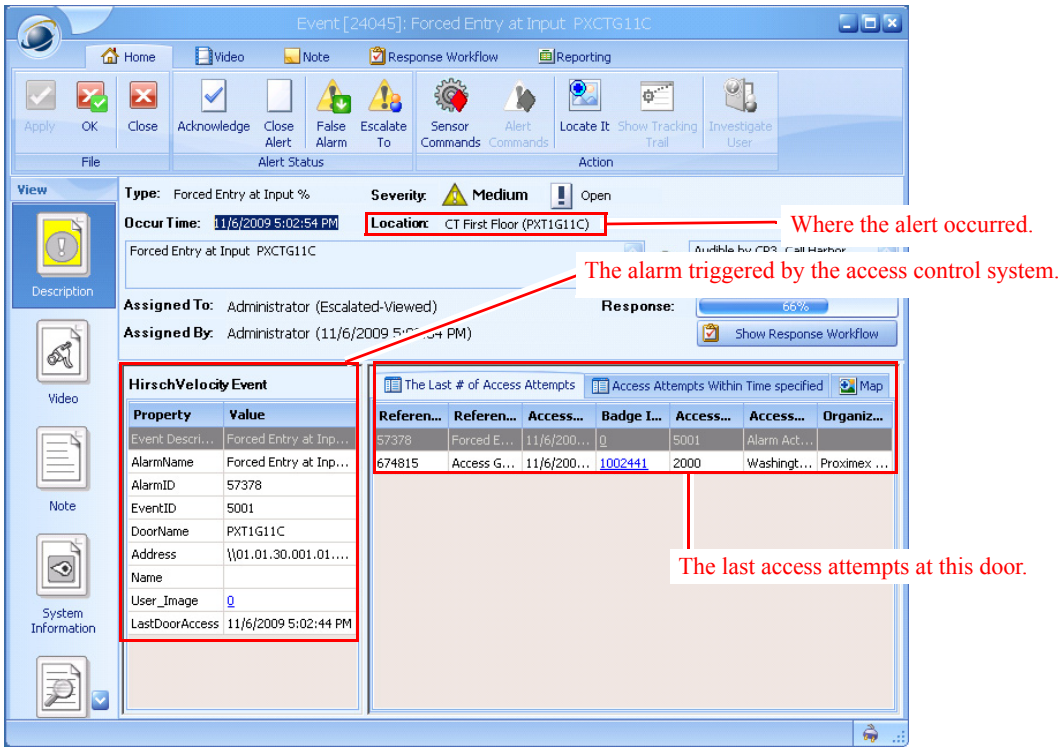
Overview of the Operation Console

Before you can understand the administration tasks that must be accomplished, you must first understand the environment you are configuring for security operators. That environment is the Operation Console, as shown next.

When an operator drills down on the map shown previously, a lower-level building floor plan appears. This floor plan shows the placement of all video camera sensors and access control devices, as shown next.



When operators view details for an alert, they see information that has been configured or enabled by a system administrator including: the location description, the sensor's assigned ID, the alarm triggered by the external access control system, the details for the last access attempts, and recorded video footage for the alert.



Further, all of this information is compiled into a printed or electronic document for notification and reporting purposes.

See the *Using Cisco Physical Security Operations Manager* guide for information about using the Operation Console.

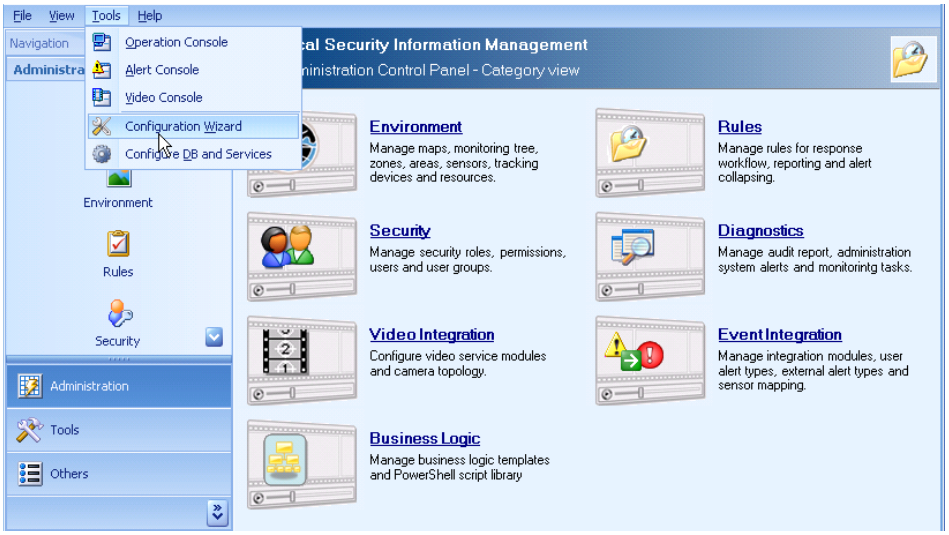
Configuring PSOM

As the administrator, you play a critical role in designing and configuring PSOM so that the right information is readily available to security operators and first responders.

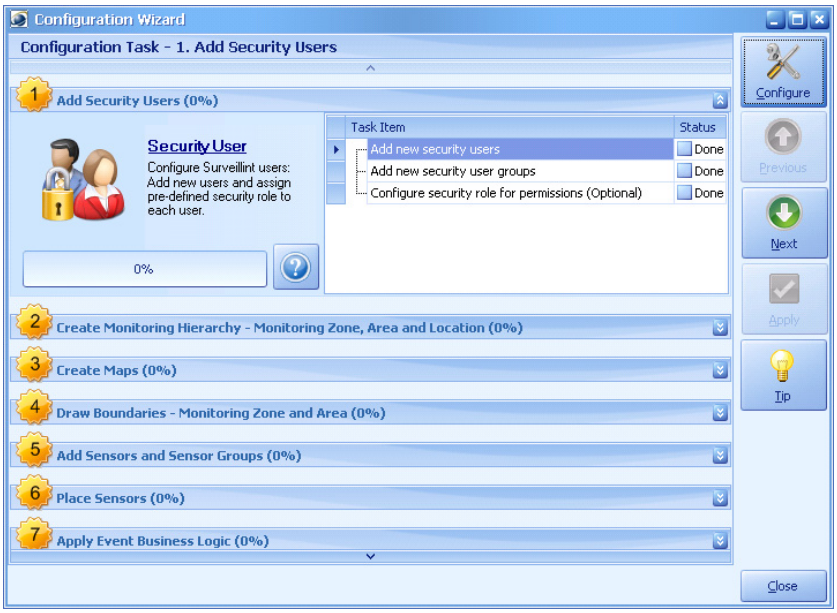
To get PSOM up and running, you must perform a series of tasks to setup the environment. You can use the Configuration Wizard to guide you through this process.

To configure PSOM using the Configuration Start Wizard:

Step 1 Select **Tools > Configuration Wizard**.



The Configuration Wizard appears.



Step 2 Select each task in order and its section will expand with a list of tasks to be completed.

Step 3 Click the **Configure** button to launch the appropriate configuration window for the task to be completed.

Step 4 Click **Next** to move on to the next administration task.

Configuration tasks you must perform as administrator include:

- Set up users and assign them to security groups.

- Establish the hierarchy of monitoring zones and areas within your security environment—This involves dividing the overall security boundary into logical top-level groups (monitoring zones), and then splitting those groups into areas that can be managed from a single view of a building floor plan (monitoring areas).
- Create maps for the monitoring hierarchy—This involves uploading graphics for the different monitoring areas and zones in your environment.
- Draw boundaries on maps for the monitoring zones and areas—This involves visually defining the monitoring zones and areas on graphical maps to show the boundaries.
- Add sensors for each video camera and access control, and define sensor groups—A sensor must be defined in PSOM for each physical sensor in the environment. And you can group sensors together that collaborate to report events; for example, group an access control device and the video camera that monitors it.
- Place sensors into the correct monitoring zone or area, and add them to maps—Then these sensors must be placed appropriately on building floor plans for your monitoring areas.
- Apply event business logic to ensure that rules are followed and security policies are consistently repeatable.
- Create response workflows that define standard operating procedures for response to incidents.
- Automate escalation of alerts to ensure prompt and appropriate incident response.
- Customize automated response with alert business logic policies.

There is a set of information you need to gather before beginning to set up PSOM for your security environment. Table 1-1 lists the details you'll need and tells you which planning worksheet you can use in Appendix A, "Planning Worksheets," to gather the information.

Table 1-1 Planning Information Needed for Deploying PSOM

To set up...	You need to gather this information...	You can use this worksheet...
Video sensors	For each video camera, you need its: • Device ID • Location (see Locations below) • View Range (in degrees)—the width of the camera's viewing area. • View Distance (in feet)—the distance from the camera to the farthest point it can accurately view. • View Direction (in degrees)—the focus angle of the camera (clockwise from 0-359). This tells PSOM the direction the camera is pointing from 0–180 degrees.	Video Camera Planning, page A-5

Table 1-1 Planning Information Needed for Deploying PSOM (continued)

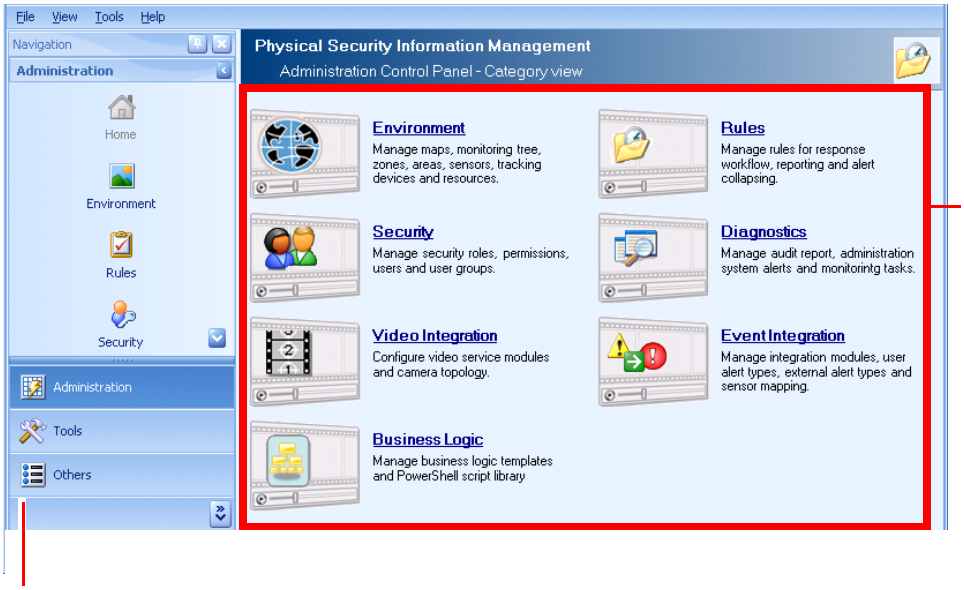
To set up...	You need to gather this information...	You can use this worksheet...
Access control system integration	For each access control system, you need its: • IP address or server name • ACS login name • ACS login password See the Integration Module documentation for details. Install the PxDocSetup.msi file to obtain all PSOM documentation.	"Access Control System Integration Planning" section on page A-2
Sensor groups	Determine which video camera sensors should be grouped with access control devices, and what other sensor groups make sense for monitoring activity in your environment.	—
Users	For each employee, you need: • Login user name • Login password • Security group assignment • Description • Security role and permissions	"User Deployment Planning" section on page A-3
Locations	For each physical space in your environment that will be monitored by PSOM, you need to create: • Location name • Description	"Locations Planning" section on page A-4
Monitoring Zones	A monitoring zone is a logical group of monitoring areas (or monitoring zones) that are associated because of physical location, business function, or other reasons. For each monitoring zone you need: • A name for the monitoring zone. • The list of monitoring areas (or zones) that should be part of the monitoring zone. **Note** Monitoring zones can contain monitoring areas, or monitoring zones, but not both.	"Monitoring Zone Planning" section on page A-6

Table 1-1 Planning Information Needed for Deploying PSOM (continued)

To set up...	You need to gather this information...	You can use this worksheet...
Monitoring Areas	A monitoring area is a virtual representation of a place within your security environment that is associated with a map or building floor plan and sensor groups that exist in that physical space. For each monitoring area you need: • A name for the monitoring area. • A description of the physical place represented by the monitoring area. • A list of sensors and sensor groups that should be part of this monitoring area.	"Monitoring Areas Planning" section on page A-7
Response Tasks Items and Response Workflow Rules	Response workflow rules are comprised of response tasks items, and apply to specific types of alerts. To perform this step, you need to know: • What are all the different actions that operators will need to perform to resolve alerts? These are defined as *response tasks items*. • For each type of alert, what are the tasks that operators need to perform? You'll define different *response workflow rules* for each type of alert. • For each response workflow rule, which response tasks items must be performed before the alert can be acknowledged? Or before it can be closed?	• "Task Items Planning" section on page A-8 • "Response Workflow Planning" section on page A-9
EZ-Track	To configure each video camera for EZ-Track, you must know: • How long it takes (in seconds) to travel from camera to camera at a regular walking stride. • Which cameras are up, down, left, right from the source camera.	"EZ-Track Planning" section on page A-10

Getting familiar with the Administration Console

From the Administration Console, you can perform most administrative tasks.



The center of the window lists all the tools you will use to set up and administer PSOM. Table 1-2 describes tasks you can perform with each of these tools.

Table 1-2 Tools You can Use to Perform Different Tasks

To do this:	Use this Tool:	See:
Add new users to PSOM.	Security	"Setting Up User Accounts" section on page 2-2
Assign users to different security groups.	Security	"Managing the Members of a User Group" section on page 2-17
Add locations, monitoring areas and monitoring zones to PSOM.	Environment	• "Adding Locations to PSOM" section on page 4-2 • "Adding Monitoring Areas to PSOM" section on page 5-2 • "Adding Monitoring Zones to PSOM" section on page 5-6
Add sensors to PSOM and group them together.	Environment	• "Adding New Sensors for Access Control Devices" section on page 6-2 • "Adding new Sensors for Video Cameras" section on page 6-7 • "Adding New Sensors for Other Types of Devices" section on page 6-16 • "Grouping Sensors" section on page 6-24

Table 1-2 Tools You can Use to Perform Different Tasks (continued)

To do this:	Use this Tool:	See:
Establish the navigation hierarchy of monitoring zones, monitoring areas, and locations.	Environment	"Setting up the Monitoring Tree Hierarchy" section on page 5-10
Add aerial maps and building floor plans to monitoring zones, monitoring areas, and locations.	Environment	"Adding Background Map Images" section on page 7-5
Add sensors to maps.	Environment	"Adding Sensors to a Map" section on page 7-21
Integrate GIS maps with PSOM.	Environment	"Integrating GIS Maps with PSOM" section on page 7-31
Set up response tasks items and response workflow rules, and apply them to alerts.	Rules	Chapter 8, "Managing Response Task Items and Response Workflow Rules"
Set up alert collapsing rules.	Rules	Chapter 9, "Managing Alert Collapsing Rules"
Configure automated reporting.	Rules	Chapter 10, "Customizing Reports"
Integrate sensors with external intrusion detection systems.	Event Integration	Chapter 11, "Integrating Sensors with External Systems, Registering Third-Party Alarm Types, and Configuring Integration Modules"
Set Homeland Security or MARSEC levels.	Preferences	"Setting Homeland Security or MARSEC levels for the Operation Console" procedure on page 1-17
Diagnose system tasks, alerts and events.	Diagnostics	Chapter 16, "Diagnosing System Tasks and Alerts"
Configure video services.	Video Camera	Chapter 3, "Configuring Video Services"
Set up video cameras to enable EZ-Track.	Video Camera	Chapter 12, "Setting Up EZ-Track"
Set up EZ-Track camera topology.	Environment or Video Camera	Chapter 12, "Setting Up EZ-Track"
Set up tracking devices and resources.	Environment	Chapter 13, "Managing Tracking Devices and Resources"
Configure business logic for alert response.	Business Logic	Chapter 14, "Managing Business Logic"

Aside from the tools you can use, you can also launch the Operation Console by clicking its name under Operations on the left side of the window.

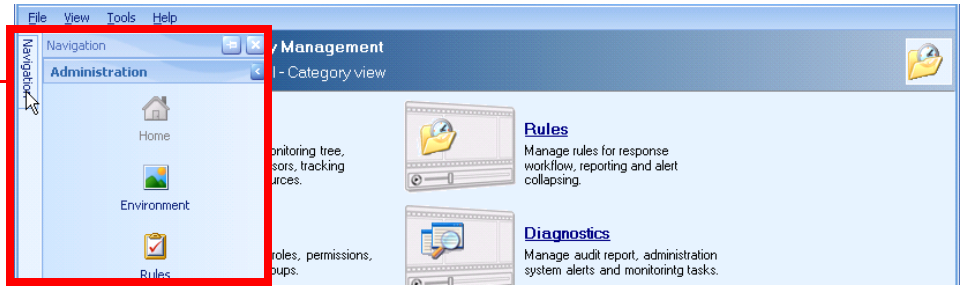
Under Others on the left side of the window, you can perform these functions:

- To change preferences for the Administration Console and Operation Consoles in your organization, click **Preferences**.
- If you want to change the permissions or password of the current login account, click **Security Profile**.
- To view licensing information, or update your license key, click **License Manager**.
- You can access help by clicking **Help and Support**.

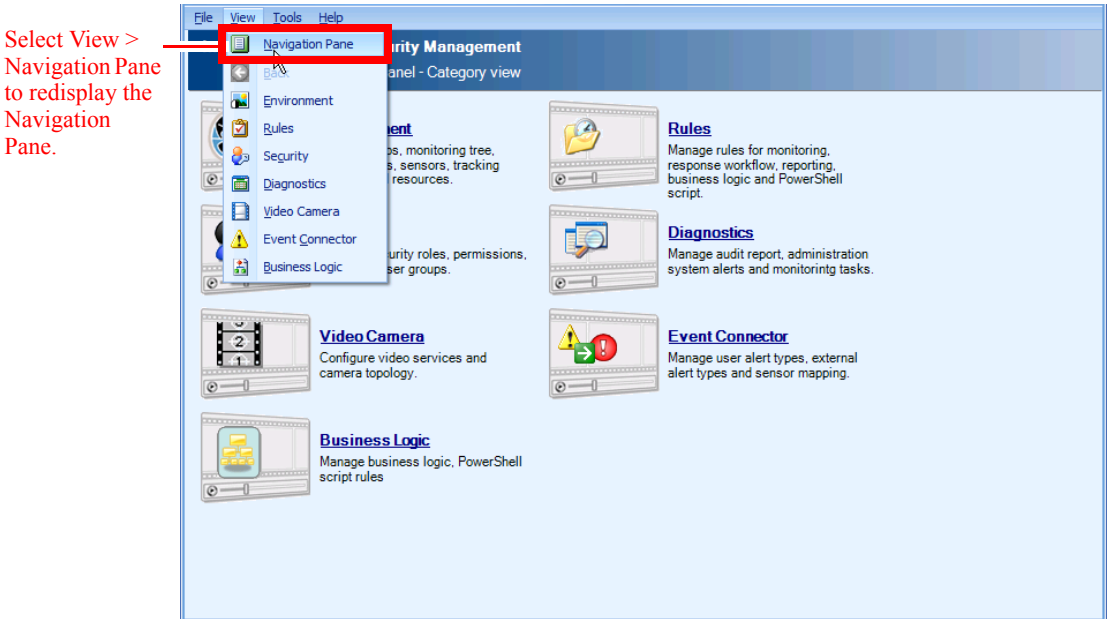
Docking and Undocking the Navigation Pane

If you want to create more working space in the Administration Console, you can undock the Navigation Pane on the left side of the window by clicking the thumbtab icon. Then click the Navigation tab when you want to see the pane.

The Navigation Pane will appear when you select the **Navigation Pane** menu.



You can completely close the Navigation Pane by clicking the **X** button at the top right corner of the pane. To subsequently redisplay the Navigation Pane, select **View > Navigation Pane** from the menus at the top of the window.

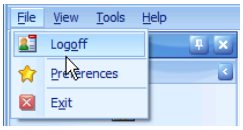


Logging On or Off

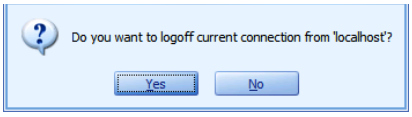
You can log off PSOM Administration Console, and then log back on as a different user, without exiting the Administration Console.

To log off the Administration Console:

Step 1 Select **File > Logoff**.



A confirmation dialog appears.

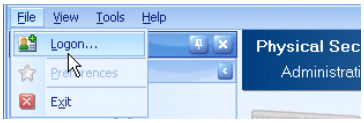


Step 2 Click **Yes**.

To log back on to the Administration Console:

Note If you're using single sign-on to login to PSOM (e.g., Windows Authentication), see the "Single Sign On and User Management" section on page 2-25.

Step 1 Select **File > Logon**.



The **Logon** window appears.

Step 2 Select your login account from the **User Name** field.

Step 3 Enter the corresponding password from the **Password** field.

Step 4 Click **Logon**.

Viewing and Updating Your License Key

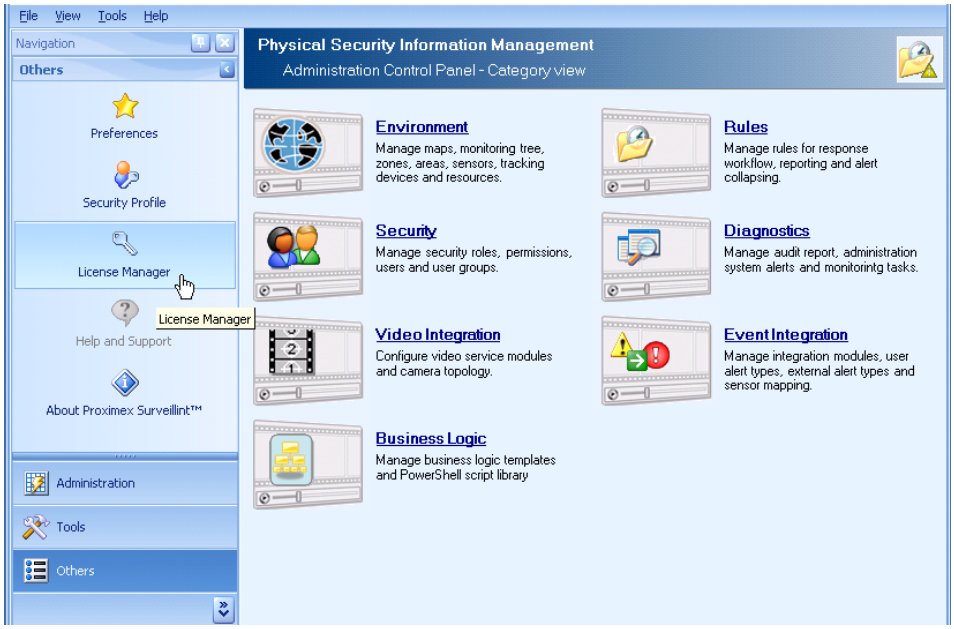
Your PSOM license key controls access to the Administration Console, Operation Console, EZ-Track functionality, and other key features. Your license key may, or may not, have an expiration date depending upon the product purchased.

The license key is a 25-character string.

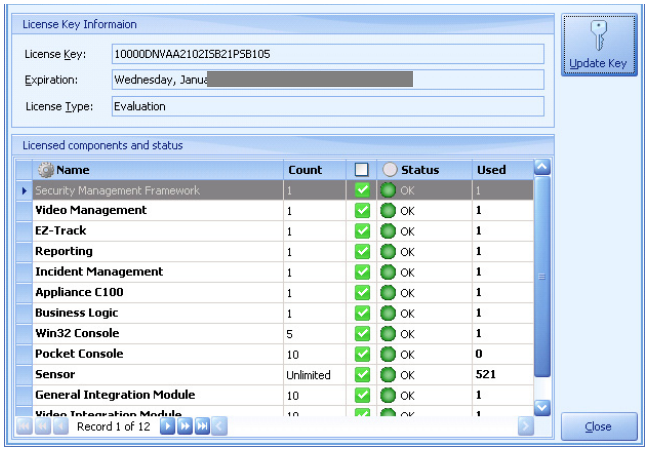
To view your license key:

Step 1 Click **Others** in the Navigation pane.

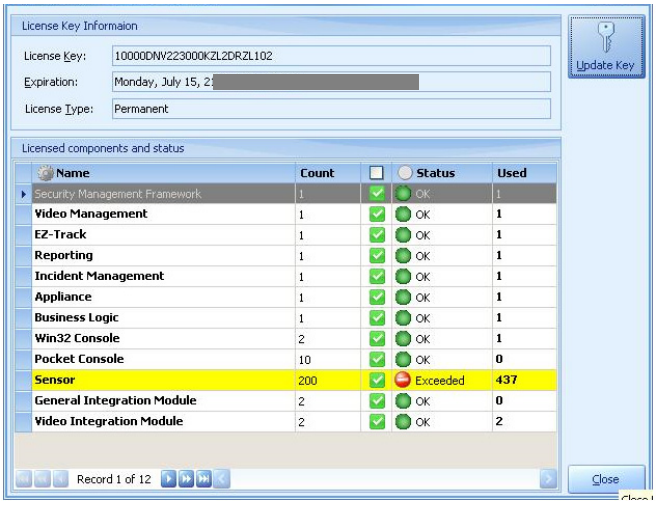
Step 2 Click **License Manager** in the Navigation pane.



The PSOM License Manager appears.



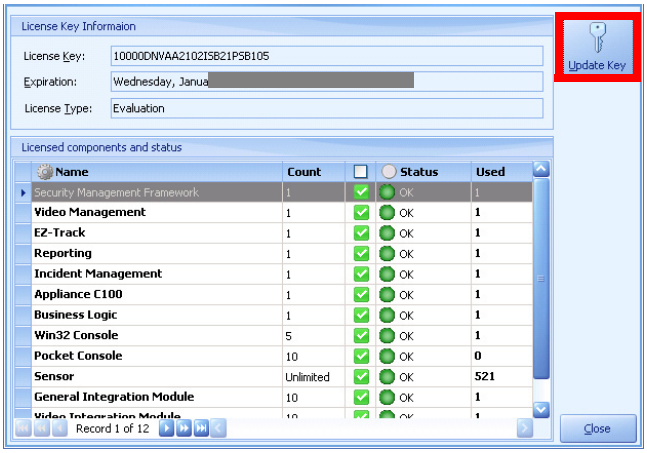
If you have exceeded your license requirement for an item, it appears highlighted in the list.



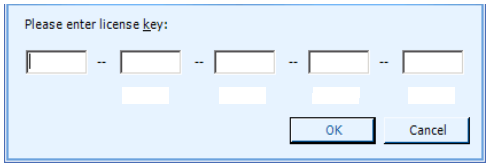
To update your license key:

Step 1 Click **Others** and then **License Manager** in the Navigation pane.

Step 2 Click the **Update Key** button.



The PSOM License Key window appears.



Type in your license key in the fields provided and click **OK**.

Setting Preferences

PSOM Administration Console has a number of preferences you can set including:

- Console—These control preferences for the Operation Console. Refer to the *Using Cisco Physical Security Operations Manager* guide for information.
- Server—These control preferences for the Administration Console, and for the Operation Console.

Table 1-3 describes the Server preferences from the Administration Console.

Table 1-3 Server Preferences that You can Set from the Administration Console

Server preference	See:
How long PSOM stores auditing information.	"Setting How Long Audit Records are Stored by PSOM" section on page 16-9
The awareness level assigned to Homeland Security and MARSEC that appears in the Operation Console.	"Setting Homeland Security or MARSEC levels for the Operation Console" section on page 1-17
Whether strong passwords are required to access PSOM; and if so, whether they expire.	"Enforcing Strong Passwords in PSOM" section on page 2-22
How often alerts are refreshed in the Operation Console and whether different sounds are applied to different alerts.	"Setting Alert Preferences for the Operation Console" section on page 1-19
How frequently alerts are refreshed in the Alert Management Console.	"Setting Alert Preferences for the Alert Management Console" section on page 1-21
How frequently alerts are refreshed in the Alert Details window for Operation Consoles.	"Setting Alert Preferences for the Alert Details Window" section on page 1-22
What order monitoring zones and areas are listed in the Monitoring Hierarchy in PSOM Consoles.	"Setting the Order of the Monitoring Hierarchy" section on page 1-23
Where incident packages are stored by default when generated by operators using the Operation Console.	"Setting a Default Directory for Incident Packages" section on page 10-10
Whether task completion should be enforced in the Operation Console.	"Enforcing Task Completion in the Operation Console" section on page 8-19
What service to use for identity management.	"Identity Management in PSOM" section on page 2-27
How to stop video alert messages for Consoles that do not have video support.	"Stopping Video Alert Messages for Consoles without Video Support" section on page 1-24

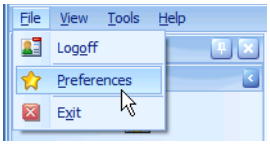
Setting Homeland Security or MARSEC levels for the Operation Console

The Operation Console displays the current Homeland Security or MARSEC level at the bottom right corner of the window.

You can manually set these levels for the Operation Console from the Administration Console.

To set the Homeland Security or MARSEC levels:

Step 1 From the Administration Console, select **File > Preferences**.

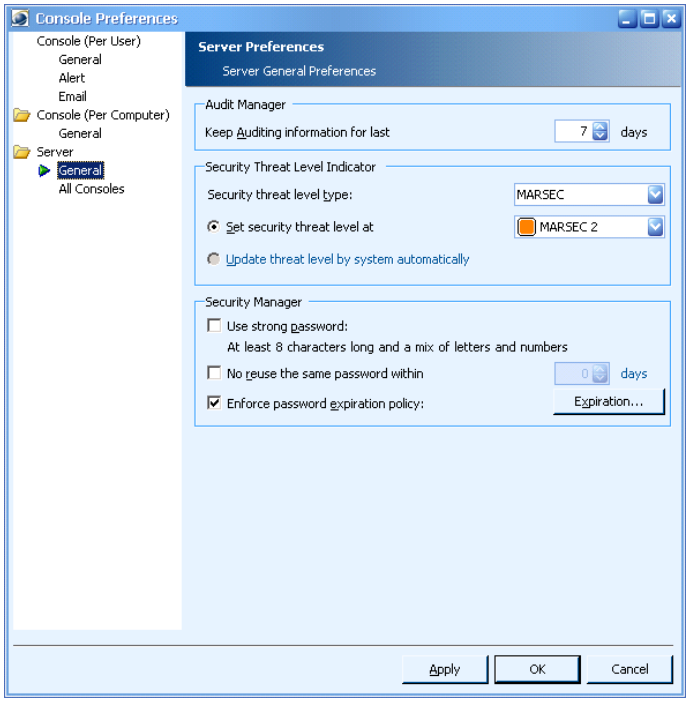


The Console Preferences window appears.

Step 2 Click **Server**.

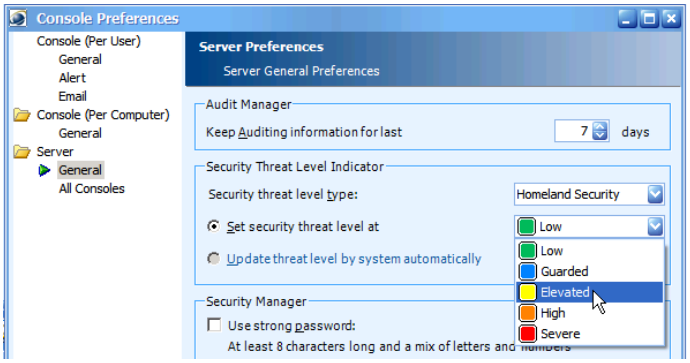
The Server preferences appear.

Step 3 In the Security Threat Level Indicator section, select the type of security threat you want to display in the Operation Console from the pull-down menu: **Homeland Security** or **MARSEC**.

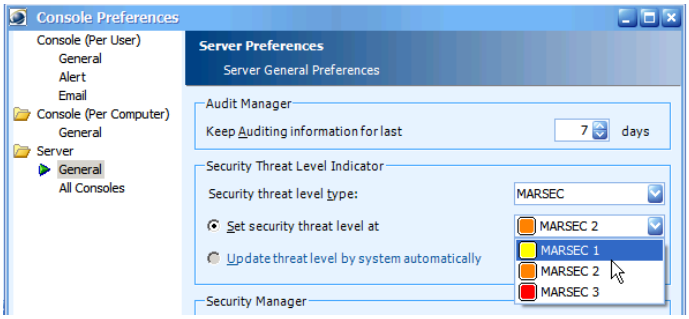


Step 4 From the **Set security threat level at** field, select a level.

For Homeland Security, the choices are: Low, Guarded, Elevated, High or Severe.



For MARSEC, the choices are: MARSEC 1, MARSEC 2 or MARSEC 3.



Step 5 Click **OK** to apply your settings.

Note For MARSEC, the levels roughly correlate to Homeland Security in this way:

- MARSEC 1—Routine maritime operations; this level aligns with Green, Blue and Yellow Homeland Security levels.
- MARSEC 2—Heightened security awareness; this level aligns with the Orange Homeland Security level.
- MARSEC 3—Imminent threats to security; this level aligns with the Red Homeland Security level.

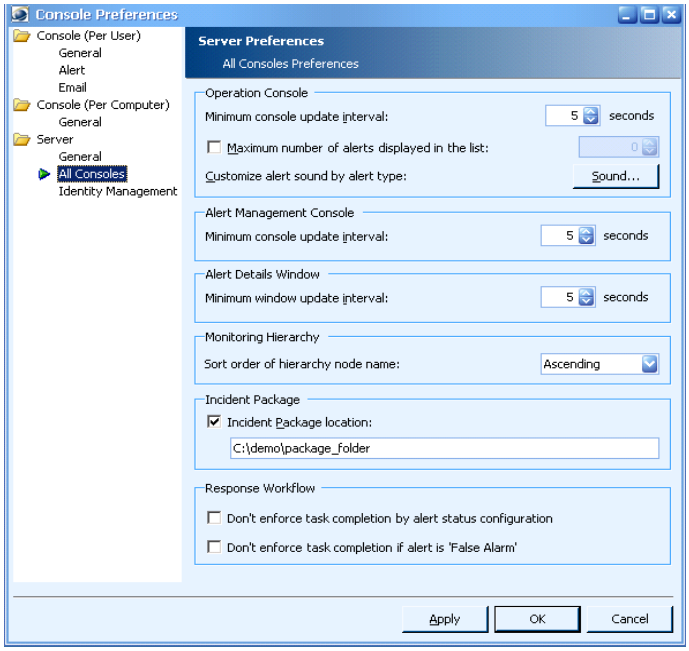
Setting Alert Preferences for the Operation Console

You can set alert preferences that apply to all Operation Consoles in the network from the Administration Console.

To set alert preferences for Operation Consoles:

Step 1 Select **File > Preferences** from the Administration Console.

Step 2 Click **All Consoles** under **Server** in the left navigation pane.

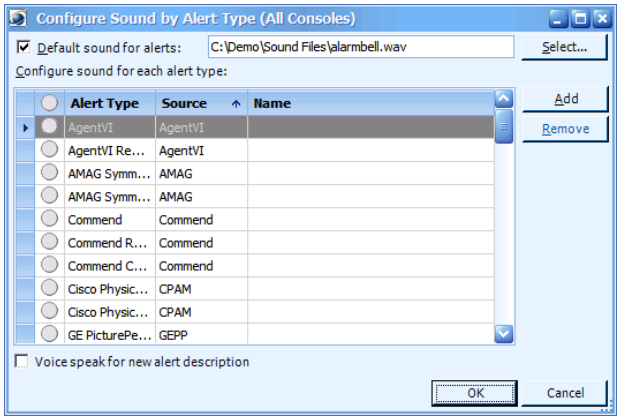


Step 3 Enter the interval at which alert information should be refreshed in the Operation Console in the **Minimum console update interval** field.

Step 4 If you want to limit the number of alerts that are displayed in the Alert Pane in the Operation Console, check the **Maximum number of alerts displayed in the list** option and enter a number in the field provided.

Step 5 If you want to associate a sound with a specific alert type, click the **Sound** button.

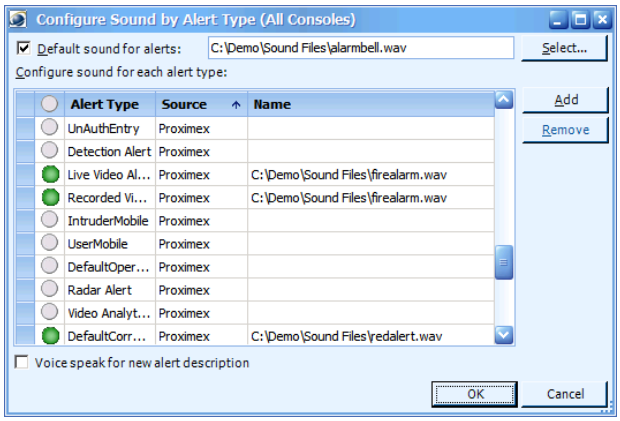
The Configure Sound by Alert Type window appears.



Step 6 To play a default sound for all alerts, check the **Default sound for alerts** option and click **Select**. Navigate and select the audio file you want played for all alerts.

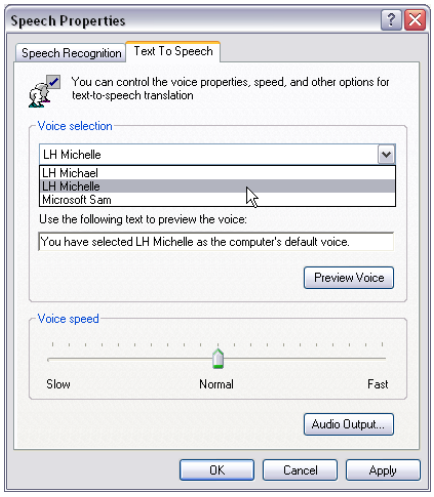
Step 7 To associate a sound with a specific type of alert, select the alert in the window and click **Add**. Navigate and select the audio file you want played for the specific alert. The sound file is now listed next to the selected alert.

Note Sound files need to be installed in the same folder across the machines where PSOM Operation Console will be running, or in a shared folder that all of these machines can access.



Step 8 If you want to have Microsoft Windows' speech functionality read alert descriptions—for example, "Alert! 'Suspect did not pass check point and disappear' at 'T2E-SecondFloorMain' Sensor 'P-108'"—then check the **Voice speak for new alert description** option.

You can configure the voice used to read the descriptions by clicking the **Speech** icon in the Control Panel in Windows. Click the **Text To Speech** tab and choose the voice you want to use from the **Voice selection** field.



Step 9 Click **OK**. Then click **Apply** or **OK** in the Console Preferences window.

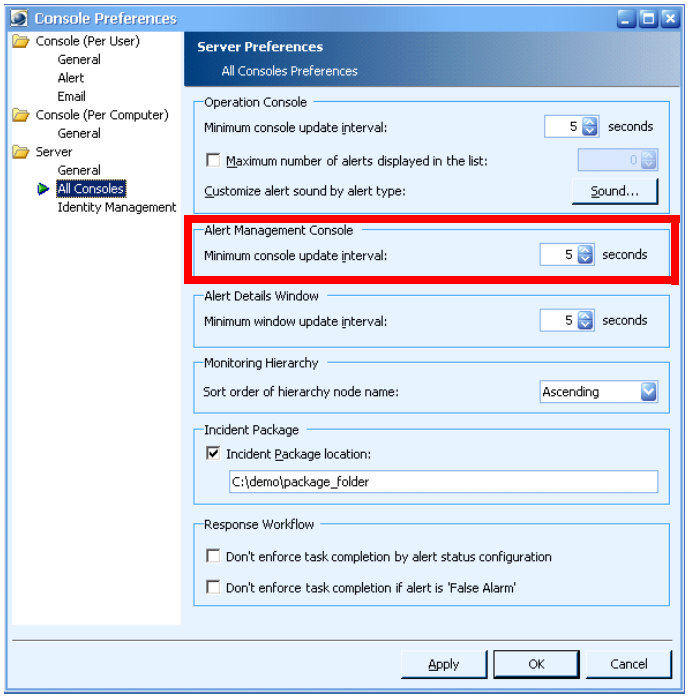
Setting Alert Preferences for the Alert Management Console

You can set preferences for the Alert Management Console.

To set alert preferences for the Alert Management Console:

Step 1 Select **File > Preferences** from the Administration Console.

Click **All Consoles** under **Server** in the left navigation pane.



Step 2 Enter the interval at which alert information should be refreshed in the Alert Management Console in the **Minimum console update interval** field.

Step 3 Click **OK**.

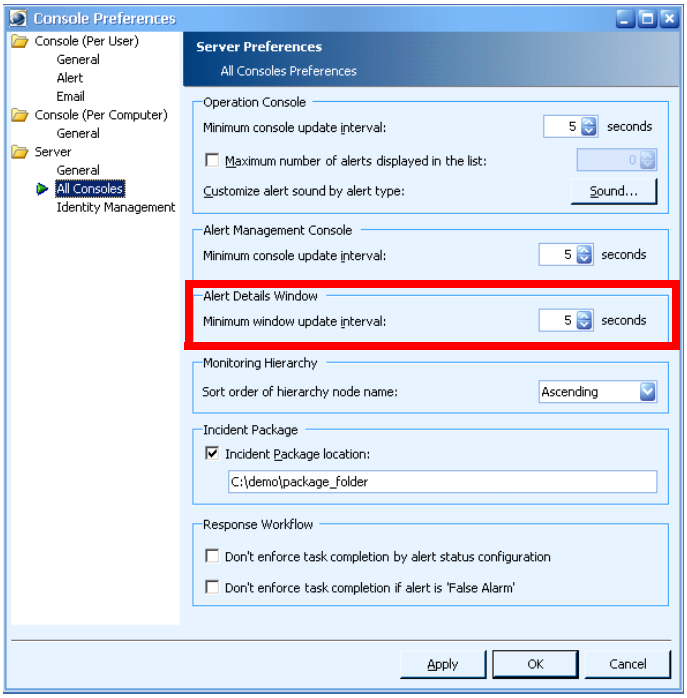
Setting Alert Preferences for the Alert Details Window

You can set preferences for the Alert Details window in all Operation Consoles.

To set alert preferences for the Alert Details:

Step 1 Select **File > Preferences** from the Administration Console.

Step 2 Click **All Consoles** under Server in the left navigation pane.



Step 3 Enter the interval at which alert information should be refreshed in the Alert Details window in the **Minimum window update interval** field.

Step 4 Click **OK**.

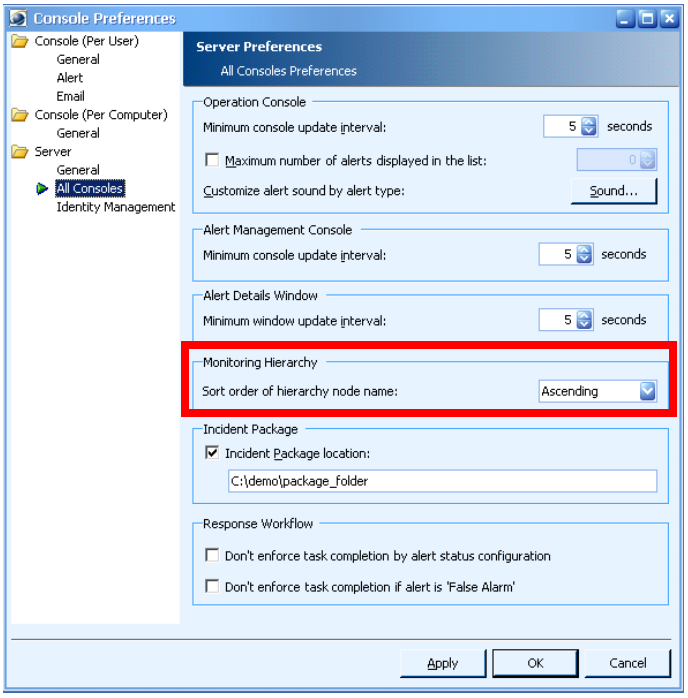
Setting the Order of the Monitoring Hierarchy

You can set the order in which node names appear in the Monitoring Hierarchy across all Consoles.

To set the order of the Monitoring Hierarchy:

Step 1 Select **File > Preferences** from the Administration Console.

Step 2 Click **All Consoles** under **Server** in the left navigation pane.



Step 3 Select the order in which you want node names to appear in the Monitoring Hierarchy from the **Sort order of hierarchy node name** field.

Step 4 Click **OK**.

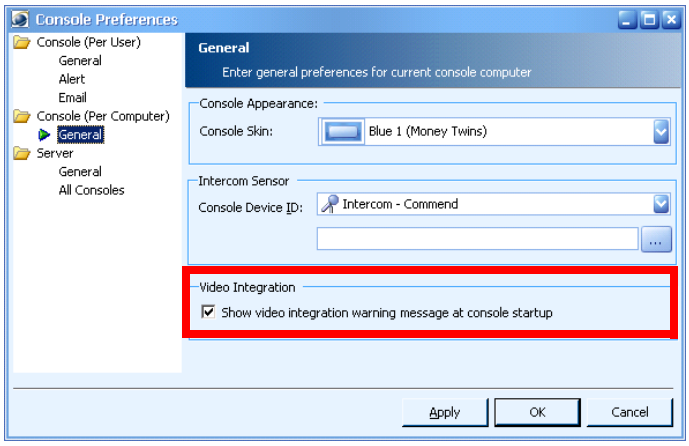
Stopping Video Alert Messages for Consoles without Video Support

If the Operation Console does not need to use video-related features, you can set an option to turn off video alert messages at startup.

To set video alert preferences for the Operation Console:

Step 1 Select **File > Preferences** from the Alert Management Console.

Step 2 Click **General** under Console (Per Computer) in the left navigation pane.



Step 3 To turn off video alert messages, deselect the **Show video integration warning message at console startup** option.

Step 4 Click **OK**.

Starting and Stopping Services

When a system is restarted, Services are configured to restart automatically. However, in cases where the services need to be manually restarted follow the instructions in this section.

There are five services for PSOM:

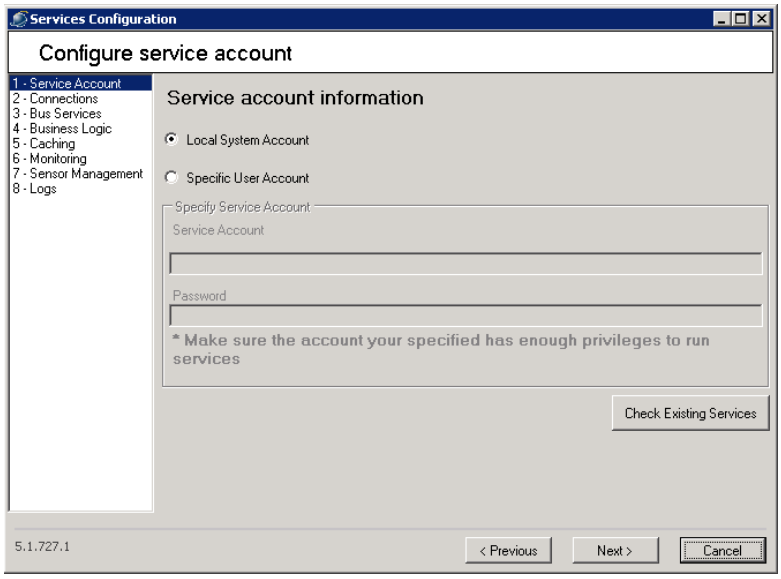
- PSOM Bus Services
- PSOM Business Logic Core Services
- PSOM Caching Services
- PSOM Monitoring Logic Services
- PSOM Sensor Management Services

These services are listed in the Windows Services dialog box.

To restart PSOM Services:

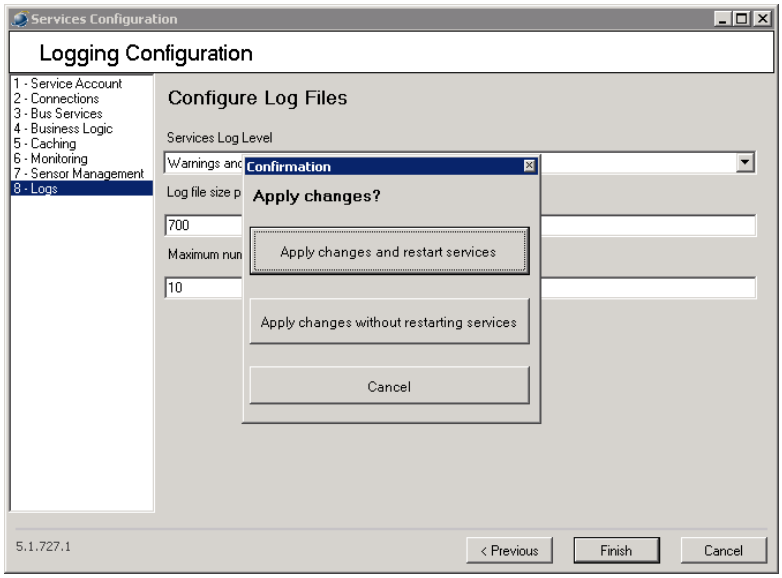
Step 1 From the Start menu, select **All Programs > Cisco Physical Security Operations Manager Services > Services Configuration**.

The **Services Configuration** window appears.



Step 2 Select **8 - Logs** in the left side of the window.

Step 3 Click **Finish**.



Step 4 Click **Apply changes and restart services**. The PSOM Services restart and a confirmation window appears.

Step 5 Click **Finish**.

CHAPTER 2

Defining Users and Managing User Groups

This chapter describes how to set up user accounts and assign them to user groups so that operators can access the Operation Console, Administration Console, Alert Management Console, Video Management Console, or Business Logic Designer.

This chapter includes these topics:

- Managing Users, page 2-1
- Viewing Users by Role, page 2-8
- Managing User Groups, page 2-12
- Permissions Within PSOM, page 2-20
- Enforcing Strong Passwords in PSOM, page 2-22
- Single Sign On and User Management, page 2-25
- Identity Management in PSOM, page 2-27

Managing Users

Before users can login to PSOM, they must have a user account. Administrators are responsible for:

- Creating new *user* accounts.
- Granting users certain privileges by assigning them a user *role*.
- Assigning users to different *user groups* that can be used for escalation of tasks or enforce access scope (e.g., limit the monitoring zones that certain users can access).
- Changing user passwords. (Users can also change their own passwords from the Security Profile window of any console.)
- Removing users from PSOM.

Types of User Roles

There are these user *roles* in PSOM:

- Operators—These users can access the Operation Console, and Video Management Console, or Alert Management Console. These users cannot access the Administration Console or Business Logic Designer.

- Power Users—These users can access a limited scope within any console. Power users cannot add, edit or delete administrator users.
- Administrators—These users can access everything within all consoles. This allows them to perform the same actions as operators, as well as create, configure, modify and view the entire PSOM system.
- Video Viewers—These users can access the Video Management Console only. This allows them to navigate the monitoring zones and areas within the environment and view surveillance videos from video sensors.

Note You cannot edit or delete these user roles.

You can add new user roles to PSOM. See the "Permissions Within PSOM" section on page 2-20.

Planning a PSOM User Deployment

When you are initially deploying PSOM within your organization, it is helpful to make a list of all users that need to be added to PSOM. For each of these users, assign them user names, passwords, roles and user groups. Table 2-1 shows a sample user deployment.

Note Appendix A, "Planning Worksheets," provides a planning table you can use for your planning efforts—Table A-2 on page A-3.

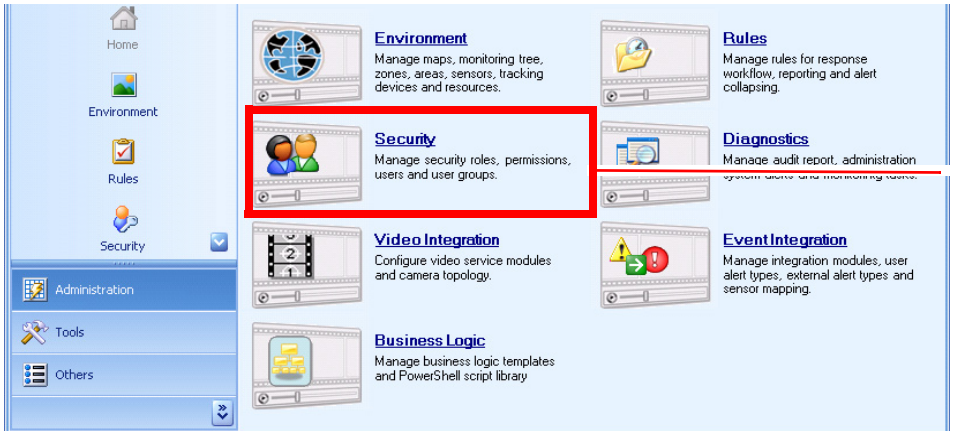
Table 2-1 Sample User Deployment Planning

Employee	User Name	Password	User Role	User Group
Operator	Operator	******	Operator	Management
Supervisor1	Supervisor1	******	Power User	Dayshift
Supervisor2	Supervisor2	******	Power User	Nightshift

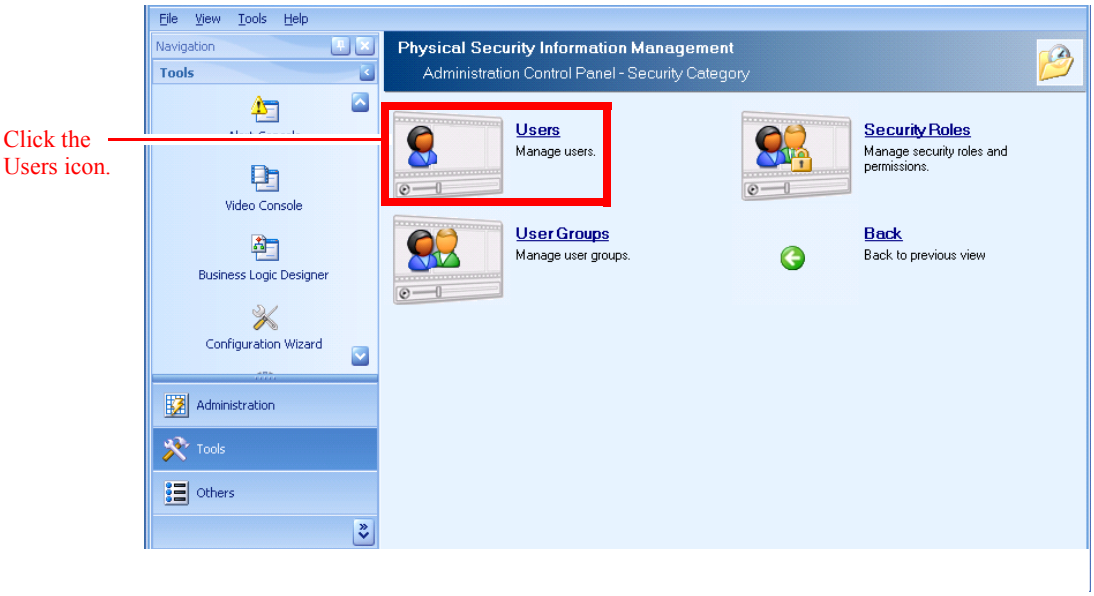
Setting Up User Accounts

To add a user account:

Step 1 Click the **Security** icon in the Administration Console.

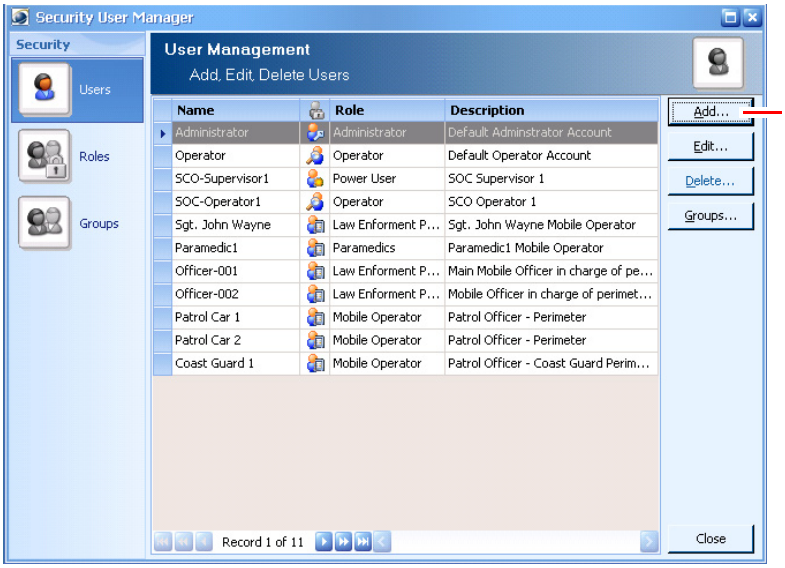


The **Security** window appears.



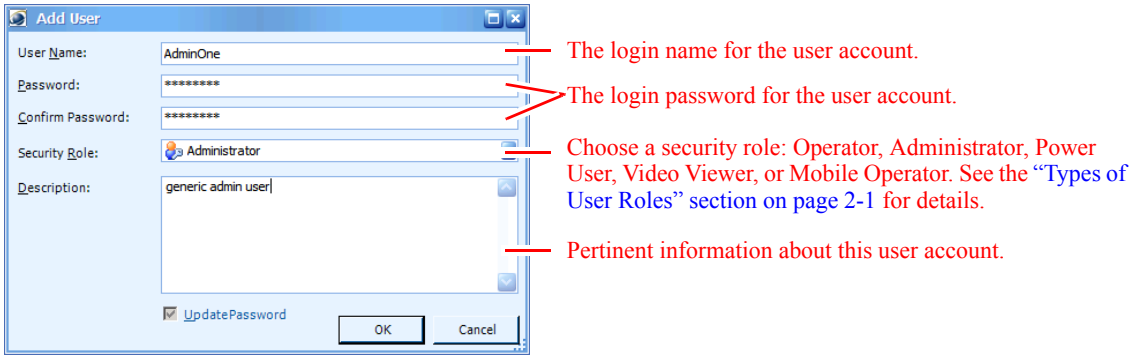
Step 2 Click the **Users** icon.

The **Security User Manager** window appears with the **Users** tab selected.



Step 3 Click the **Add** button to create a new user account.

The Add User window appears.



Step 4 In the **User Name** field, enter the name you want to assign to the user account. If you're using single sign on, you click the ... button and select the user from Active Directory. See the "Single Sign On and User Management" section on page 2-25.

Step 5 In the **Password** and **Confirm Password** fields, enter the password for the account. If you're using single sign on, these fields are greyed out. See the "Single Sign On and User Management" section on page 2-25.

Step 6 From the **Security Role** field, select the security role you want to assign to this account: **Administrator**, **Power User**, **Video Viewer**, **Operator**, **Paramedics**, **Law Enforcement Personnels**, or **Mobile Operator**.

See "Types of User Roles" section on page 2-1 for details.

Step 7 In the **Description** field, enter any notes about this user that are needed.

Step 8 Click **OK** to save the user account to the database.

Once saved, the entry is displayed in the Security User Manager window.

Changing a User Password or Security Role

You can edit a user's password or security role from the Security User Manager.

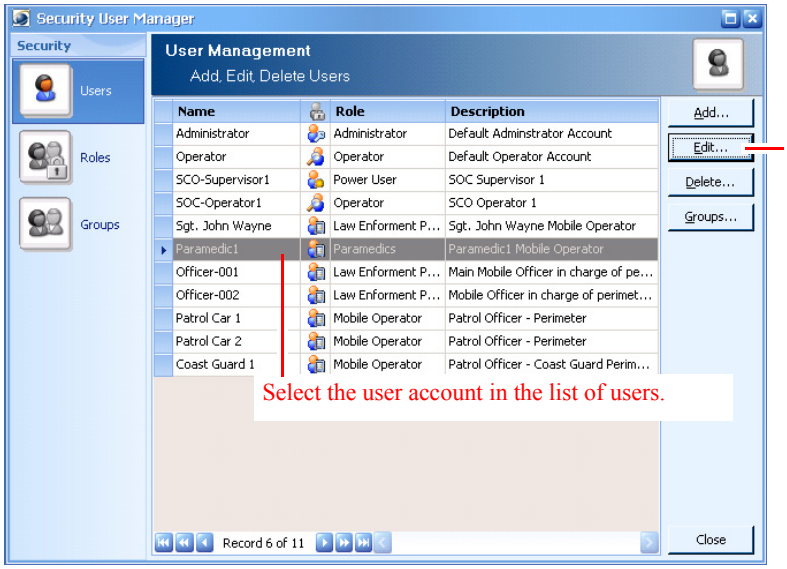
Note Users can also change their own passwords from the Security Profile window of any console.

To change a user's password or security role:

Step 1 Click the **Security** icon in the Administration Console.

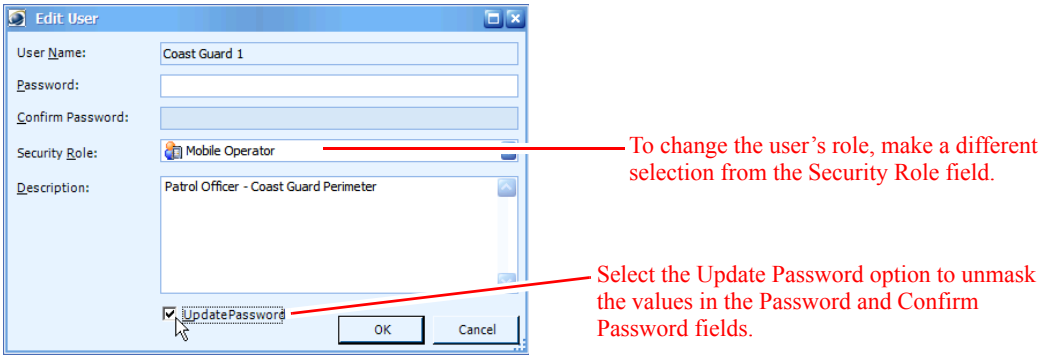
Step 2 Click the **Users** icon.

The Security User Manager window appears with the **Users** tab selected.



Step 3 Select the user account you want to change in the list, and click the **Edit** button.

The Edit User window appears.



Step 4 To change the user's security role, make a different selection from the **Security Role** field.

Step 5 To change the user's password:

a. Check the **Update Password** option to unmask the **Password** and **Confirm Password** fields.

b. Enter the new password into the **Password** and **Confirm Password** fields.

Step 6 Click **OK** to store the new password or security role to the database.

Changing the Name Assigned to a User

For this release, you cannot change the name assigned to a user account once it has been created. To change the name of a user account, you must delete the user account and then recreate it using the preferred name.

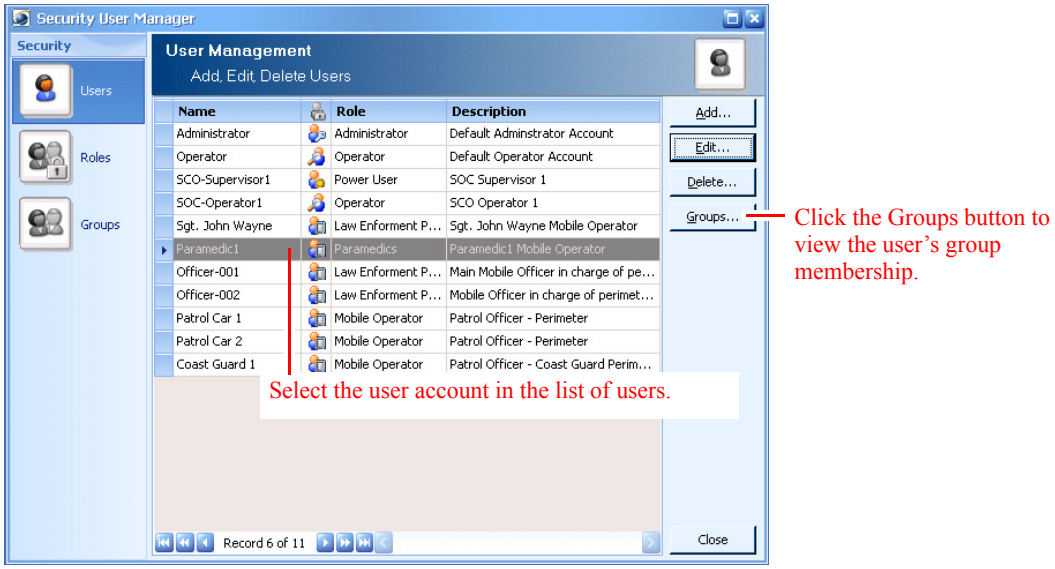
Viewing the Groups to which a User Belongs

To view a user's group membership:

Step 1 Click the **Security** icon in the Administration Console.

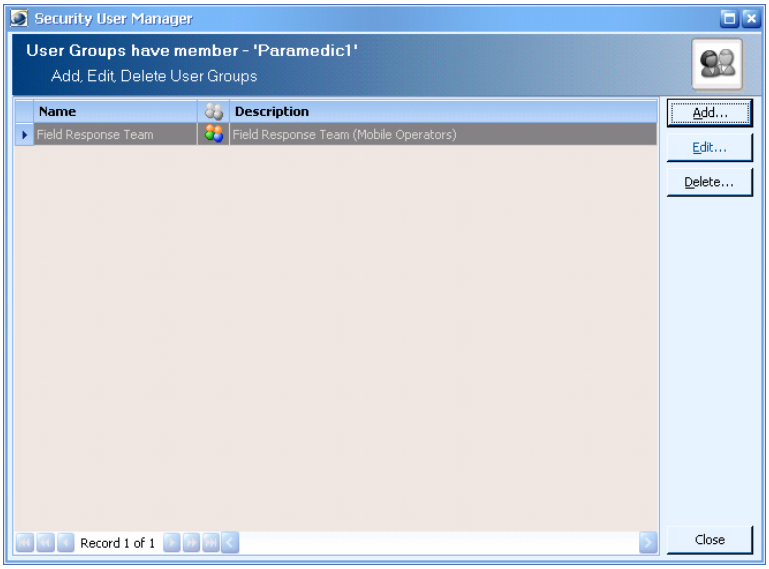
Step 2 Click the **Users** icon.

The Security User Manager window appears with the **Users** tab selected.



Step 3 Select the user account from the list, and click the **Groups** button.

The User Groups window appears displaying all the groups to which the selected user belongs.



Step 4 Click **Close** when you are finished.

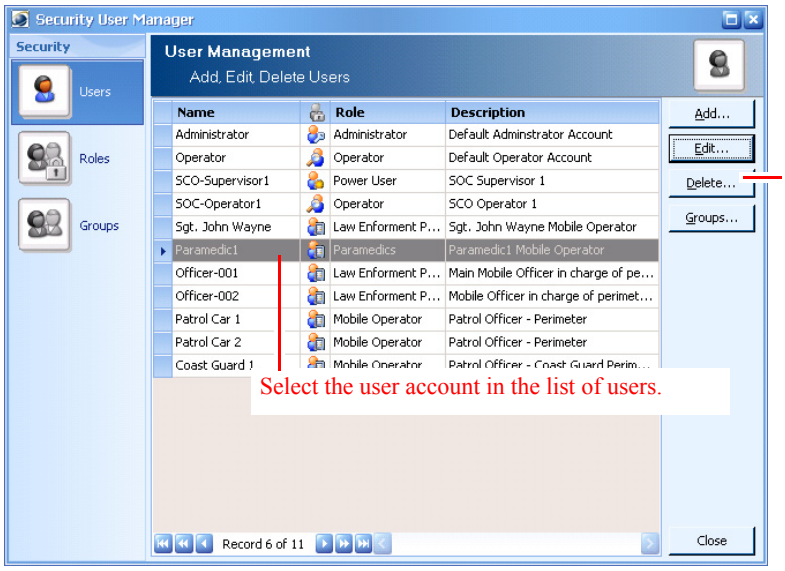
Removing a User from PSOM

To delete a user account:

Step 1 Click the **Security** icon in the Administration Console.

Step 2 Click the **Users** icon.

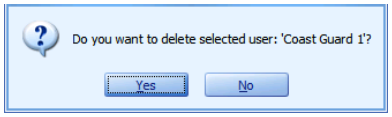
The Security User Manager window appears with the **Users** tab selected.



Step 3 Select the user account in the list of users.

Step 4 Click the **Delete** button.

A confirmation dialog box appears.



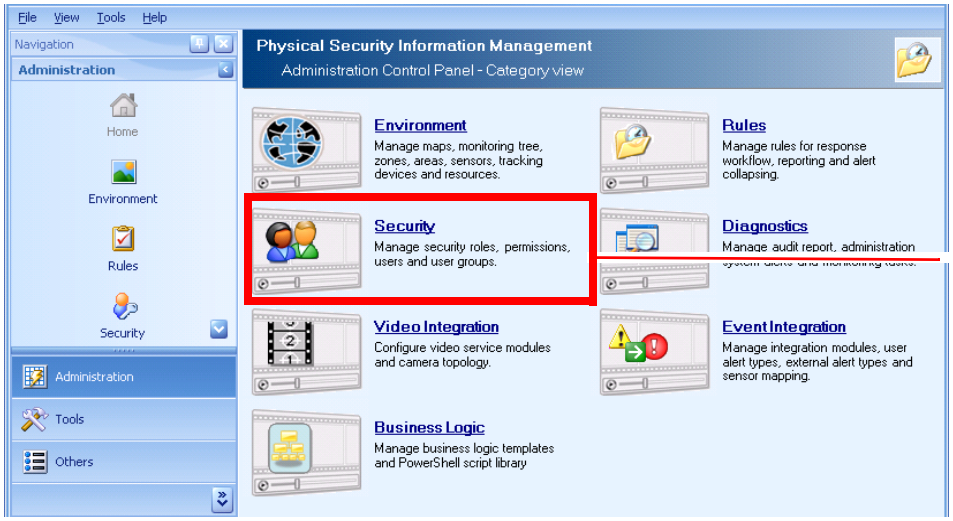
Step 5 Click **Yes** to permanently remove the user account from PSOM.

Viewing Users by Role

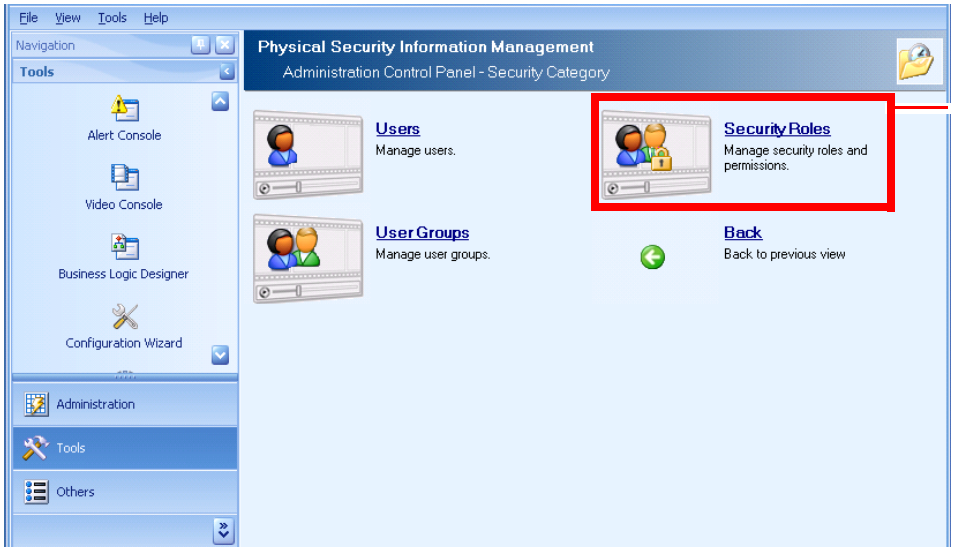
You can view all of the users with a particular role; for example, you can find out which users have been assigned the Administrator role. You can also view and change the permissions assigned to a role.

To view all users with a certain role:

Step 1 Click the **Security** icon in the Administration Console.

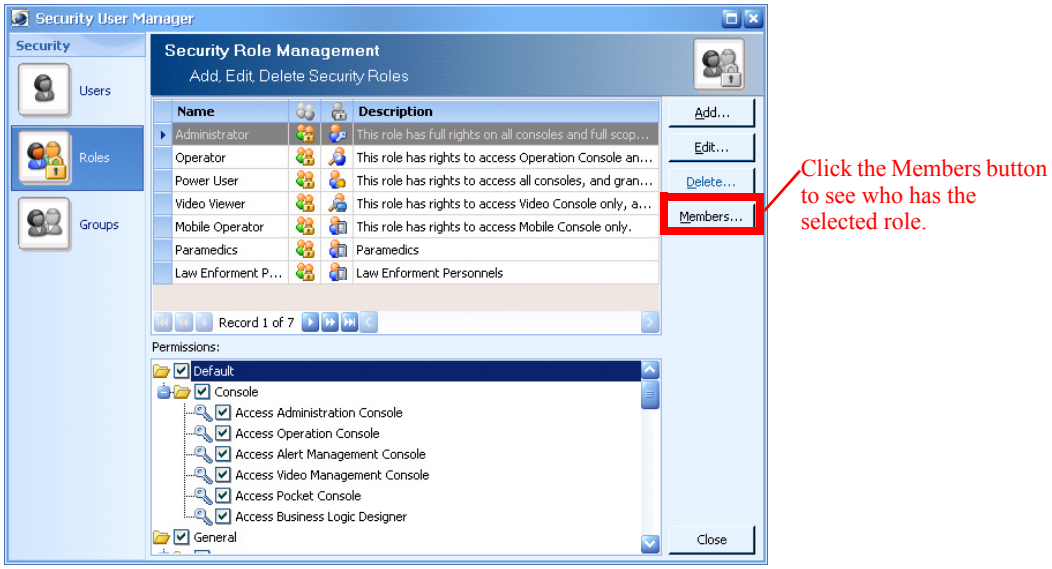


Step 2 The Security window appears.



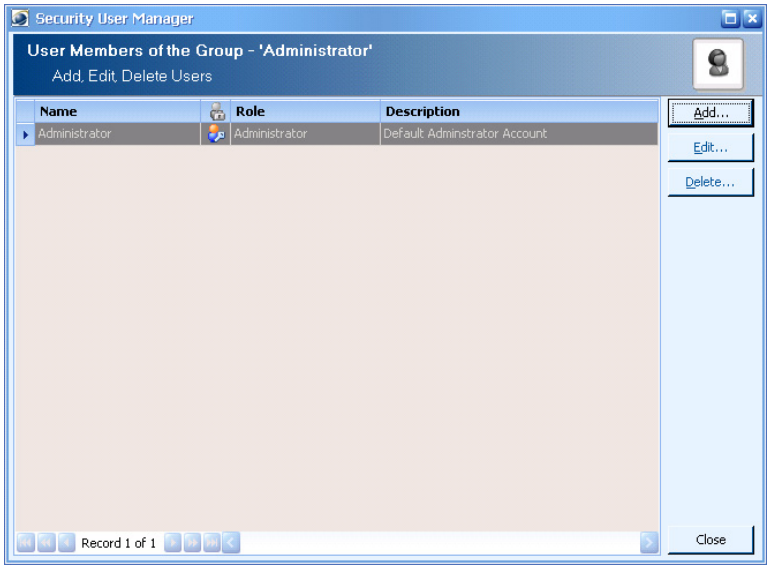
Step 3 Click the **Security Roles** icon.

The Security User Manager window appears with the **Roles** tab selected.



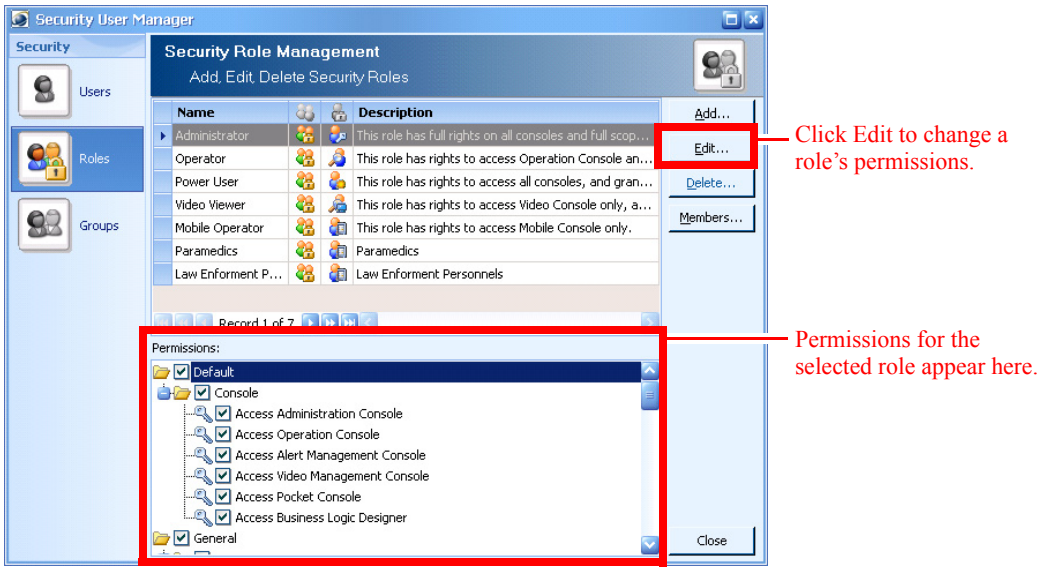
Step 4 To see which users belong to a role, select a user role from the list and click the **Members** button.

The User Members window appears.

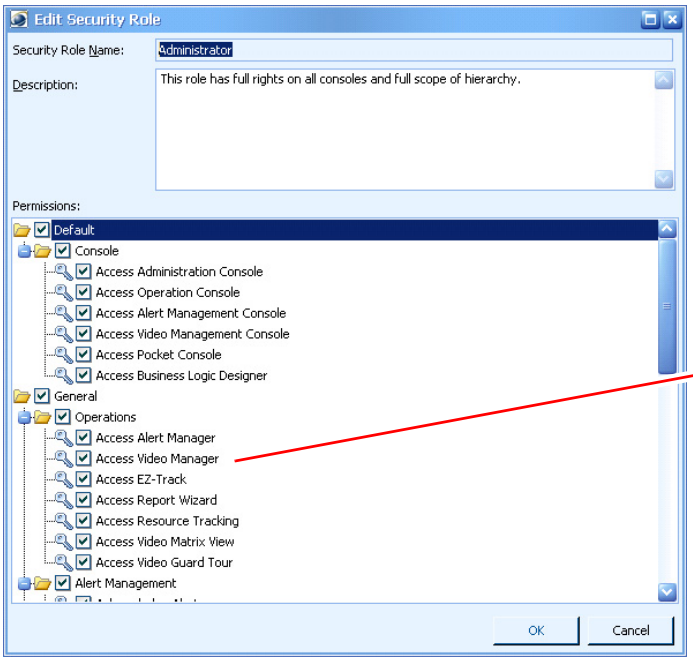


Click **Close** when you are finished.

Step 5 To see the permissions assigned to a user role, look in the lower half of the Security User Manager window.

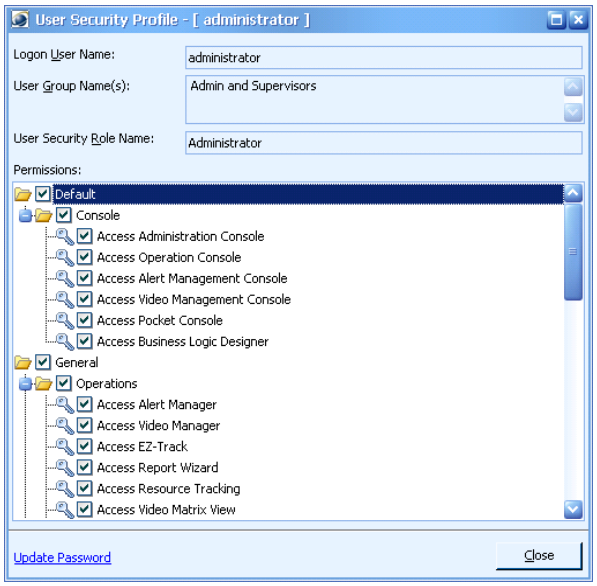


Step 6 To change permissions assigned to a user role, select the role in the list and click **Edit**. The Edit Security Role window appears.



Note Check or uncheck individual permissions under the **Permissions** area. Click **OK** when finished. See the "Permissions Within PSOM" section on page 2-20 for information about the different permissions.

Note You can view your security permissions (for the login account you are currently using) by clicking **Others** and then **Security Profile** in the Navigation Pane of the Administration Console.



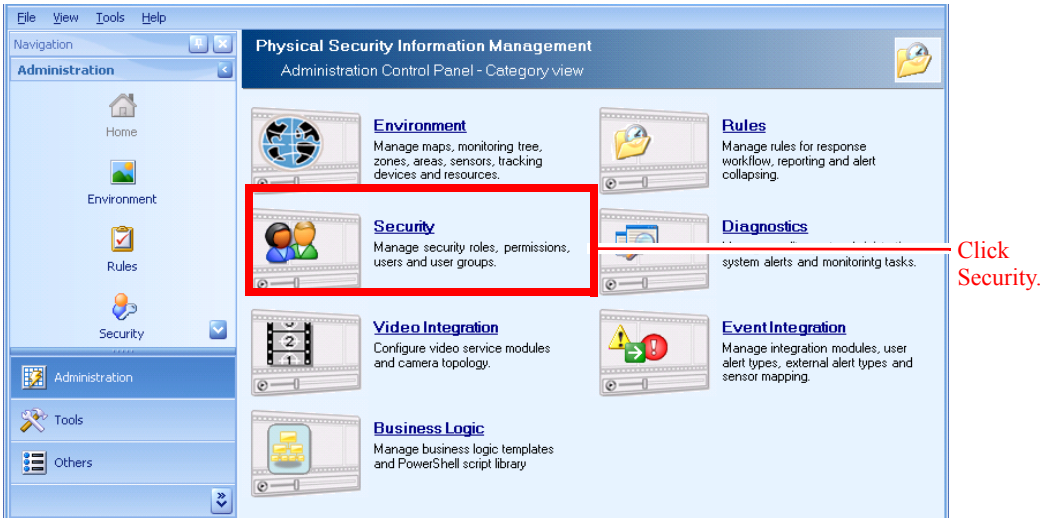
Managing User Groups

You can create as many different user groups as you need to represent the functional operations of your security team, and then assign users to be members of these groups. User groups are useful with escalation of tasks within PSOM; for example, you can define a Supervisor group to whom alerts are escalated when they are not handled within the designated time frame. User groups are also useful for limiting the scope of access for certain users to specific monitoring zones or areas.

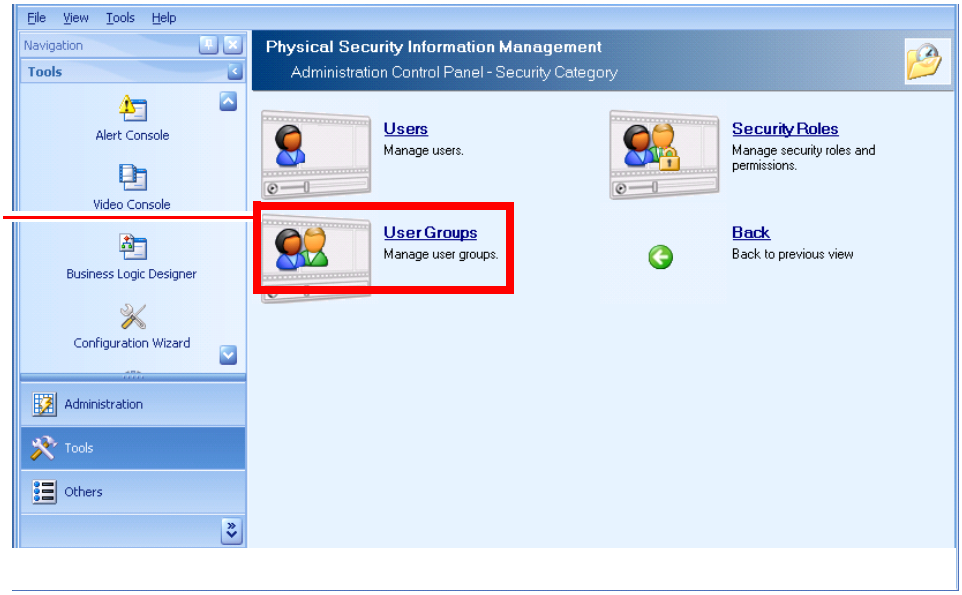
Creating a User Group

To create a new user group:

Step 1 Click the **Security** icon in the Administration Console.

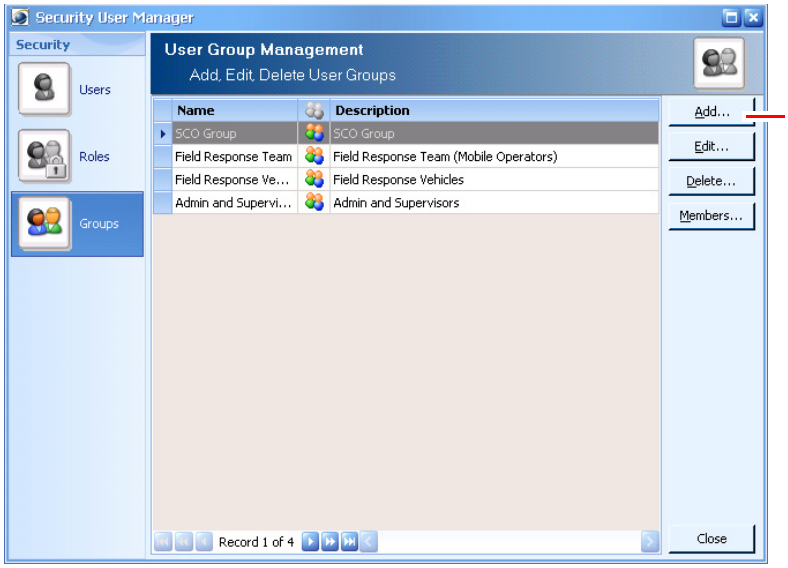


The Security window appears.



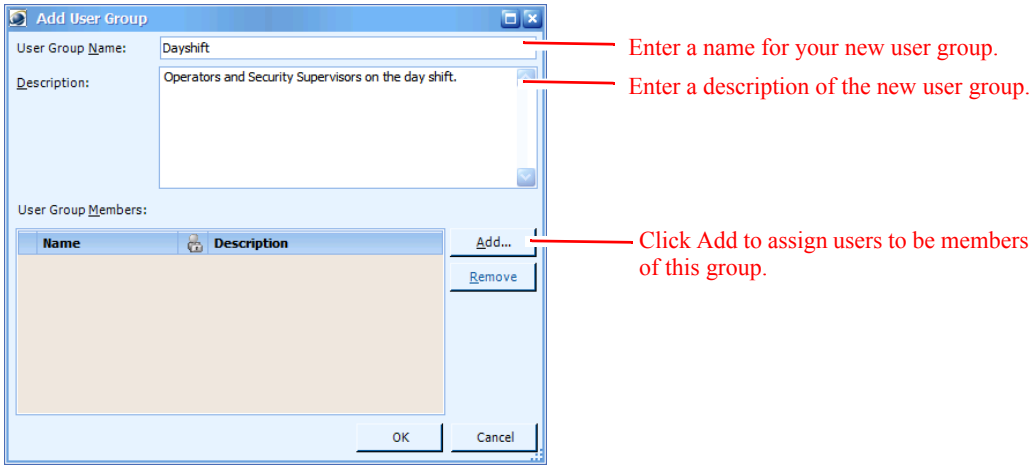
Step 2 Click the **User Groups** icon.

The Security User Manager window appears with the **Groups** tab selected.



Step 3 Click the **Add** button to create a new user group.

The **Add User Group** window appears.

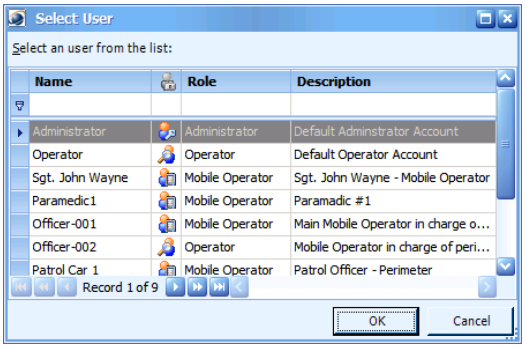


Step 4 In the **User Group Name** field, enter a name for this new user group.

Step 5 In the **Description** field, enter information about this user group.

Step 6 Click the **Add** button to assign users to be members of this new group.

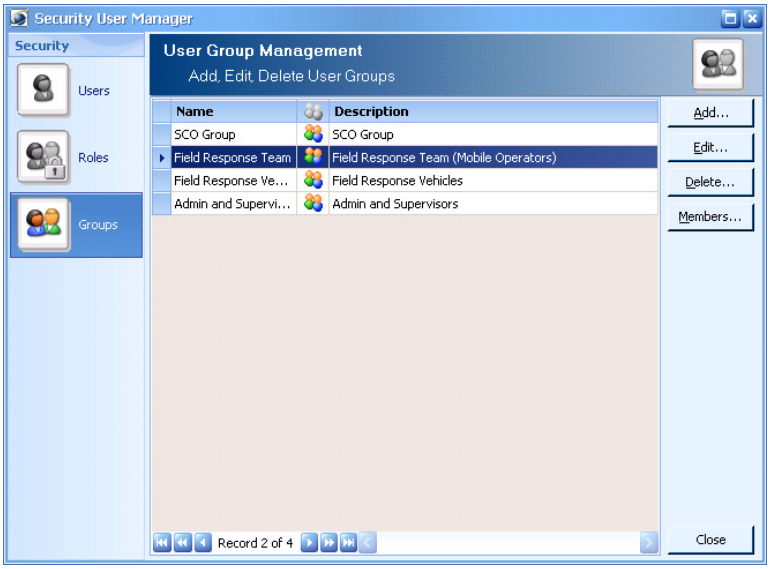
The Select User window appears.



Step 7 Select the users that should be members of this group. Use CTRL-click or SHIFT-click to select multiple users.

Step 8 Click **OK**.

The Add User Group window shows your new user group.



Step 9 Click **OK** to save your new group.

Editing a User Group

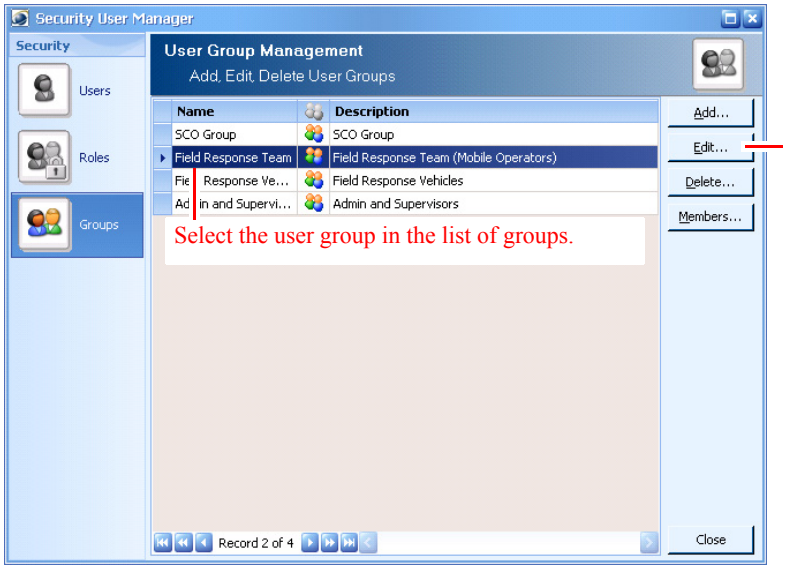
To edit a user group:

Step 1 Click the **Security** icon in the Administration Console.

The Security window appears.

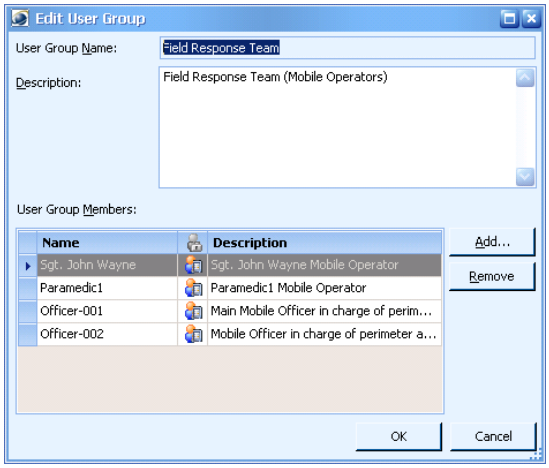
Step 2 Click the **User Groups** icon.

The Security User Manager window appears with the **Groups** tab selected.



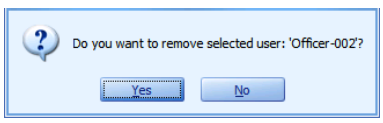
Step 3 Select the user group you want to change, and click the **Edit** button.

The Edit User Group window appears.



Step 4 To change the description of the group, change the text in the **Description** field.

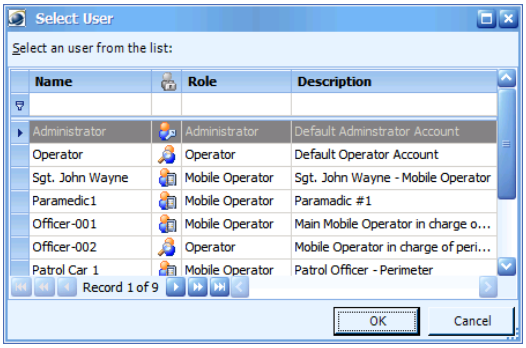
Step 5 To remove a member from the group, select the member in the list under **User Group Members**, and click the **Remove** button. A confirmation appears.



Click **Yes** to remove the user.

Step 6 To add more members to the group, click the **Add** button.

The Select User window appears.



a. Select the users that should be members of this group. Use CTRL and SHIFT to select multiple users.

b. Click **OK**.

Step 7 Click **OK** to save your changes to the user group.

Managing the Members of a User Group

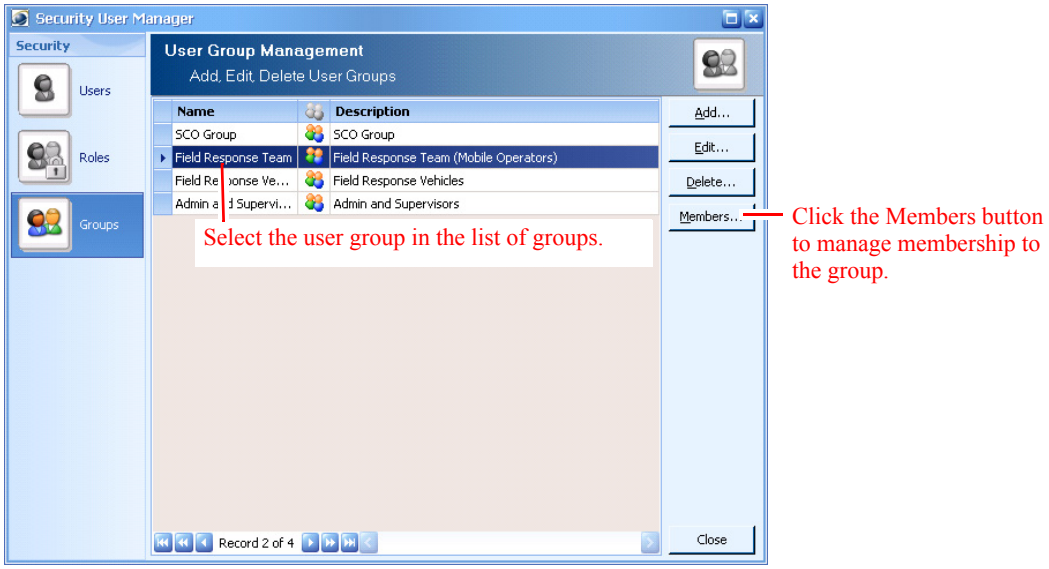
To manage the members of a user group:

Step 1 Click the **Security** icon in the Administration Console.

The Security window appears.

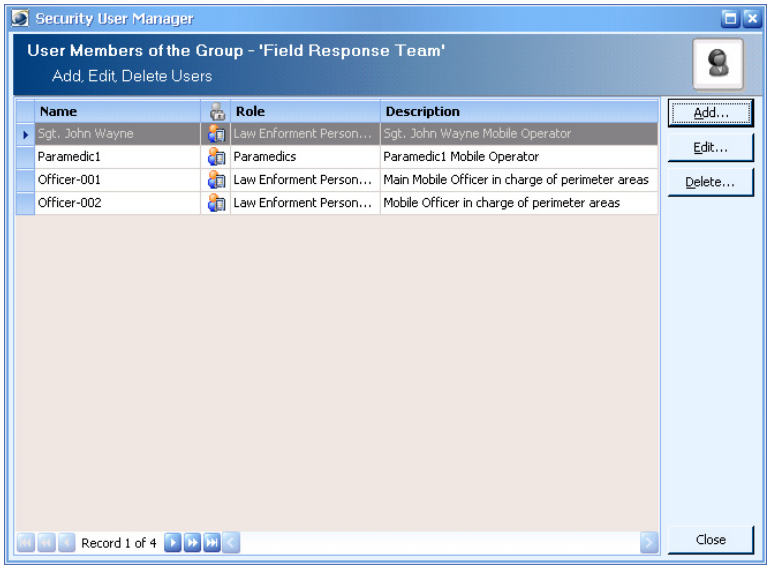
Step 2 Click the **User Groups** icon.

The Security User Manager window appears with the **Groups** tab selected.



Step 3 Select the user group for which you want to manage membership, and click the **Members** button.

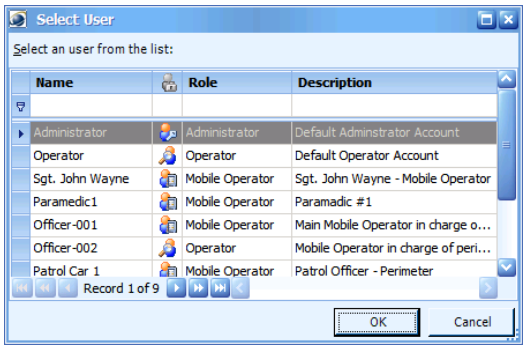
The User Members window appears.



Step 4 To add more members to this group:

a. Click the **Add** button.

The **Select User** window appears.



b. Select the users that should be members of this group. Use CTRL and SHIFT to select multiple users.

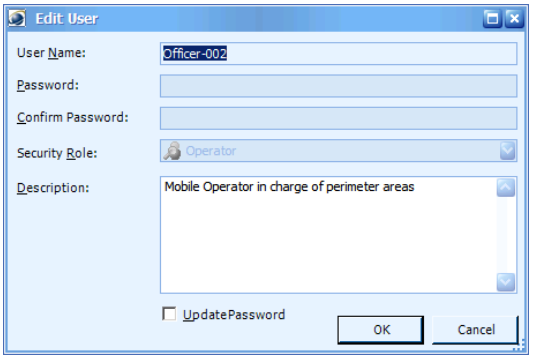
c. Click **OK**.

Step 5 To edit a member's information:

a. Select the member from the list.

b. Click the **Edit** button.

The Edit User window appears.



c. Enter new information in the **Description** field.

d. To change the user's password, check the **Update Password** field and enter the password into the **Password** and **Confirm Password** fields.

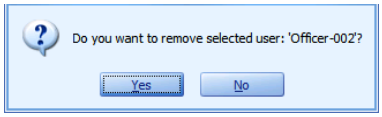
e. Click **OK**.

Step 6 To remove a member from the group:

a. Select the member from the list.

b. Click the **Delete** button.

A confirmation dialog box appears.



c. Click **Yes** to remove the user.

Step 7 Click **Close**.

Deleting a User Group

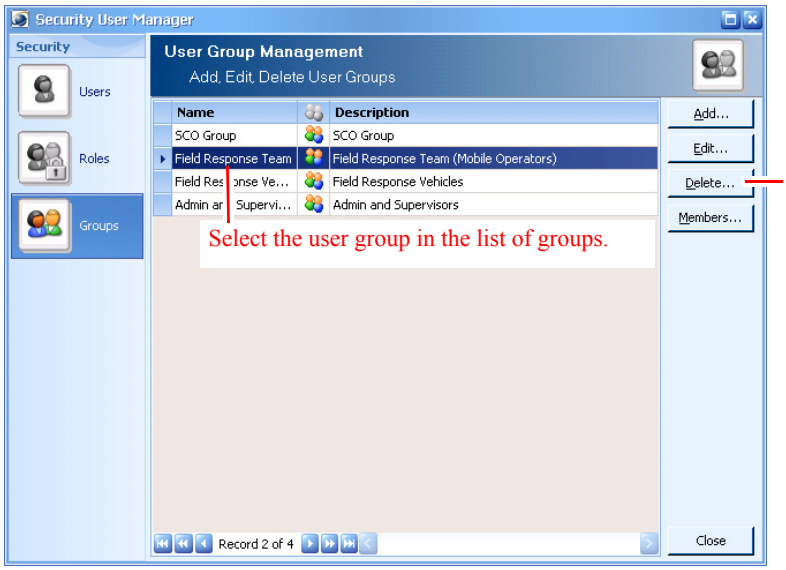
To delete a user group:

Step 1 Click the **Security** icon in the Administration Console.

The Security window appears.

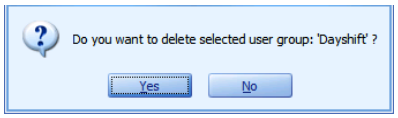
Step 2 Click the **User Groups** icon.

The Security User Manager window appears with the **Groups** tab selected.



Step 3 Select the user group you want to change, and click the **Delete** button.

A confirmation dialog box appears.



Step 4 Click **Yes** to delete the group.

Permissions Within PSOM

Within PSOM, users have permissions to perform certain actions. Table 2-2 describes the permissions that the Permissions area of the Roles tab in the Security Role Management shows.

Table 2-2 Permissions in Security Role Management

Area	Permission	Description
Console	Access Administration Console	Whether the user can launch the Administration Console.
	Access Operation Console	Whether the user can launch the Operation Console.
	Access Alert Management Console	Whether the user can launch the Alert Management Console.
	Access Video Management Console	Whether the user can launch the Video Management Console.
	Access Business Logic Designer	Whether the user can launch the Business Logic Designer.

Table 2-2 Permissions in Security Role Management (continued)

Area	Permission	Description
Operations	Access Alert Manager	Whether the user can launch the Alert Manager to view current alerts in PSOM.
	Access Video Manager	Whether the user can launch the Video Manager to view video.
	Access EZ-Track	Whether the user can perform actions using EZ-Track.
	Access Report Wizard	Whether the user can access or run reports.
	Access Resource Tracking	Whether the user can track resources.
	Access Video Matrix View	Whether the user can view video matrixes in the Video Management Console.
	Access Video Guard Tour	Whether the user can view guard tours in the Video Management Console.
Alert Management	Acknowledge Alert	Whether the user can acknowledge an open alert in PSOM.
	Close Alert	Whether the user can close an open or acknowledged alert in PSOM.
	Delete Alert	Whether the user can delete a closed alert.
	View Alert Details	Whether the user can view details for an alert.
	View Deleted Alerts	Whether the user can view details for a deleted alert.
	Print Alert Details	Whether the user can print alert details.
	Export Alert Details	Whether the user can export alert details from PSOM.
	Email Alert Details	Whether the user can email alert details.
	Add Notes to Alert Details	Whether the user can add notes to an alert's details.

Table 2-2 Permissions in Security Role Management (continued)

Area	Permission	Description
Video	Export Video	Whether the user can export recorded video from PSOM.
	Video Snapshot	Whether the user can take video snapshots of live video in PSOM.
	Create Video Alert	Whether the user can manually create an alert from video in PSOM.
	Manage Public Video Matrix View	Whether the user can add a video matrix to the Video Management Console that others can see.
	Manage Video Guard Tour	Whether the user can add a guard tour to the Video Management Console that others can see.
	View Recorded Video	Whether the user can view recorded video, and if so, how many past days of video can be viewed. See the "Controlling User Access to Video" section on page 3-3 for more information.
Report	Run a Report	Whether the user can run a report.
	Save a Report	Whether the user can save a report that has been executed.
	Save a Report as a New Report	Whether the user can save a report as a new report.
	Print a Report	Whether the user can print out a report.
	Export a Report	Whether the user can export a report from PSOM.
Business Logic	Manage Business Logic Rule	Whether the user can add or modify business logic rules using the Business Logic Designer.
	Test Business Logic Rule	Whether the user can run Test in the Business Logic Designer to debug the operation of a business logic rule.
Other	Access Preferences	Whether the user can access preferences.
Command	*Variable based on installed Integration Modules*	Whether the user can execute the listed external method.

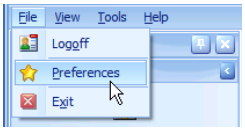
Enforcing Strong Passwords in PSOM

You can require users to define strong passwords (at least 8 characters with a mix of letters and numbers) for accessing PSOM from the Administration Console's **Preferences** area. You can also require users to update passwords at whatever frequency is desired for adequate security.

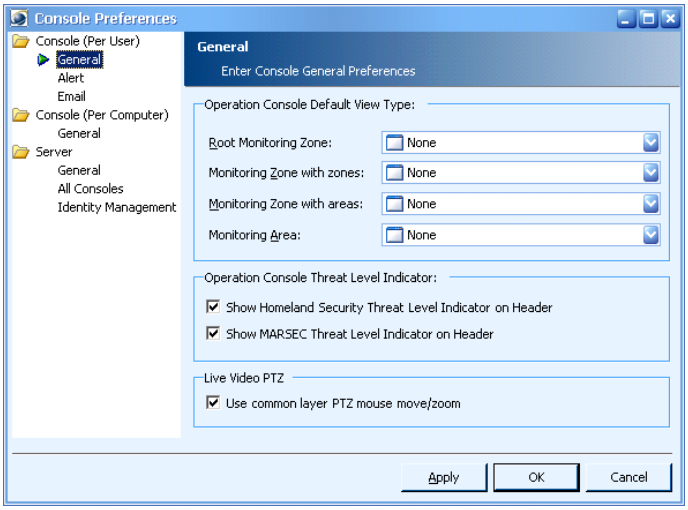
Note If a user has a weak password before you perform the steps to enforce a strong password, they will be able to keep using that password ***unless*** you also specify a password expiration policy that requires users to change their passwords at certain intervals.

To enforce strong passwords:

Step 1 From the Administration Console, select **File > Preferences**.

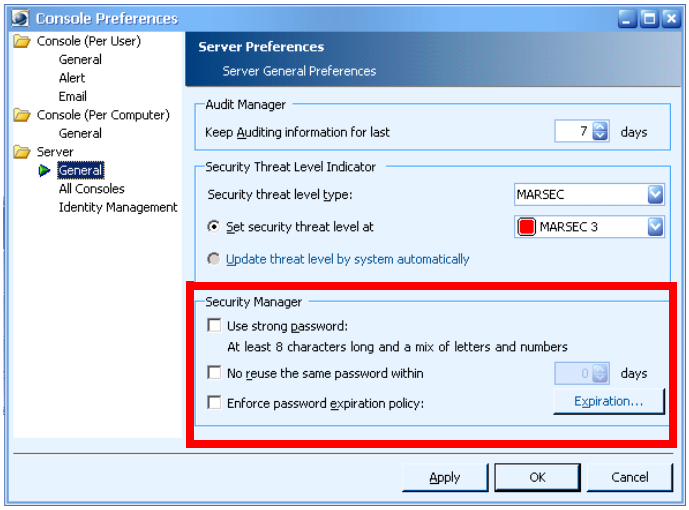


The Console Preferences window appears.



Step 2 Click **Server > General** in the left navigation.

The following dialog appears.

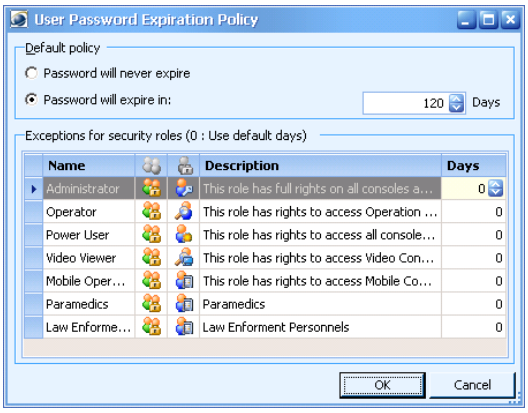


Step 3 To use strong passwords, check **Use strong password** under **Security Manager**.

Step 4 To prevent users from using the same password within a certain amount of time, check **No reuse the same password within** and enter a number of days in the field provided.

Step 5 To require users to change passwords at set intervals, check **Enforce password expiration policy** and click the **Expiration** button.

The User Password Expiration Policy window appears.



Step 6 Determine the default policy for the interval at which passwords will expire by selecting the **Password will expire in** option and entering a number of days in the field provided. Otherwise, select **Password will never expire**.

Step 7 To set an expiration policy specific to different security roles, select the security role from the table and enter a number of days in the field at the far right.

Step 8 Click **OK** when finished.

Step 9 Click **Apply** or **OK** in the Console Preferences window to save your changes.

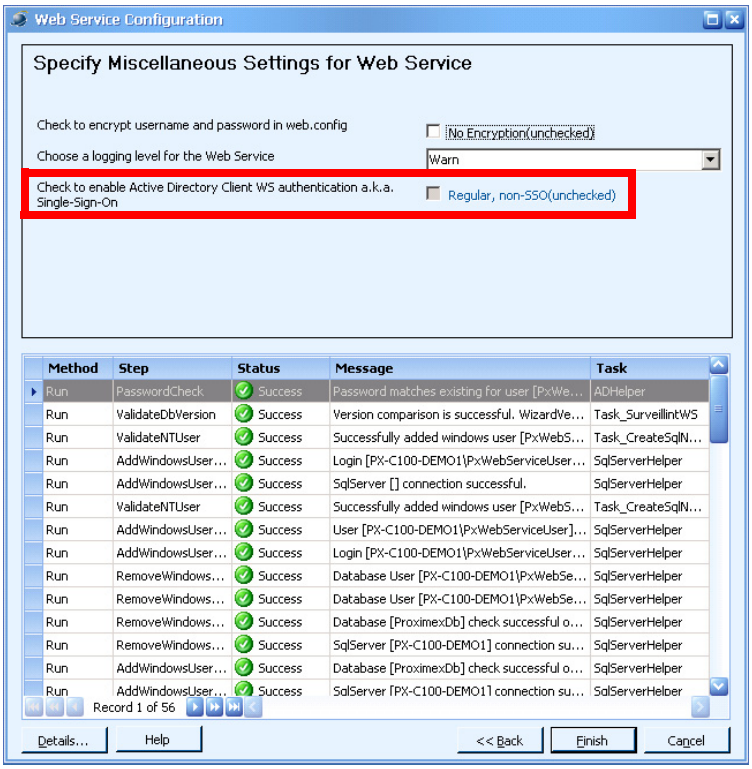
Single Sign On and User Management

When logging onto PSOM, you can choose to use single sign on (SSO) and thereby leverage Windows authentication. To login to PSOM using SSO, you must enable the PSOM Web Service to use SSO.

Once logged into PSOM using SSO, in order to add or remove PSOM users the Windows administrator account used to login to PSOM must have privileges for adding or removing users from an Active Directory group. When SSO is in effect, PSOM users are managed using the PxWebServiceGroup in Active Directory. Therefore, the Windows administrator account you use to login to PSOM should belong to the Account Operators group in Active Directory so that you have appropriate privileges.

Enabling PSOM Web Service to use SSO

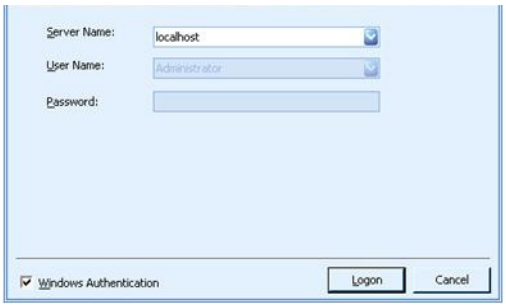
To enable PSOM Web Service to use SSO, you must re-configure the Web Service following the instructions in the "Changing the Configuration of the PSOM Web Service" section on page C-16. Then on the Specify Miscellaneous settings for Web Service window, select the **Check to enable Active Directory Client WS authentication** option. By default, Active Directory is not used for user authentication by PSOM or the Web Service.



To configure the PSOM Web Service to use SSO, you must use an administrator account with privileges to create a User Group and add users to it in Active Directory.

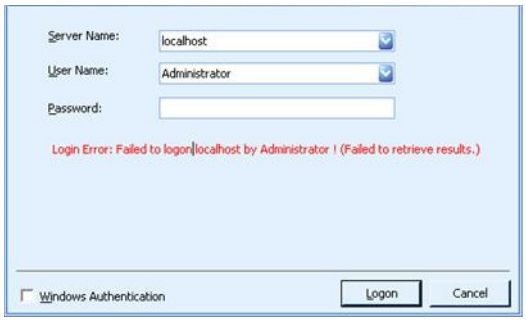
Logging Into PSOM with SSO

To login to PSOM using SSO, be sure the PSOM Web Service is enabled to use SSO, and check the **Windows Authentication** option during login. The **User Name** and **Password** fields grey out.



Click **Logon** and the check state will be saved and loaded from the last saved state.

If the PSOM Web Service is not enabled for SSO, and you check the **Windows Authentication** option during login to PSOM, you will see an error message.

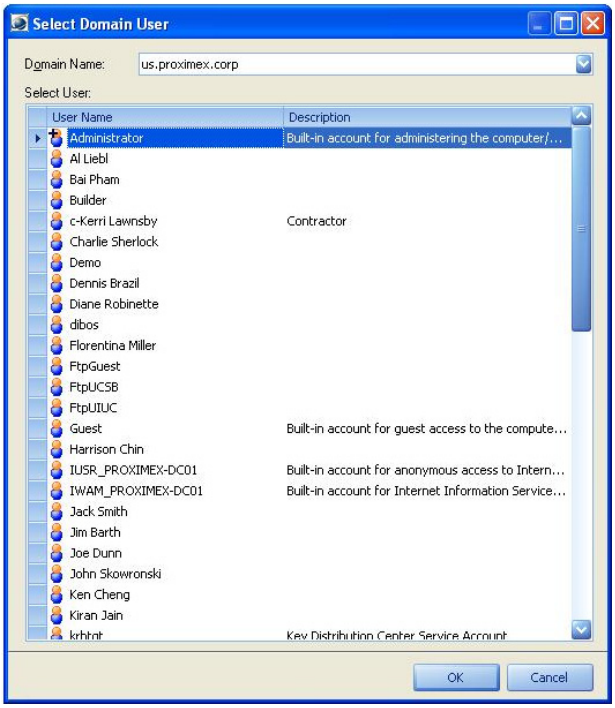


Adding Users from Active Directory

When single sign on is enabled for the PSOM Web Service, you add users from Active Directory. The **Add User** dialog box appears as follows.

To add a user, you can enter the user name using the format *domain name\user name*, or click the ... button and select the user from Active Directory using the **Select Domain User** window.

Note The **Password** and **Confirm Password** fields are greyed out when SSO is in effect in PSOM.



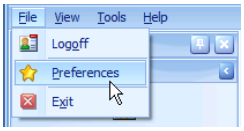
If you enter an incorrect user name in the **User Name** field, an error message appears.

Identity Management in PSOM

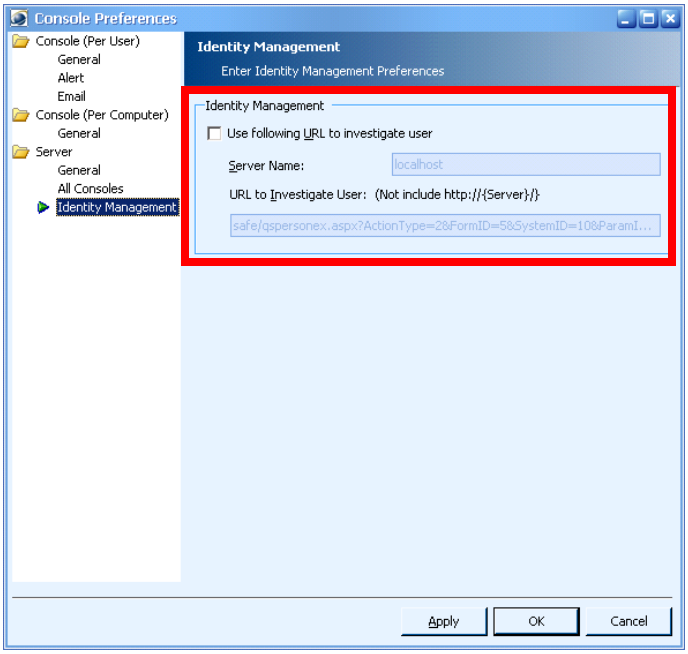
In the Operation Console, operators can click the **Investigate User** button in the Alert Details window of the Operations Console to display additional badge details for a user.

To designate identity management software:

Step 1 Select **File > Preferences**.



Step 2 Click **Identity Management** under **Server**.



Step 3 Check the **Use following URL to investigate user** option.

Step 4 Enter the IP address or server name of the machine hosting the third-party identity management software in the **Server Name** field.

Step 5 Enter the URL for accessing the identity management software in the **URL to Investigate User** field. At the end of the URL, add the following syntax to pass the user's badge ID from PSOM to the identity management software when the **Investigate User** button is clicked in the Alert Details window:

```
%BADGEID%
```

The full URL may look similar to the following:

```
safe/qspersonex.aspx?ActionType=2&FormID=5&SystemID=10&ParamID=%BADGEID%
```

Step 6 Click **OK**.

CHAPTER 3

Configuring Video Services

This chapter covers the basic steps to enable video streaming in the Operation Console.

This chapter includes these topics:

- Enabling Video Integration with PSOM, page 3-1
- Configuring Access to Video Servers for Monitoring, page 3-1
- Adding New Sensors for Video Cameras, page 3-3
- Controlling User Access to Video, page 3-3
- Performing Batch Imports for Video Camera Sensors, page 3-4
- Managing Video Matrix Views and Guard Tours, page 3-6

Enabling Video Integration with PSOM

There are two methods for enabling video integration with PSOM:

- Manually enter camera information into PSOM using the Administration Console. Use this method if you only have a limited number of cameras to configure. See the "Configuring Access to Video Servers for Monitoring" section on page 3-1.
- Perform a batch import of cameras. If you have hundreds or thousands of video cameras to integrate with PSOM, you will want to use this method. Using this method, you will obtain sensor information from the appropriate Integration Module, save it to XML, make whatever changes are necessary using Excel or other spreadsheet, and import the result into PSOM to define all video cameras from your video server at once. See the "Performing Batch Imports for Video Camera Sensors" section on page 3-4.

Configuring Access to Video Servers for Monitoring

To enable manual video integration, you need to obtain some information from the video server's configuration.

For each video camera, you need the information such as:

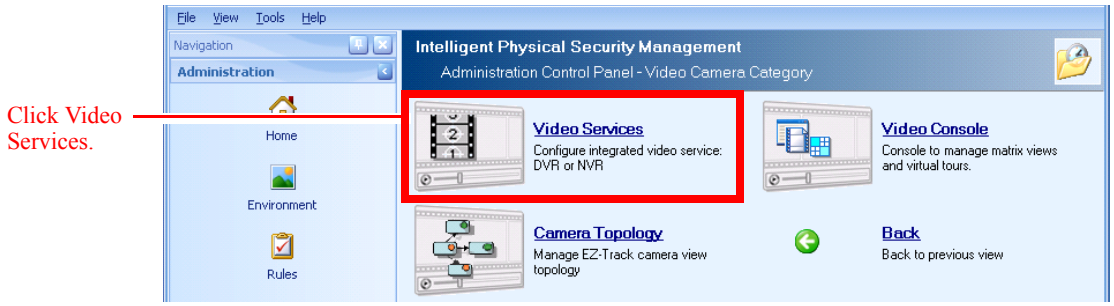
- DVR/NVR server name or IP address
- Server login name
- Server login password

You can integrate as many different video servers as you wish in PSOM.

To manually configure access to video servers in PSOM for monitoring:

Step 1 Click the **Video Integration** icon in the tools area of the Administration Console.

The Video window appears.



Step 2 Click **Video Services** to configure access to a video server.

The **Video Service Integration Module Configuration** window appears.

Step 3 Choose the Cisco video service integration module.

Follow the instructions in the *Configuring Cisco Video Service* document complete configuration using the Video Service Integration Module Configuration window.

When you are finished, restart the PSOM Administration Console to enable the new video service configuration.

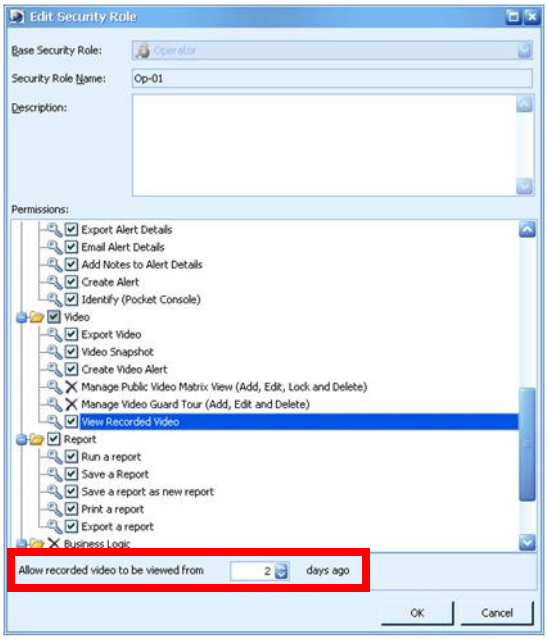
Adding New Sensors for Video Cameras

After you have completed video server configuration, the next step is to add sensors to PSOM for the video cameras following the instructions in the "Adding new Sensors for Video Cameras" section on page 6-7.

Controlling User Access to Video

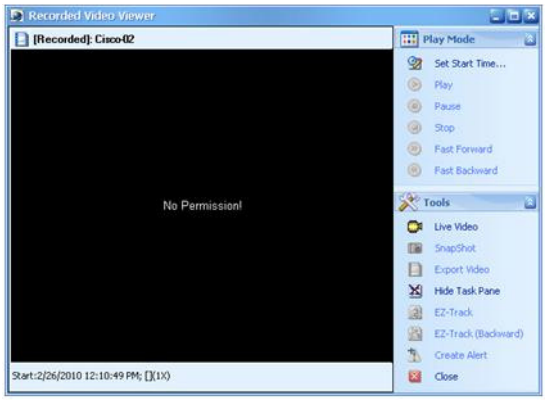
You can set user permissions that control whether users can view recorded video, export video, take snapshots, create video alerts, and manage video matrixes or guard tours. See the "Permissions Within PSOM" section on page 2-20 for information.

When you assign a user the permission to view recorded video, you can also determine how many past days of recorded video they are allowed to see.

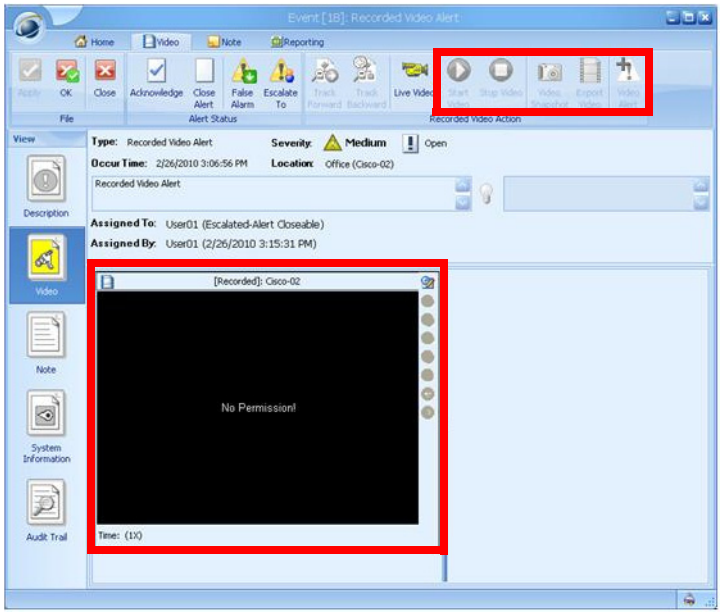


Enter the number of past days of recorded video the user can see in the **Allow recorded video to be viewed from** field.

If the user tries to view video past that number of days, an error message appears in the Recorded Video Viewer window.



If a user does not have permission to view recorded video, buttons for accessing recorded video are disabled.

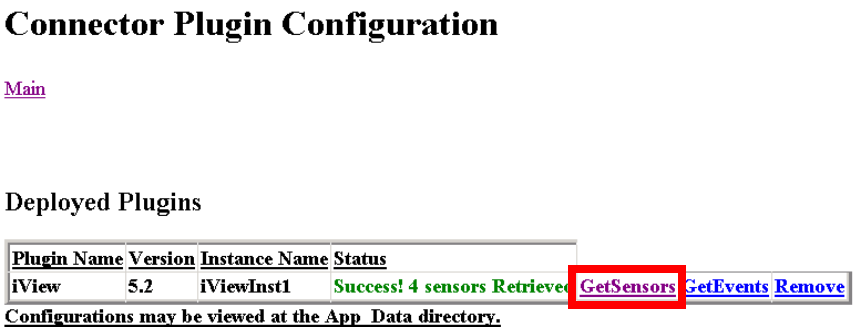


Performing Batch Imports for Video Camera Sensors

To add video camera sensors to PSOM all at once:

Step 1 Open Internet Explorer and navigate to http://localhost/PxConnectorWS/PluginPages/default.aspx.

The Connector Plugin Configuration window appears.



Step 2 Click **Get Sensors** next to the Integration Module for your video server under **Deployed Plugins**.

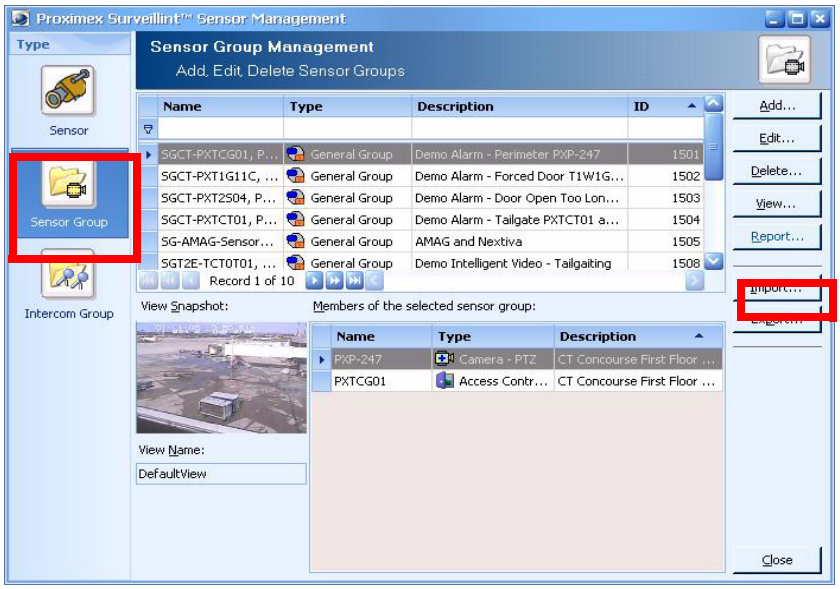
Step 3 Click **Generate Bulk Insert XML**. An XML string appears in the text box.

Step 4 Select the text in the box and copy it (CTRL-C).

Step 5 Launch Notepad. Paste the XML text into Notepad, select **File > Save As**, and give the file a name with an .xml extension.

Step 6 In the Administration Console, open the Sensor Management window and click the **Sensor Group** icon.

Step 7 Click **Import** and select the file you just created to insert the sensors into PSOM. This process will create the appropriate type of sensors for your video cameras.



Step 8 Restart all services and the verify addition of the video server's sensor type.

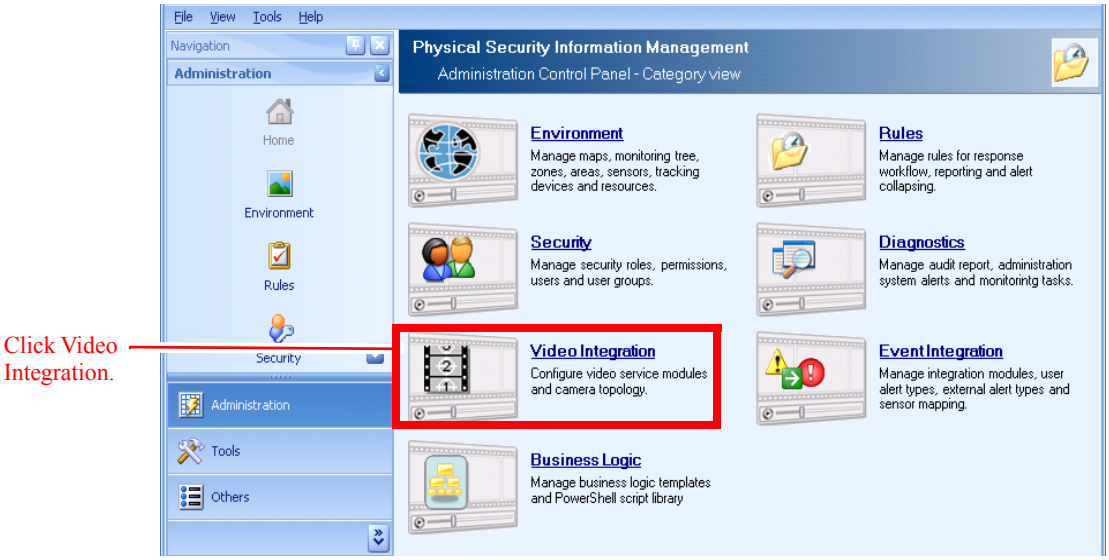
Managing Video Matrix Views and Guard Tours

You can set up video matrix views and guard tours in the Video Management Console. Instructions are covered in "Using the Video Management Console" in Chapter 4 of the Using Cisco Physical Security Operations Manager guide.

You can launch the Video Management Console from the PSOM Administration Console.

To launch the Video Management Console:

Step 1 Click the **Video Integration** icon in the tools area of the Administration Console.



The Video window appears.

Step 2 Click **Video Console** to launch the Video Management Console.

The Video Management Console appears.

See "Using the Video Management Console" in Chapter 4 of the *Using Cisco Physical Security Operations Manager* guide for instructions on setting up video matrix views and guard tours.

CHAPTER 4

Defining Locations

The first step to defining your monitoring areas and zones is to establish the *locations,* or physical spaces, within your environment that will be monitored by PSOM.

This chapter includes these topics:

- Planning Locations for your Environment, page 4-1
- Adding Locations to PSOM, page 4-2
- Editing Locations, page 4-3
- Deleting Locations, page 4-5
- Importing or Exporting Location Names, page 4-6

Planning Locations for your Environment

Locations are the physical spaces in your environment that will be monitored by PSOM. When you start adding sensors to PSOM, you will need to assign each of them to a location. So your locations should be places where there are sensors you want to integrate with PSOM for monitoring.

Setting up locations within PSOM is much easier if you have first performed some planning. Table 4-1 shows a sample plan for locations within a building that lists location names and describes their physical spaces.

Suggestion: Make your names and descriptions detailed so that operators will instantly know exactly where alerts are taking place when they see the location.

Note A blank version of this table is provided in Appendix A, "Planning Worksheets," to help you with location planning—Table A-3 on page A-4.

Table 4-1 Sample Planning for Locations

Location Name	Description
Public Elevator 1	The public elevator located on level 1 by baggage claim #1.
Ticket Counters - American	The 5 ticket counters for American Airlines.
Baggage 1	Baggage carousel #1.
Checkpoint 1	Security check area 1 on the east side of terminal 1.

Adding Locations to PSOM

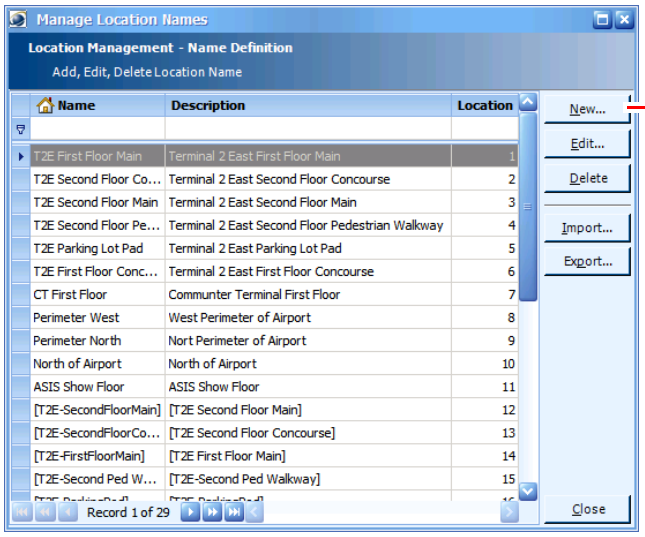
To add a location to PSOM:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click **Location Names** to manage your locations.

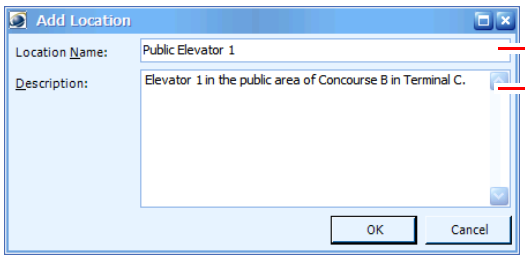
The Manage Location Names window appears.



Click the New button to add a location to PSOM for monitoring.

Step 3 Click the **New** button.

The Add Location window appears.



Enter a detailed name in the Location Name field.

Enter a description that will help operators know exactly where an alert is occurring. For example, "Elevator on 1st floor close to the Baggage Claim 1 area."

Step 4 In the **Location Name** field enter the name you want to assign to this place.

Step 5 In the **Description** field, enter a detailed description of the location that will tell operators exactly where it is in the security environment.

Step 6 Click **OK** to save the location to the database.

Step 7 Repeat this procedure to define each location.

When you finish adding locations, they will all appear when you access the Manage Location Names window.

Editing Locations

As operators in your organization use PSOM, you may discover that some location names or descriptions need to change to enable faster response times. You can edit location names and descriptions using the Administration Console.

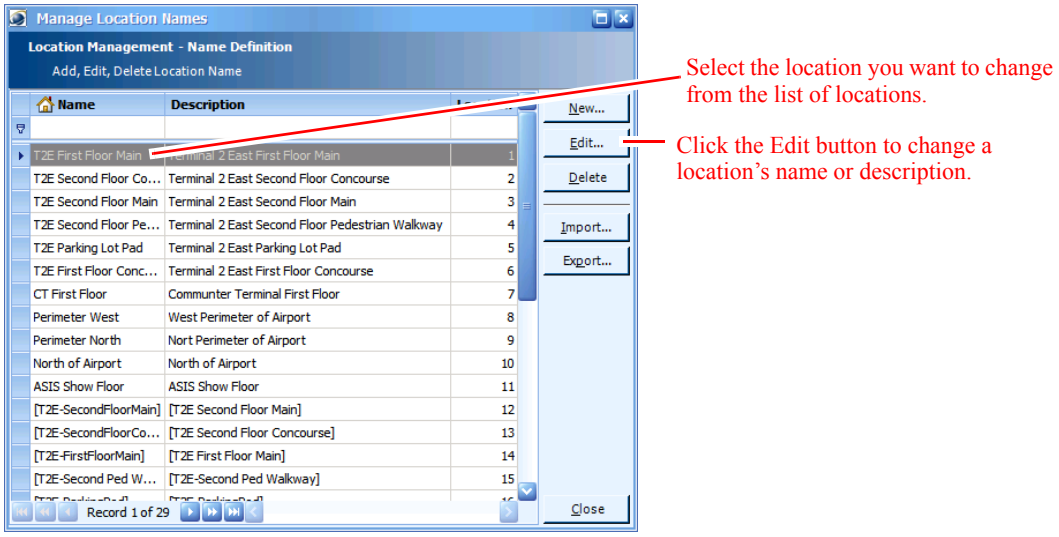
To edit a location:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click **Location Names** to manage your locations.

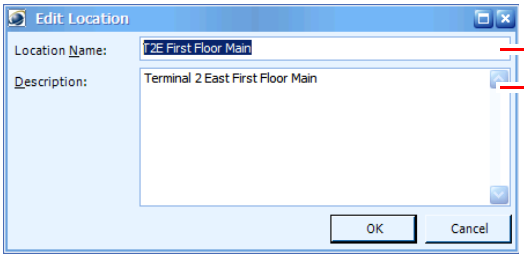
The Manage Location Names window appears.



Step 3 Select the location you want to edit from the list.

Step 4 Click the **Edit** button.

The Edit Location window appears.



Step 5 To change the location's name, enter a new name in the **Location Name** field.

Step 6 To change the location's description, enter a new description in the **Description** field.

Step 7 Click **OK** to store your changes to the database.

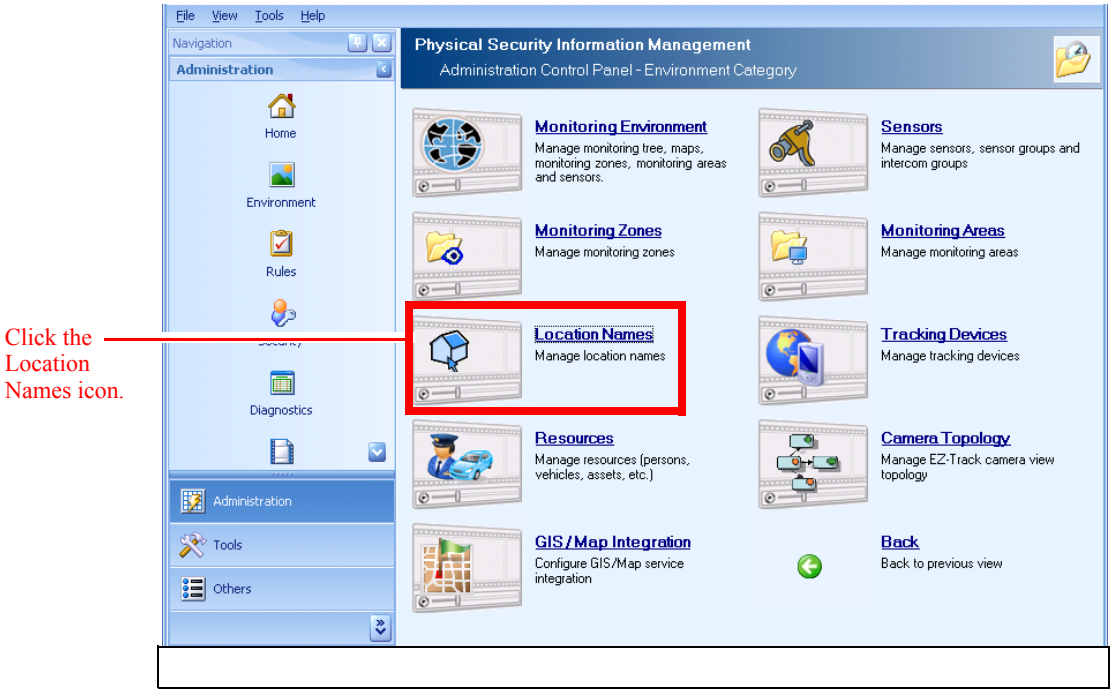
Deleting Locations

If changes occur within the physical environment, you may find it necessary to remove locations from PSOM.

To remove a location from PSOM:

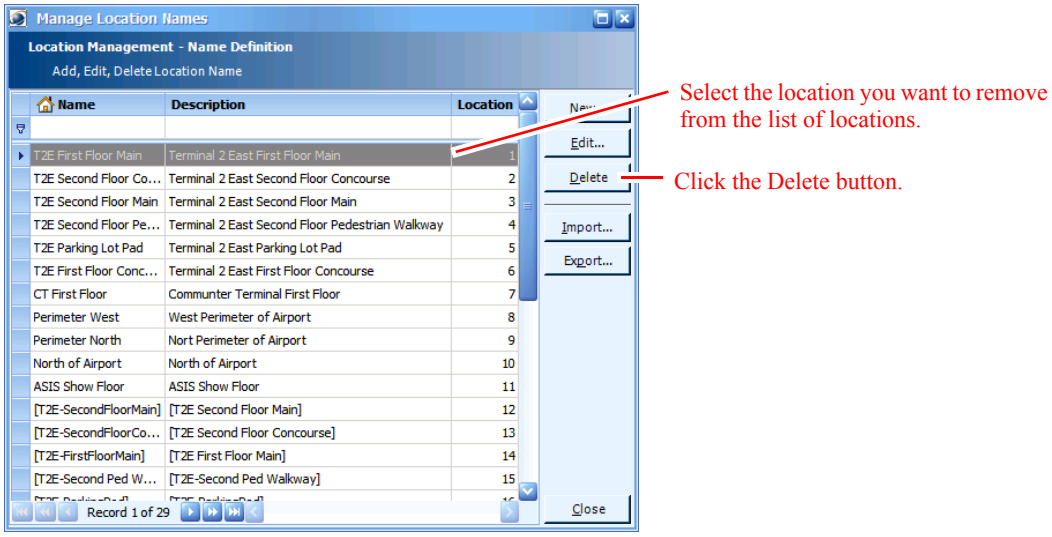
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.



Step 2 Click **Location Names** to manage your locations.

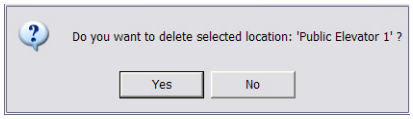
The Manage Location Names window appears.



Step 3 Select the location you want to remove from the list.

Click the **Delete** button.

A confirmation dialog box appears.



Step 4 Click **OK** to remove the location from PSOM.

Note Related sensors, monitoring areas and monitoring zones will be affected when you remove a location from PSOM. Sensors that are associated with this location may become orphaned if you delete the location.

If changes occur within the physical environment, you may find it necessary to remove locations from PSOM.

Importing or Exporting Location Names

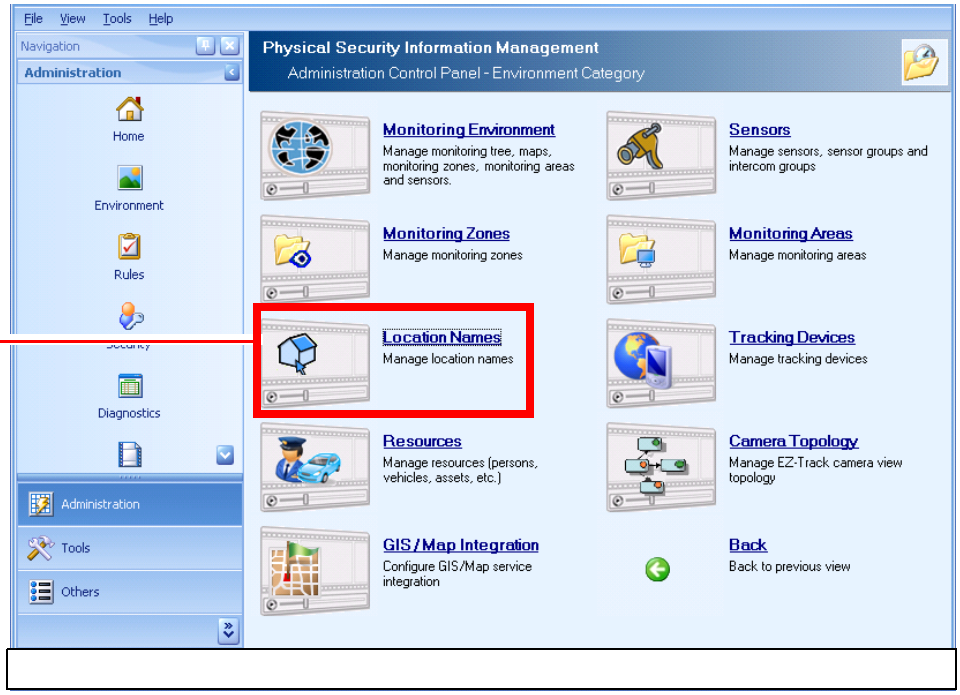
You can export location definitions from PSOM to an XML file, update the XML content in Microsoft Excel, and import the updated location definitions to PSOM.

Note See the "Importing and Exporting Sensors, Sensor Groups, and Intercom Groups with PSOM" section on page 6-36 for information about how to open the XML file in Microsoft Excel, edit the data, and save out to the correct format for re-import to PSOM.

To export or import locations:

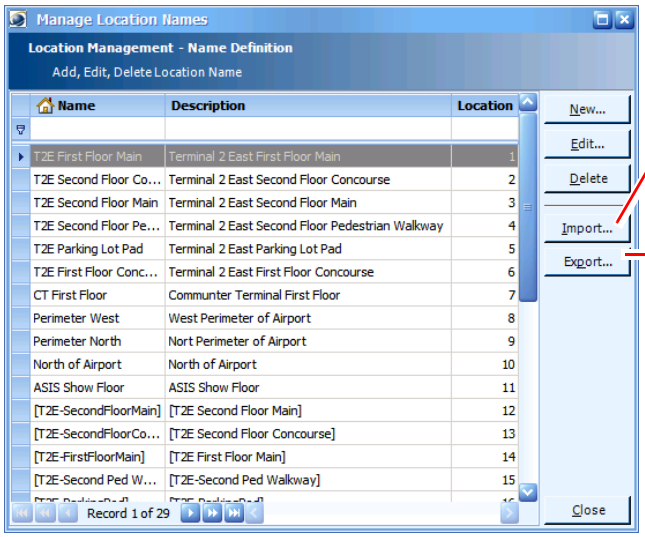
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.



Step 2 Click **Location Names** to manage your locations.

The Manage Location Names window appears.



Step 3 Click **Import** to import location names from an XML file (should be named PxLocation.xml), then select the XML file on your system that has the definitions.

Step 4 Click **Export** to save an XML file with the location names defined in PSOM. It will save the file as PxLocation.xml.

CHAPTER 5

Managing Monitoring Areas and Zones

Once you've set up locations and sensors in PSOM, you can define monitoring areas and zones, and then create the navigation hierarchy for traversing across your security environment.

This chapter explains:

- The difference between monitoring areas and monitoring zones.
- How to add a monitoring area to PSOM and include sensor groups as members.
- How to add a monitoring zone to PSOM and include monitoring areas as members.
- Establish the hierarchical navigation tree that allows users to traverse the security environment from the Navigation Pane in the Operation Console.

This chapter includes these topics:

- Understanding Monitoring Areas and Zones, page 5-1
- Planning Monitoring Areas and Zones, page 5-2
- Adding Monitoring Areas to PSOM, page 5-2
- Adding Monitoring Zones to PSOM, page 5-6
- Setting up the Monitoring Tree Hierarchy, page 5-10
- Adding Maps to Monitoring Areas and Zones, page 5-19
- Editing or Deleting Monitoring Areas, page 5-20
- Editing or Deleting Monitoring Zones, page 5-23
- Importing or Exporting Monitoring Areas, page 5-26

Understanding Monitoring Areas and Zones

You need to setup both monitoring areas and monitoring zones for PSOM. Table 5-1 explains the differences between them.

Table 5-1 Differences Between Monitoring Areas and Zones

	Description	Members	Examples
Monitoring Area	A virtual representation of a place within your security environment that is associated with a map or building floor plan and sensor groups that exist in that physical space.	• Maps or building floor plans of a particular physical location • Groups of sensors located within that physical space	A ticket counter for a gate within an airport terminal. A security checkpoint within an airport terminal.
Monitoring Zone	Logical groups of monitoring areas that are associated because of physical location, business function, or other reasons.	Monitoring areas or monitoring zones.	Terminal 1 at an airport would contain a ticket counter for a gate and a security checkpoint.

Planning Monitoring Areas and Zones

Planning the structure of your surveillance environment might streamline your configuration of monitoring areas and zones.

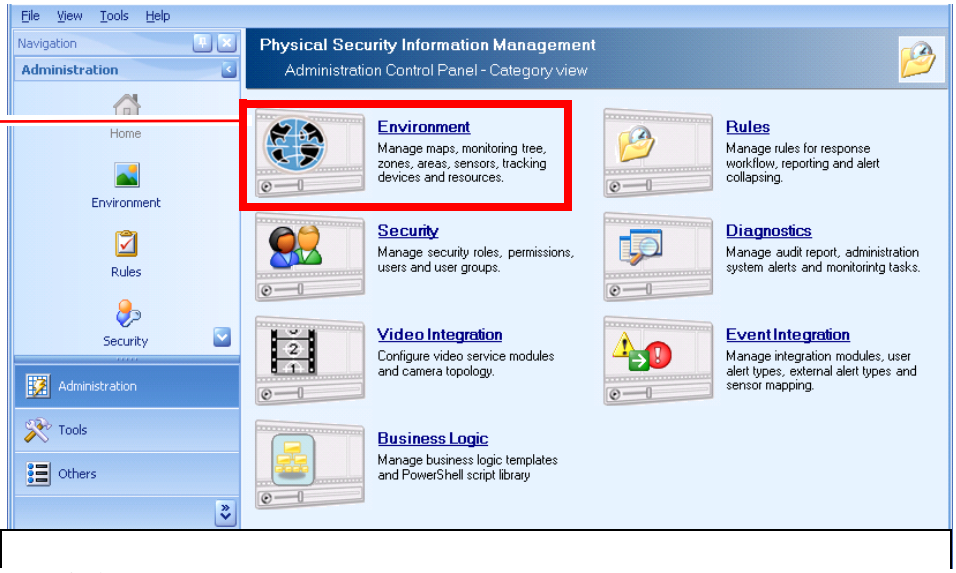
Appendix A, "Planning Worksheets," includes planning tables you can use to determine the structure top-down from monitoring zones to monitoring areas:

- Monitoring zone planning—Table A-5 on page A-6.
- Monitoring areas planning—Table A-6 on page A-7.

Adding Monitoring Areas to PSOM

To add a monitoring area:

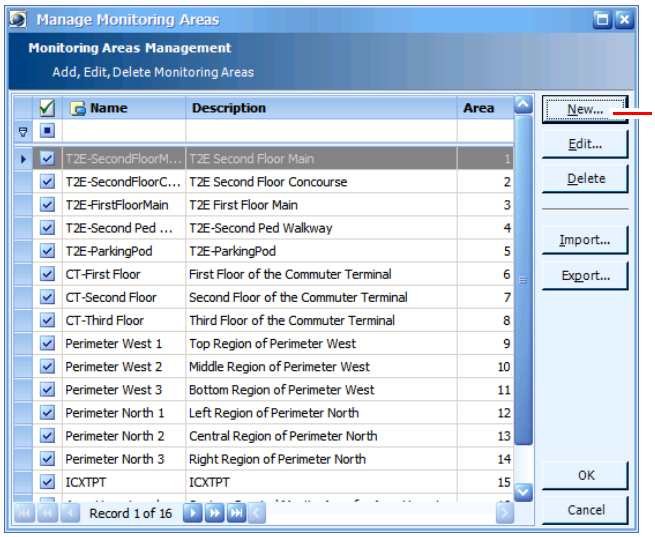
Step 1 Click the **Environment** icon in the Administration Console.



The Environment window appears.

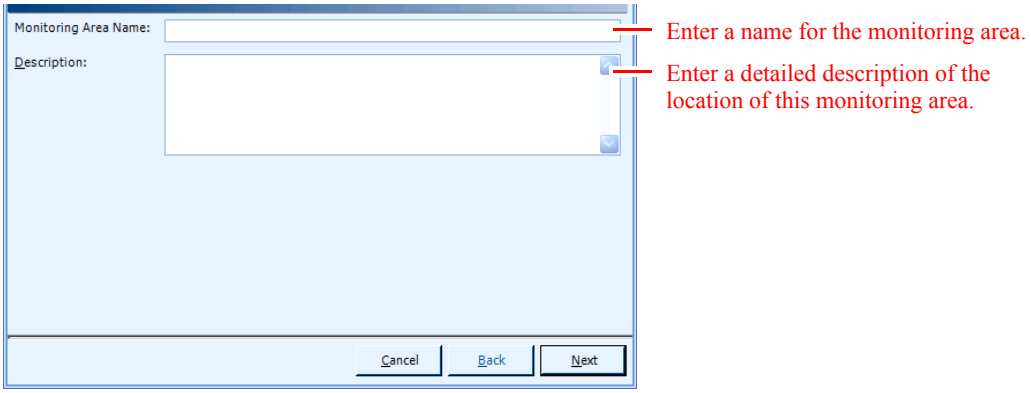
Step 2 Click the **Monitoring Areas** icon.

The Manage Monitoring Areas window appears.



Step 3 Click the **New** button.

The PSOM Area Wizard window appears.

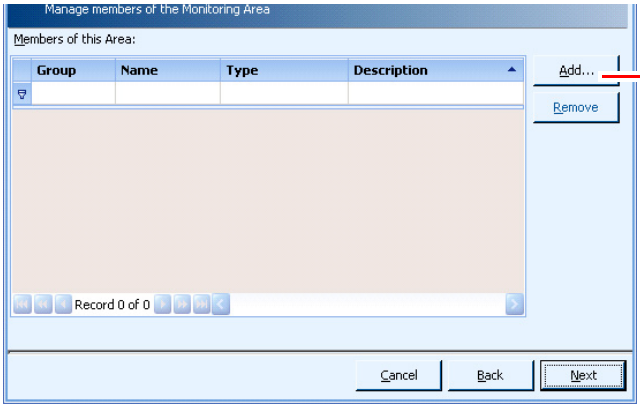


Step 4 In the **Monitoring Area Name** field, enter a name for this monitoring area.

Step 5 In the **Description** field, provide a detailed description of the location this monitoring area represents.

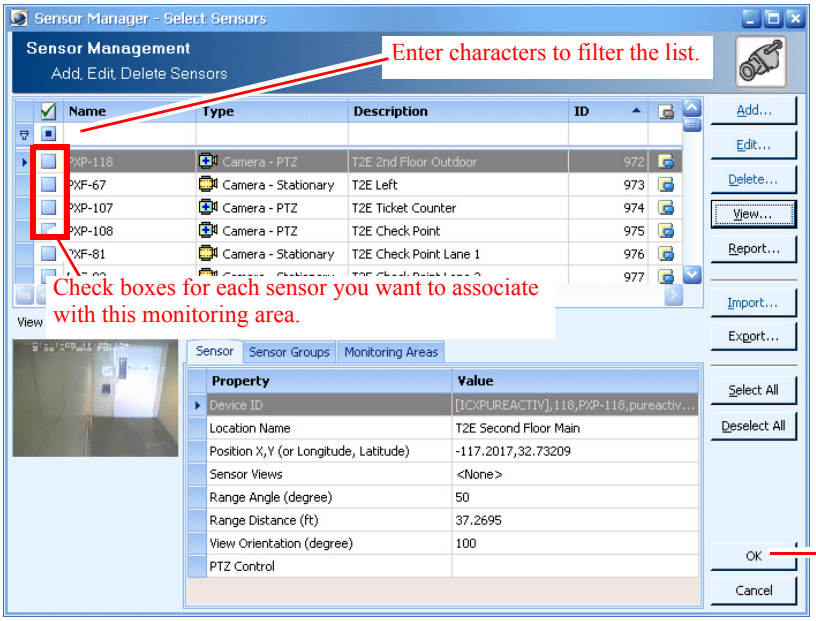
Step 6 Click **Next**.

Step 7 The Monitoring Area - Member window appears.



Step 8 Click the **Add** button to associate sensors with this monitoring area.

The Select Sensors window appears.

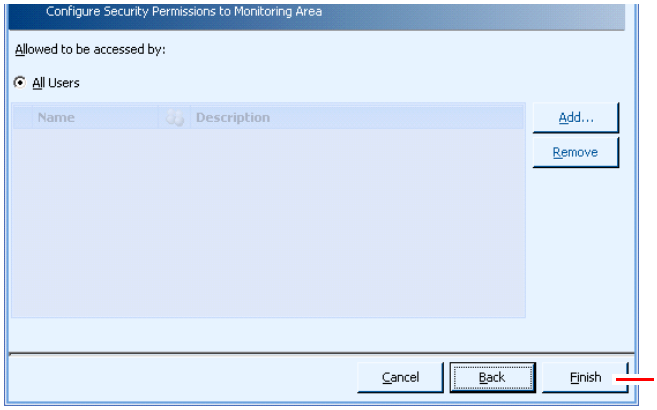


Step 9 Check boxes for all sensors in the list you want to include. You can refine the list of sensors displayed in the list by typing the first few characters of the items you're seeking in the filter field at the top of the list.

Step 10 Click **OK** when you're finished adding sensors to the monitoring area.

Step 11 At the Monitoring Area - Member screen, click **Next** to continue.

Step 12 The Monitoring Area - Security window appears.



Note: You cannot change these settings for this product release.

Click Finish.

This screen shows the users that are allowed to access the monitoring area.

Note For this product release, all users are allowed access to monitoring areas by default. This setting cannot be changed.

Step 13 Click **Finish** to save your monitoring area to PSOM.

Adding Monitoring Zones to PSOM

To add a monitoring zone:

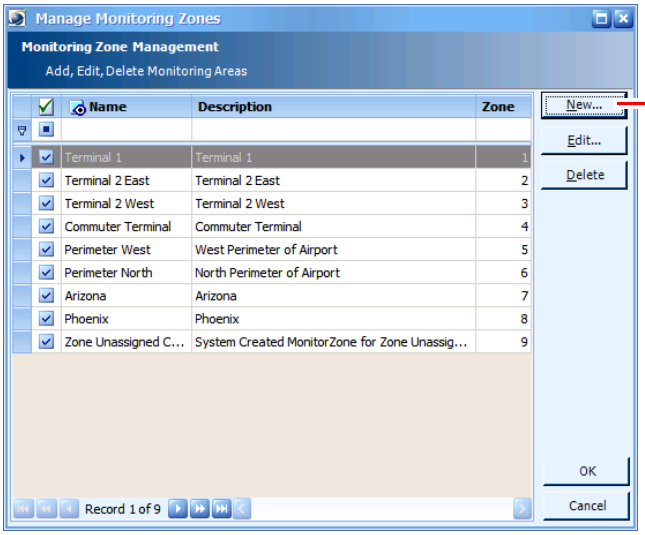
Step 1 Click the **Environment** icon in the Administration Console.

Click the Environment icon.

The Environment window appears.

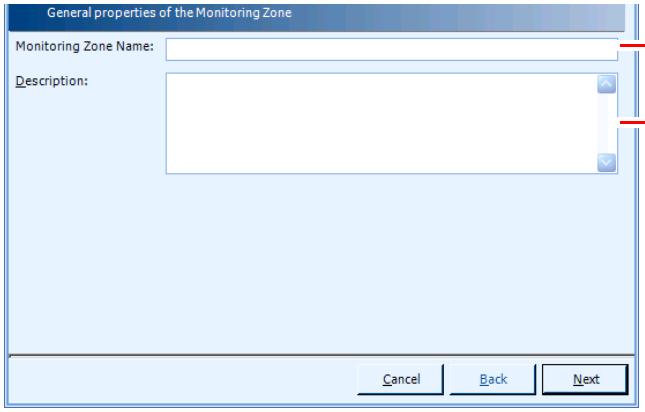
Step 2 Click the **Monitoring Zones** icon.

The Manage Monitoring Zones window appears.



Step 3 Click the **New** button.

The PSOM Zone Wizard window appears.

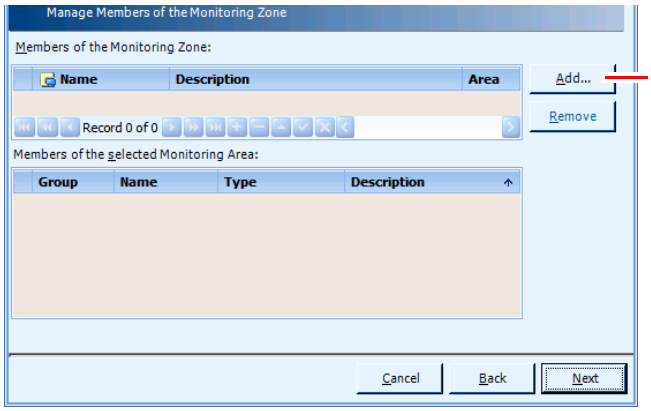


Step 4 Enter a name for the monitoring zone in the **Monitoring Zone Name** field.

Step 5 Enter a detailed description of the physical or logical area covered by this monitoring zone in the **Description** field.

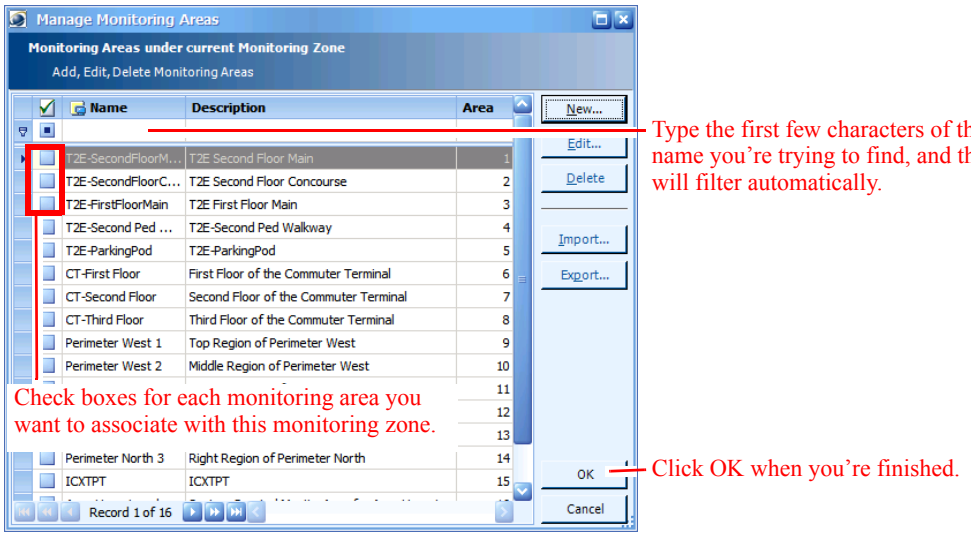
Step 6 Click **Next**.

The Monitoring Zone - Member window appears.



Step 7 Click the **Add** button to associate monitoring areas with this monitoring zone.

The Manage Monitoring Areas window appears.



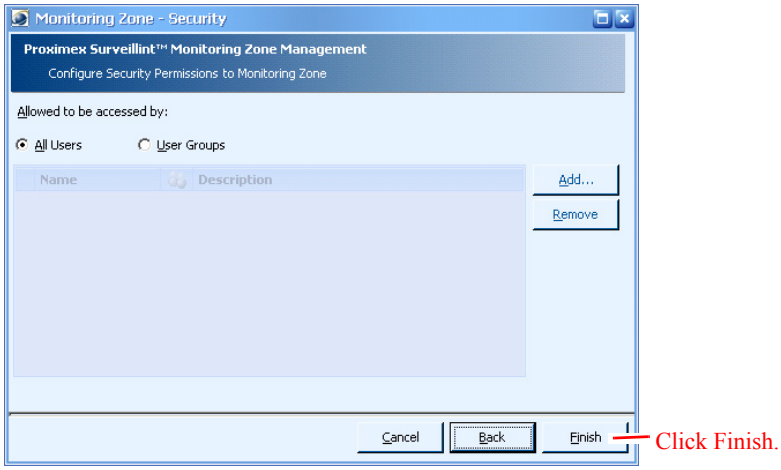
Step 8 Check the boxes for all monitoring areas that should be associated with this monitoring zone. To filter the list of areas displayed, type the first few characters of the area you're seeking in the filter field at the top of the list.

Step 9 Click **OK** when you're finished selecting monitoring areas.

The Monitoring Zone - Member window re-appears.

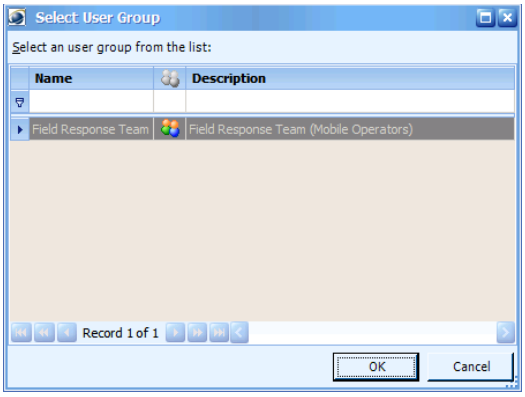
Step 10 Click **Next**.

The Monitoring Zone - Security window appears.



Step 11 If you want all users to access this monitoring zone, leave the **All Users** option checked. Otherwise, check the **User Groups** option and click **Add** to select user groups that can access this monitoring zone.

The Select User Group window appears.



Select the group(s) that can access this monitoring zone and click **OK**.

Step 12 Click **Finish** to save your monitoring zone to PSOM.

Setting up the Monitoring Tree Hierarchy

The hierarchy you define for the Monitoring Tree in the Administration Console is what appears to users in the Navigation Pane of the Operation Console. It is the list-type view of monitoring zones and areas that allows operators to traverse the global monitoring environment with simple point-and-click actions.

To set up the Monitoring Tree hierarchy, you need to:

Step 1 Add monitoring zones to the Monitoring Tree.

Step 2 Add multiple levels of monitoring zones.

Step 3 Add monitoring areas under the monitoring zones in the Monitoring Tree.

Adding Monitoring Zones to the Monitoring Tree

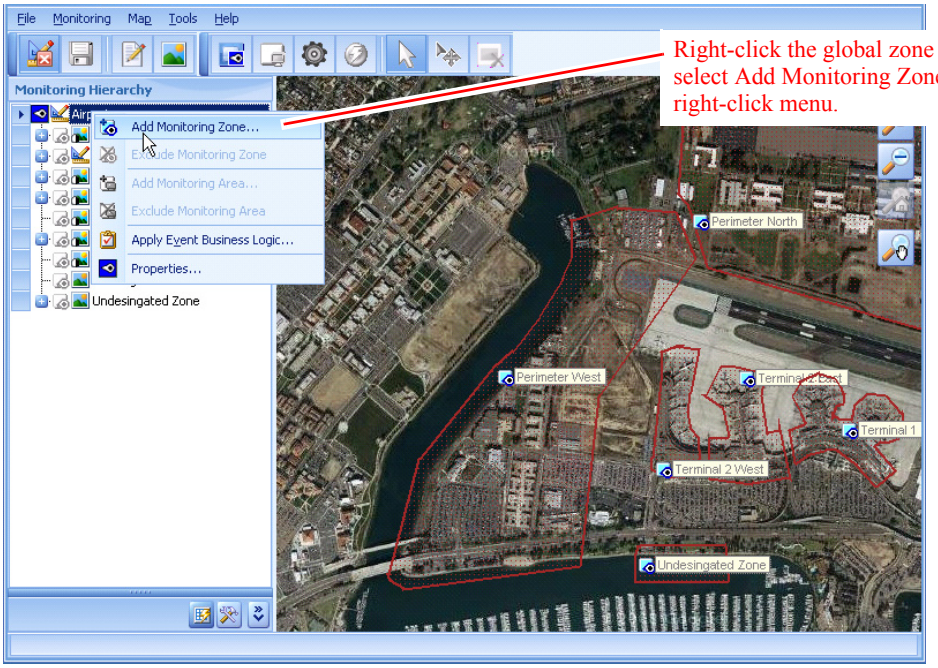
To add monitoring zones to the Monitoring Tree:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Monitoring Environment** icon.

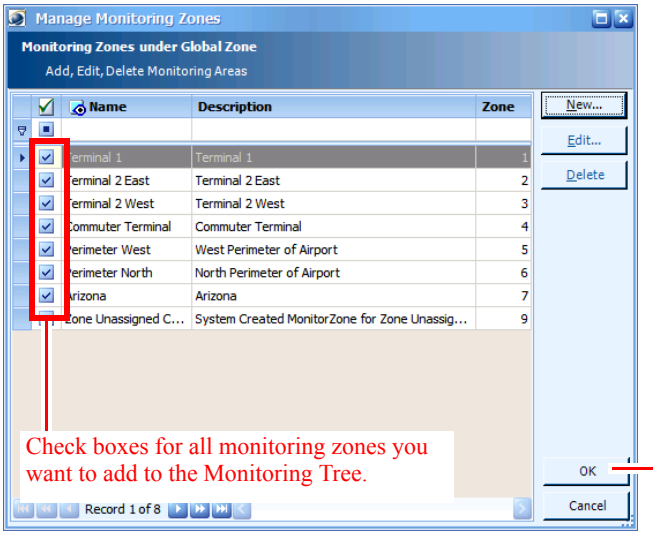
The PSOM Environment Management window appears.



Step 3 Right-click the global zone (top-most) node in the Monitoring Tree.

Step 4 Select **Add Monitoring Zone** from the right-click menu.

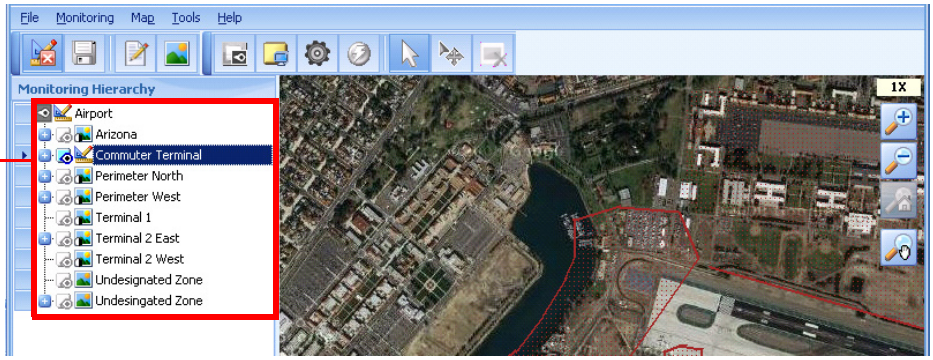
The Manage Monitoring Zones window appears.



Step 5 Check boxes for each monitoring zone you want to add to the Monitoring Tree.

Step 6 Click **OK**.

The Monitoring Tree is updated to include all the monitoring zones you selected; the monitoring zones are listed as nodes under the top-level “global zone” node.

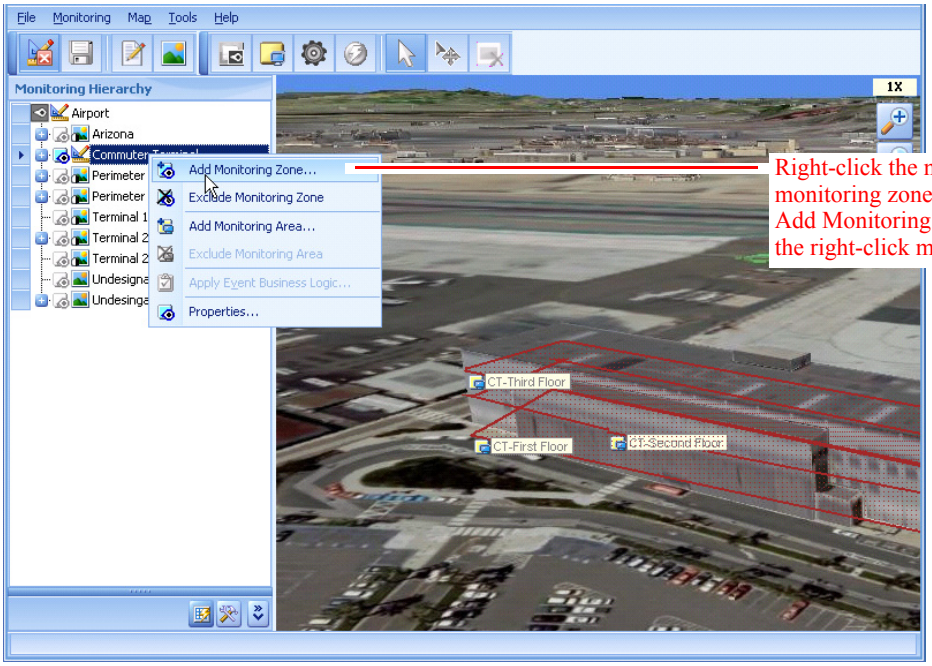


The selected monitoring zones now appear in the Monitoring Tree as nodes under the global zone.

Adding Multiple Levels of Monitoring Zones to the Monitoring Tree

To add an additional level of monitoring zone to the Monitoring Tree:

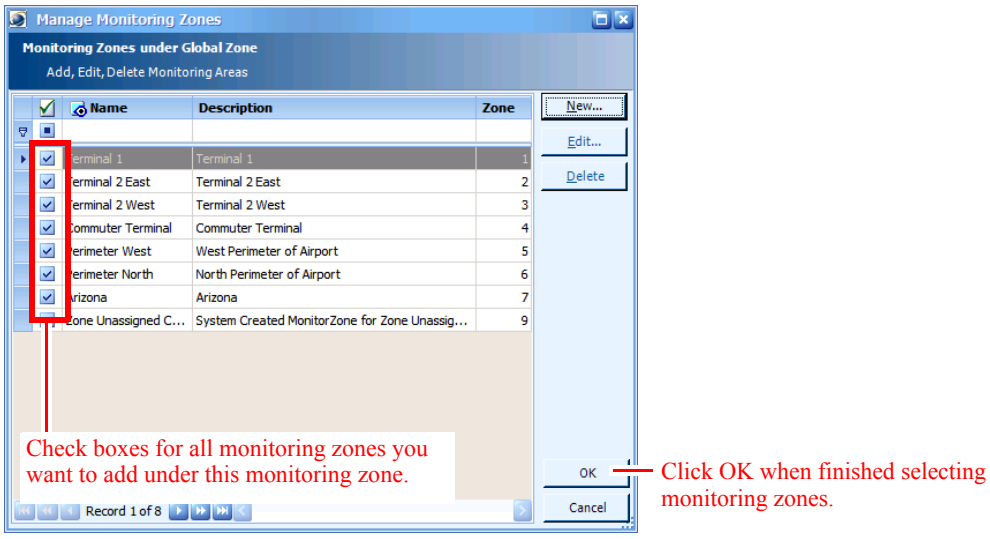
Step 1 In the **Monitoring Tree**, locate and right-click the monitoring zone to which you want to add additional level of monitoring zone.



Right-click the node for the monitoring zone and select Add Monitoring Zone from the right-click menu.

Step 2 Select **Add Monitoring Zone** from the right-click menu.

The **Manage Monitoring Zones** window appears.



Step 3 Check boxes for each monitoring zone you want to add under the selected monitoring zone in the Monitoring Tree.

Step 4 Click **OK**.

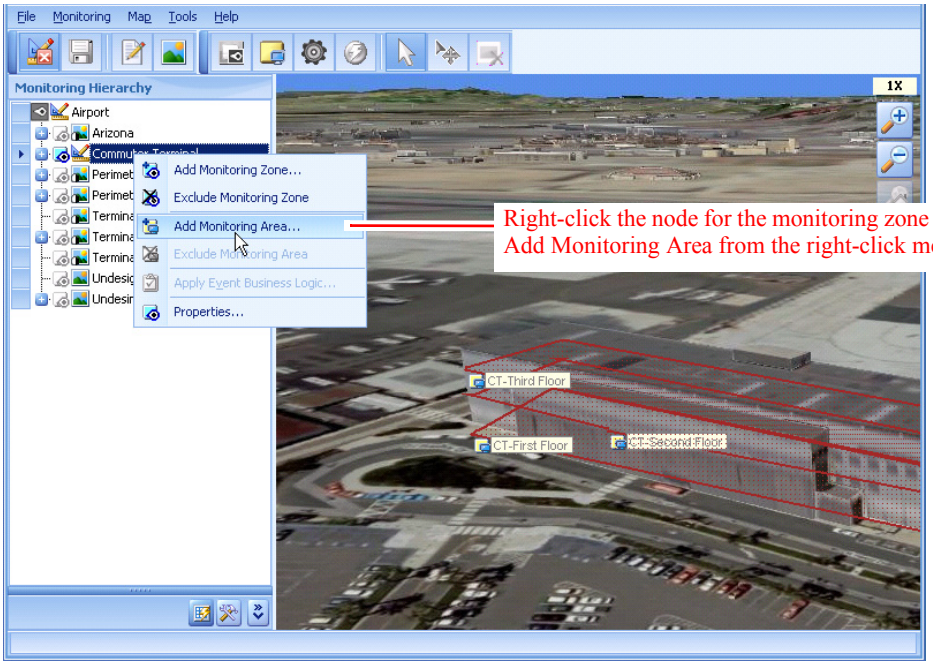
The **PSOM Environment Management** window re-appears. The newly added monitoring zone and its monitoring areas are added to the **Monitoring Tree.**

Adding Monitoring Areas to the Monitoring Tree

To add monitoring areas to the Monitoring Tree:

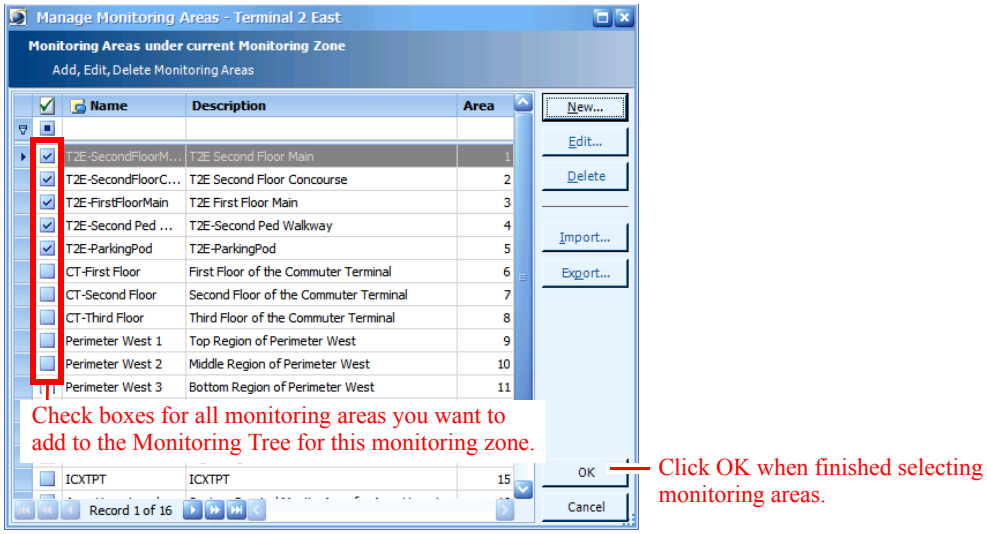
Step 1 Open the PSOM Environment Management window.

Step 2 In the **Monitoring Tree**, locate and right-click the monitoring zone to which you want to add monitoring areas.



Step 3 Select **Add Monitoring Area** from the right-click menu.

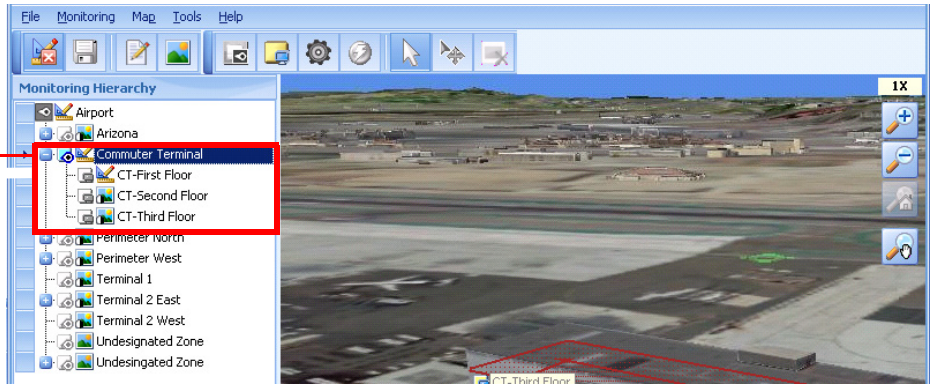
The Manage Monitoring Areas window appears.



Step 4 Check boxes for each monitoring area you want to add to the selected zone.

Step 5 Click **OK** when finished.

The Monitoring Tree is updated to list all the monitoring areas you selected as nodes under the monitoring zone's node.

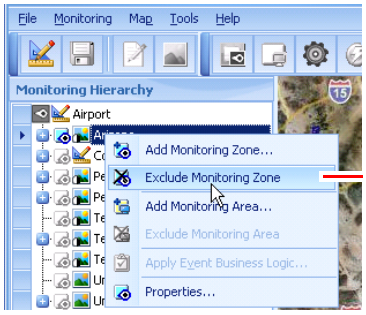


The selected monitoring areas now appear in the Monitoring Tree as nodes under the monitoring zone.

Removing Nodes from the Monitoring Tree

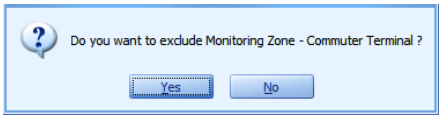
To exclude a monitoring zone node from the Monitoring Tree:

Step 1 Right-click the monitoring zone and select **Exclude Monitoring Zone**.



Right-click the monitoring zone node and select Exclude Monitoring Zone from the right-click menu.

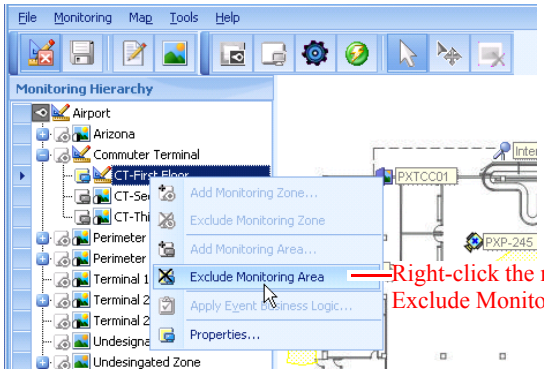
A confirmation dialog box appears.



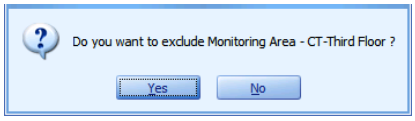
Step 2 Click the **Yes** button to confirm the exclusion of the node.

To exclude a monitoring area from the Monitoring Tree:

Step 1 Right-click the monitoring area and select **Exclude Monitoring Area**.



A confirmation dialog box appears.



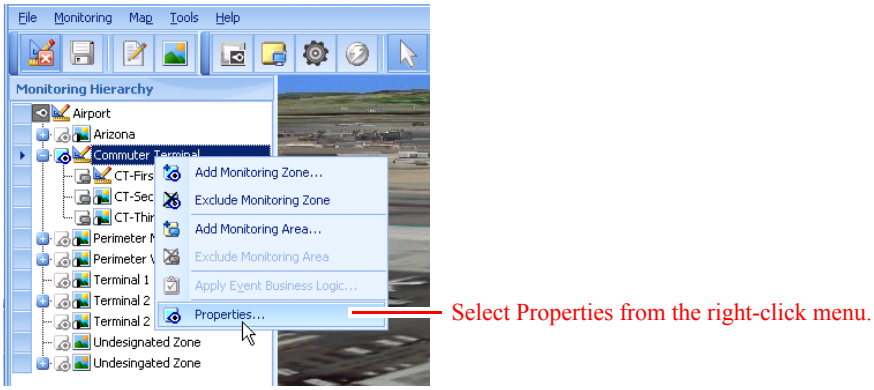
Step 2 Click the **Yes** button.

In either case, the node is excluded from the Monitoring Tree, but the underlying configuration for the zone or area is unaffected; the node will stay in the global pool.

Viewing Properties for Monitoring Tree Nodes

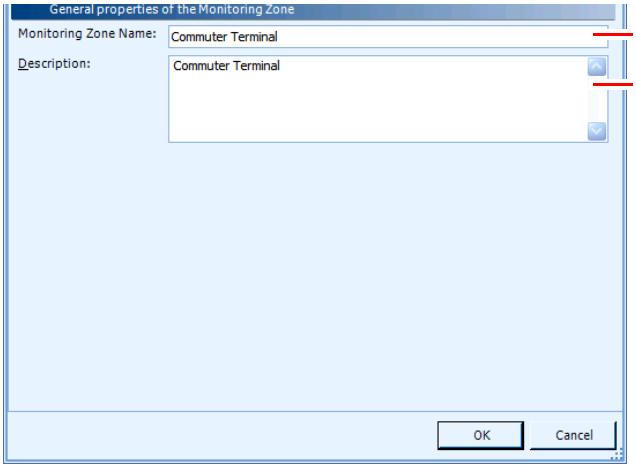
To view properties for a node:

Step 1 Right-click the node and select **Properties** from the right-click menu.

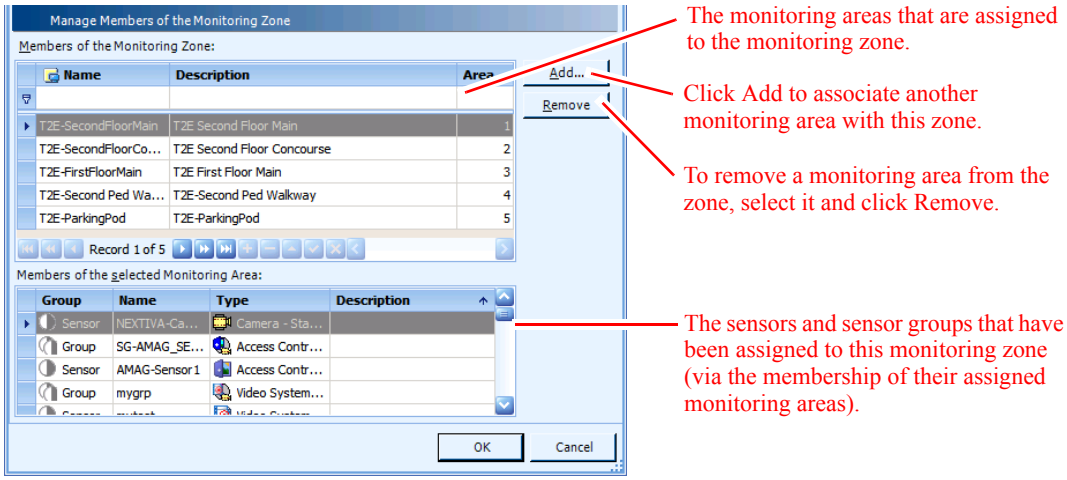


The Properties window appears with the **General** tab selected.

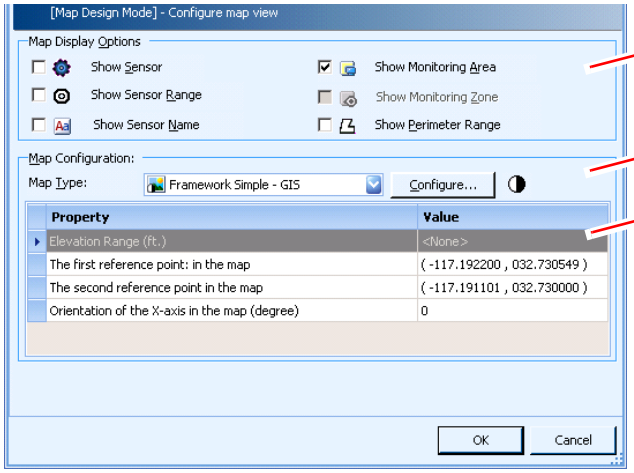
Note The windows shown in this section are for monitoring zone properties.



Step 2 To view the monitoring areas and sensors that are members of this monitoring zone, click the **Member** tab.

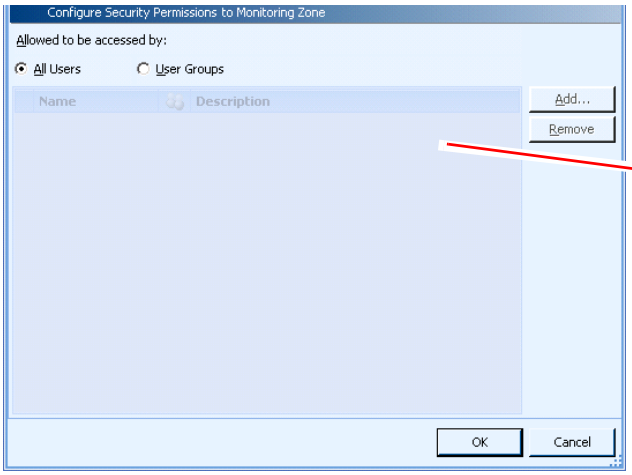


Step 3 To view the display settings for the zone's map area, click the **View** tab.



Note These options are only activated when you select **Map > Enter Map Design Mode** from the menu bar. To learn how to set these display properties from Design Mode, see the "Configuring Origin and Scale for a Map" section on page 7-6 and the "Setting Display Options for a Map" section on page 7-14.

Step 4 To view the security groups that have permission to view this monitoring zone, click the **Security** tab.



Step 5 When you're finished viewing properties for the monitoring zone, click **OK**.

Adding Maps to Monitoring Areas and Zones

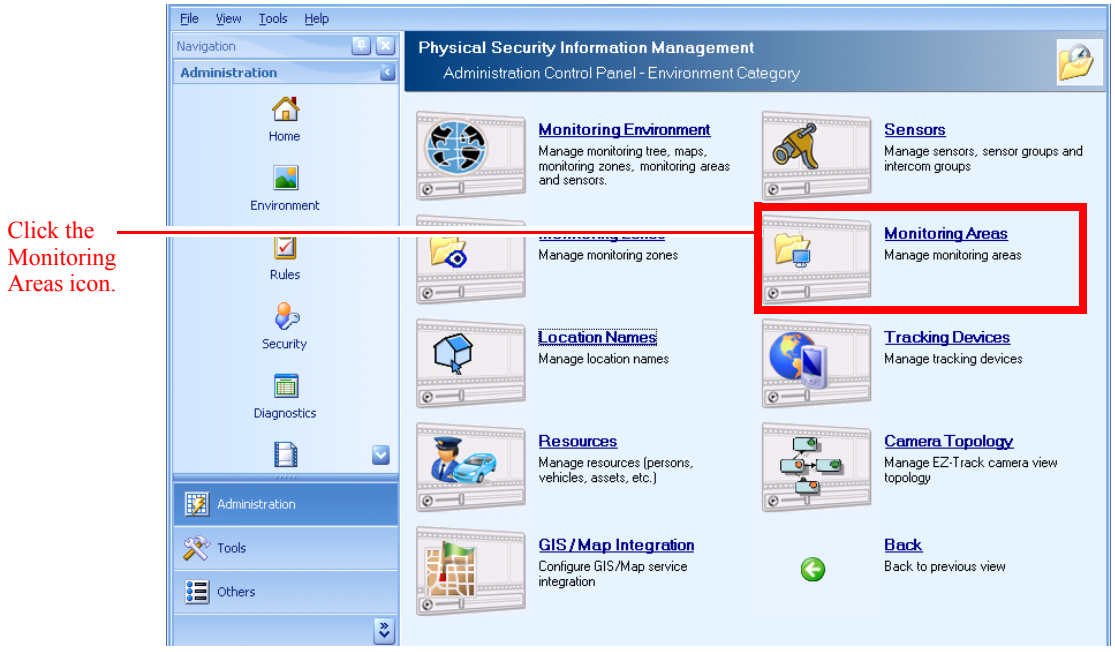
The next step to defining your monitoring zones and areas is to add appropriate background map or building plan images that will be displayed in the Map View Pane when the zone or area is selected in the Navigation Pane. See the "Adding Background Map Images" section on page 7-5 for instructions.

Editing or Deleting Monitoring Areas

To edit or delete a monitoring area:

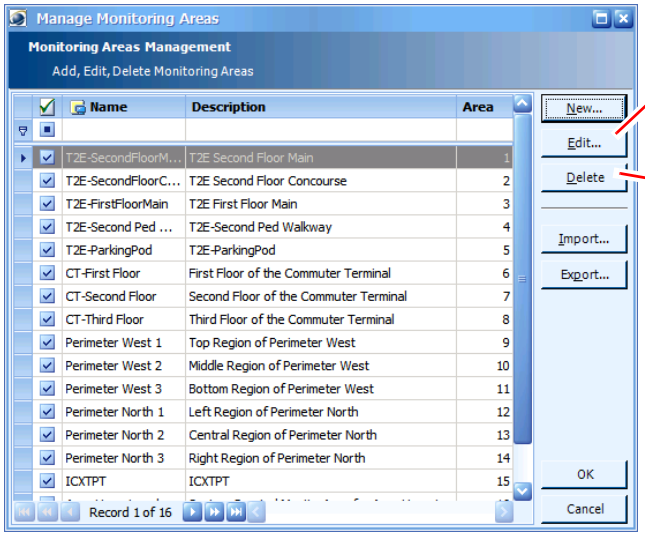
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.



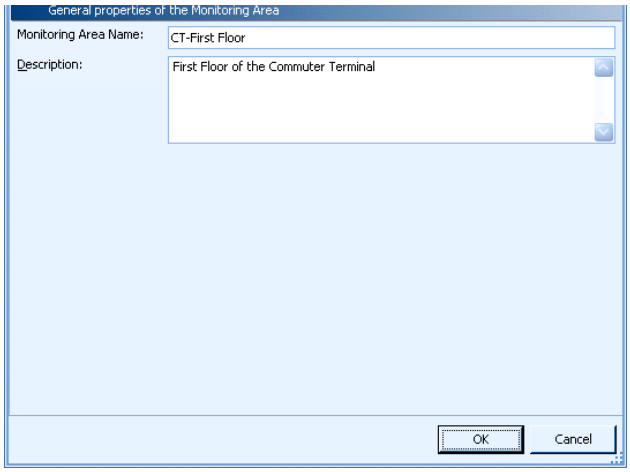
Step 2 Click the **Monitoring Areas** icon.

The Manage Monitoring Areas window appears.



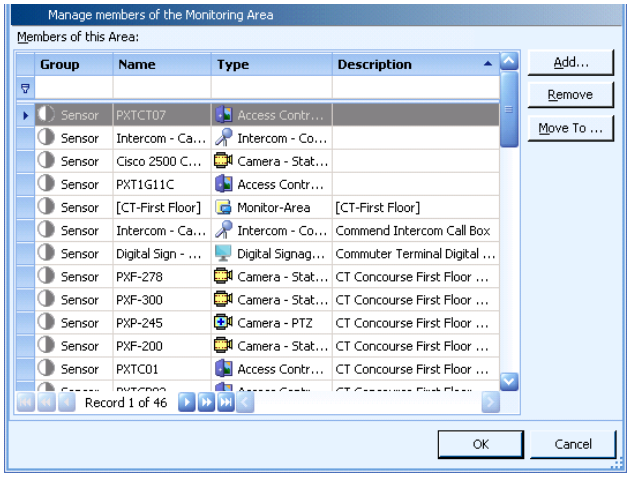
Step 3 **To edit a monitoring area,** select it and click the **Edit** button.

The Monitoring Area Properties window appears.



a. Enter a new name or description for the area on the **General** tab.

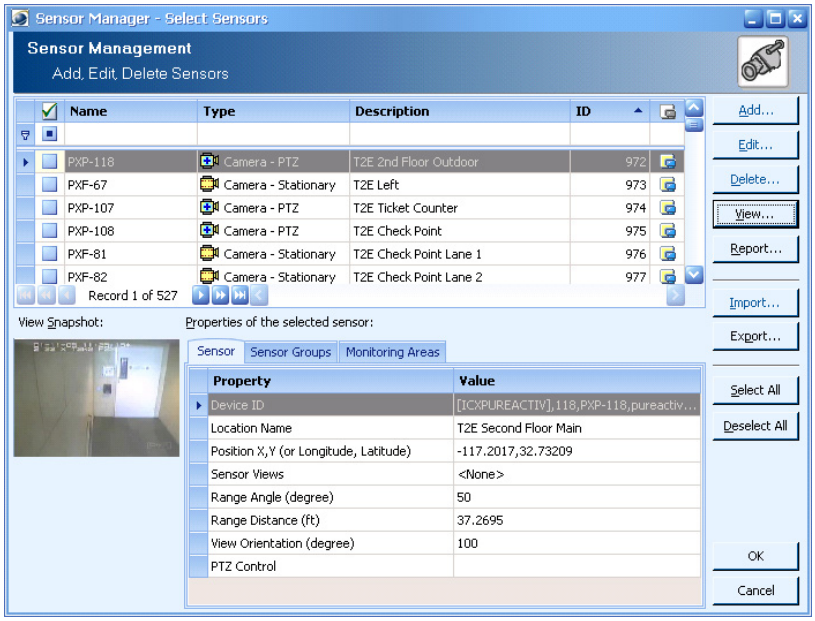
b. Click the **Member** tab.



c. To remove a sensor from the monitoring area, select it and click **Remove**.

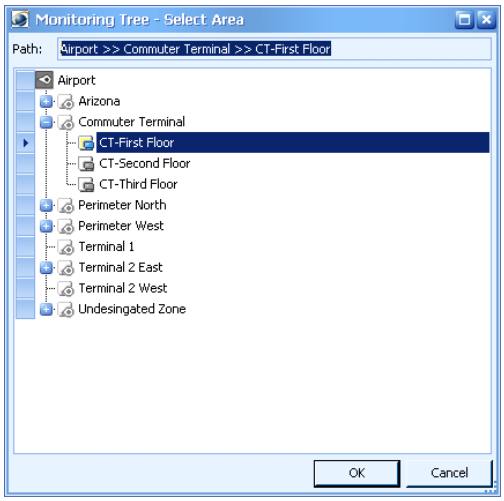
d. To add a sensor to the monitoring area, click **Add**.

The **Select Sensors** window appears where you can select the sensors you want to add and click **Add**.



e. To move the monitoring area to a different part of the Monitoring Tree, click the **Move To** button.

The **Monitoring Tree - Select Area** window appears.



Select the location where you want to move the monitoring area and click **OK**.

f. Click **OK** to store your changes. Any changes will be immediately reflected in the Monitoring Tree.

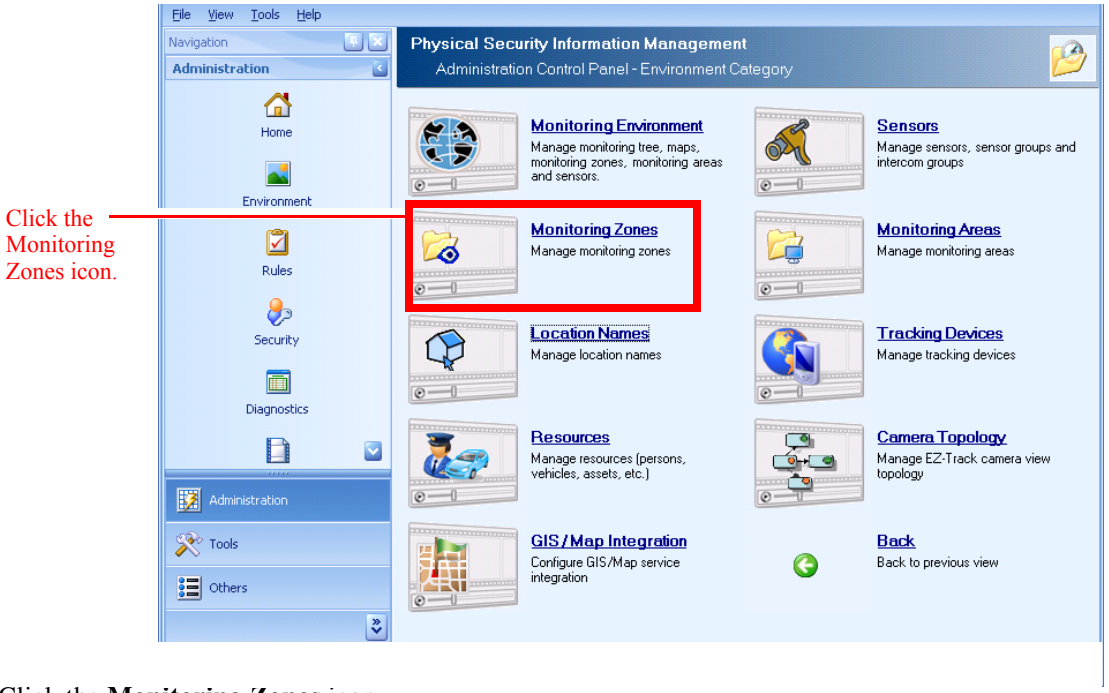
Step 4 To delete a monitoring area, click the **Delete** button. A confirmation dialog box appears. Click **Yes** to confirm the deletion. The monitoring area will be removed from the Monitoring Tree; and the monitoring area will be removed from the global pool.

Editing or Deleting Monitoring Zones

To edit or delete a monitoring zone:

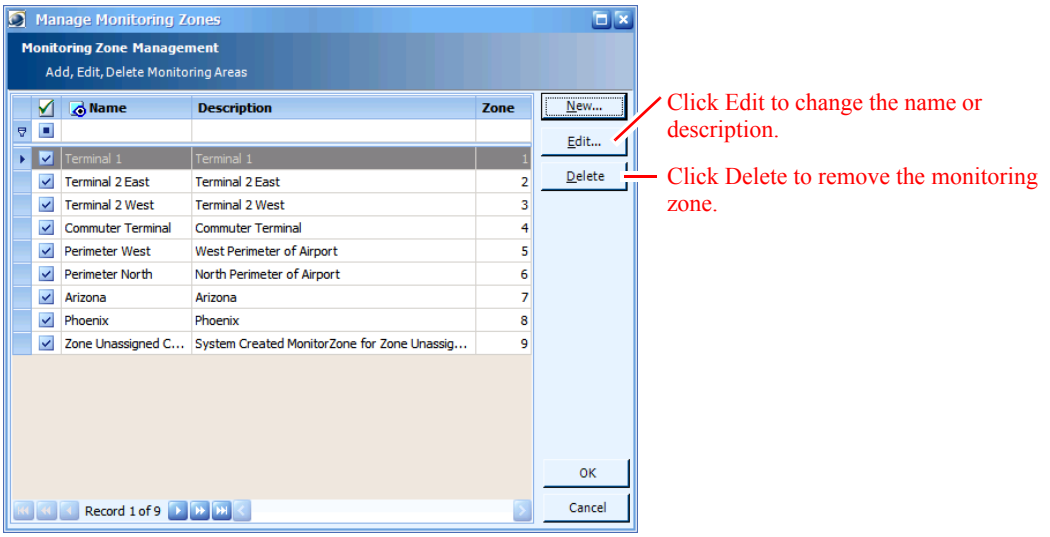
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

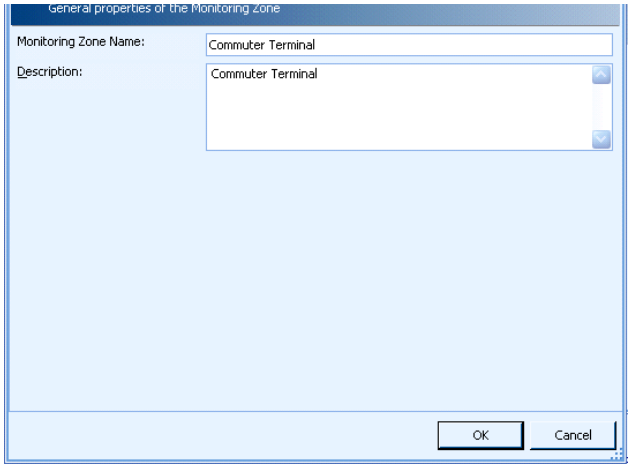


Step 2 Click the **Monitoring Zones** icon.

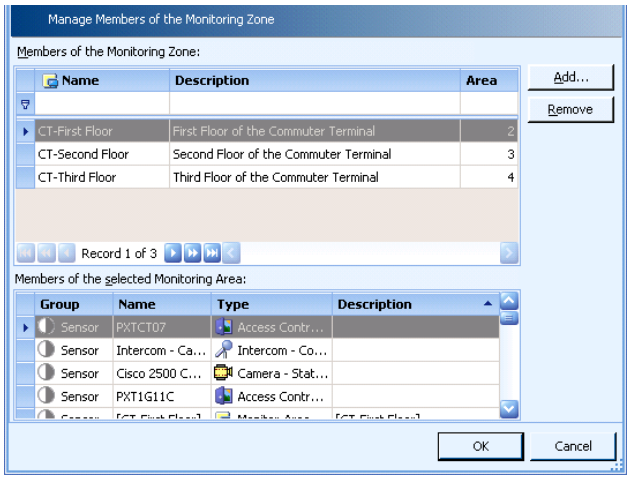
The Manage Monitoring Zones window appears.



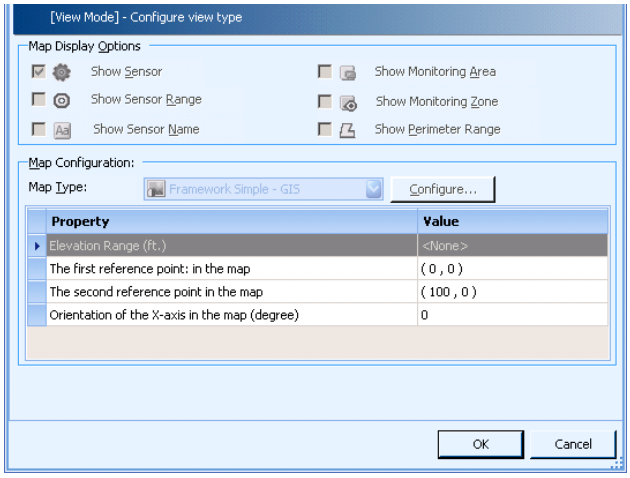
Step 3 To edit a monitoring zone, click the **Edit** button. In the Edit Monitoring Zone window you can change the name or description of the zone.



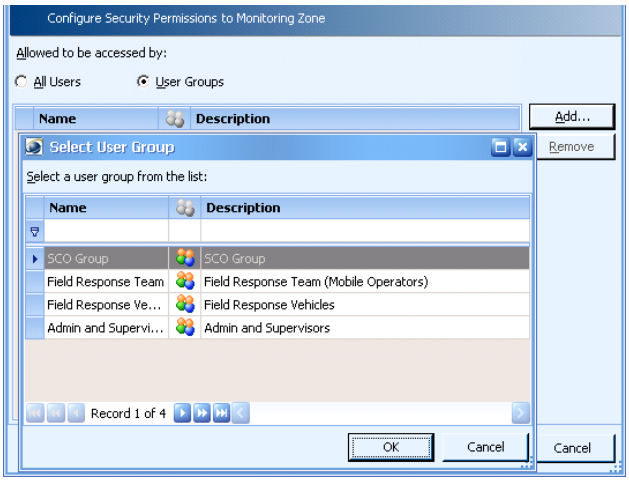
a. You can add monitoring areas to this monitoring zone by clicking the **Member** tab. Click the **Add** button to add a monitoring area.



b. You can change map view settings for the zone by clicking the **View** tab.



c. You can change the security settings for the monitoring zone by clicking the **Security** tab. Click **User Groups** and click the **Add** button to give a specific user group access to this monitoring zone. Select a user group and click **OK**.



d. Click **OK** to store your changes. These changes will automatically be made to the Monitoring Tree.

Step 4 To delete a monitoring zone, click the **Delete** button. A confirmation dialog box appears. Click **Yes** to confirm the deletion. The monitoring zone and its associated monitoring areas are removed from the Monitoring Tree. While the monitoring zone is deleted (it has also been removed from the global pool), its associated monitoring areas are not deleted from PSOM; they can be reassigned to a different monitoring zone.

Importing or Exporting Monitoring Areas

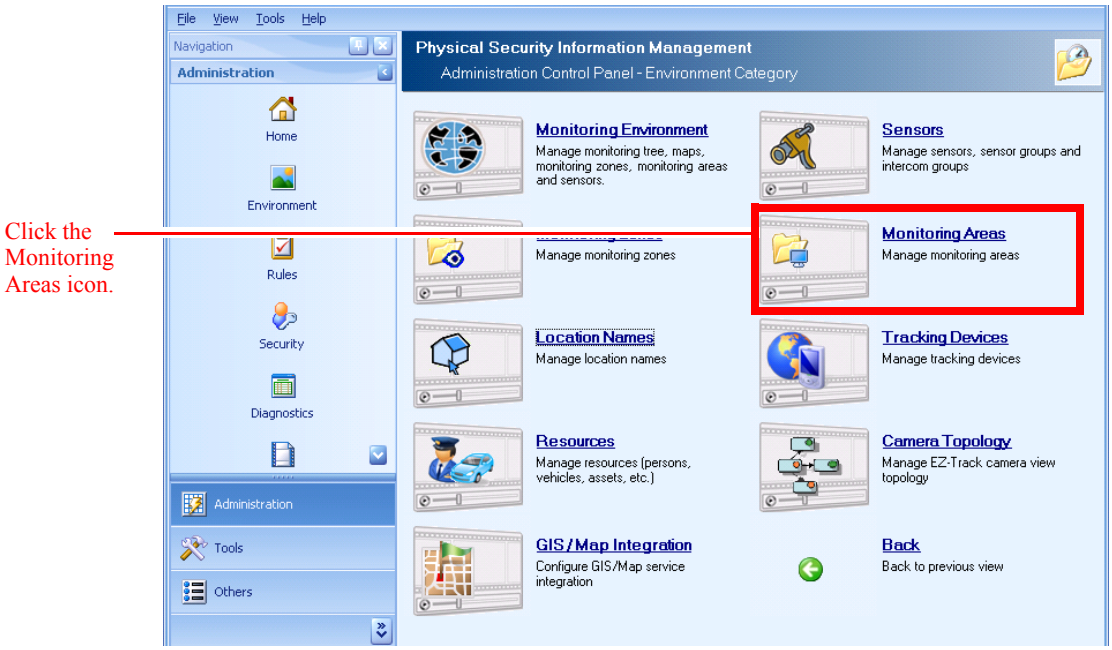
You can export monitoring area definitions from PSOM to an XML file, update the XML content in Microsoft Excel, and import the updated monitoring area definitions to PSOM.

Note See the "Importing and Exporting Sensors, Sensor Groups, and Intercom Groups with PSOM" section on page 6-36 for information about how to open the XML file in Microsoft Excel, edit the data, and save out to the correct format for re-import to PSOM.

To export or import monitoring areas:

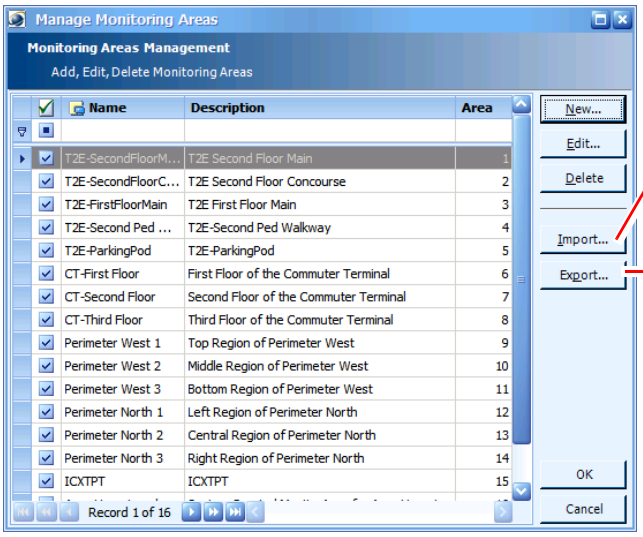
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.



Step 2 Click **Monitoring Areas** to manage your monitoring areas.

The Manage Monitoring Areas window appears.



Click the Import button to import monitoring areas, then select the XML file on your system that has the definitions.

Click the Export button to save an XML file with the monitoring areas defined in PSOM. It will save the file as PxArea.xml.

Step 3 Click **Import** to import monitoring areas from an XML file (should be named PxArea.xml), then select the XML file on your system that has the definitions.

Step 4 Click **Export** to save an XML file with the monitoring areas defined in PSOM. It will save the file as PxArea.xml.

CHAPTER 6

Managing Sensors

Every physical sensor in your environment (video cameras and access control devices) needs to be represented in PSOM with a *sensor* definition.

This chapter explains how to:

- Add access control devices as sensors in PSOM
- Add video camera devices from video servers as sensors in PSOM
- Add other types of devices—such as hazard detection devices—as sensors in PSOM
- Add camera view angle, distance, direction and field of view to the sensor definition
- Group sensors together for monitoring certain locations
- Group intercom devices together
- Import and export sensors, sensor groups, and intercom groups with PSOM

This chapter includes these topics:

- Types of Sensors and Connectors, page 6-1
- Planning Sensor Integration, page 6-2
- Adding New Sensors for Access Control Devices, page 6-2
- Adding new Sensors for Video Cameras, page 6-7
- Adding New Sensors for Other Types of Devices, page 6-16
- Editing Sensors, page 6-20
- Grouping Sensors, page 6-24
- Managing Intercom Device Groups, page 6-30
- Importing and Exporting Sensors, Sensor Groups, and Intercom Groups with PSOM, page 6-36

Types of Sensors and Connectors

To enable monitoring by PSOM, you must add sensor definitions for all sensor devices in your environment. PSOM integrates with these types of sensors:

- Cisco physical access control systems, and access control systems from other vendors.
- Cisco Video Surveillance IP Cameras, and cameras from other vendors.
- Hazard or fire detector systems such RAE Systems.

- Intelligent video (IV) systems.
- Intercom or Public Announcement (PA) systems.
- Radar and sonar devices.
- Digital signage systems.
- Microwave systems.
- Electronic fence systems.
- Intrusion detection systems.
- Emergency duress systems.
- IP devices.
- HVAC (heating, ventilating and air conditioning systems).
- BAC (Basic Access Control (BAC) systems used to read passports).
- Glass Break Detector.
- Seismic Detector.
- UPS (Universal Power Supply).
- Gas Detector.

Once sensors are added to PSOM for each device, they can be associated with certain locations and then grouped together as necessary.

Planning Sensor Integration

PSOM can access the database for external systems to obtain a list of active devices if the connection has been established and is active. Otherwise, you will need to know the device IDs of all devices to be monitored by PSOM. See the Integration Module documentation for instructions on integrating various external systems with PSOM; install PxDocSetup.msi to obtain all PSOM documentation.

PSOM can also access video servers (such as Vicon Video Server) to obtain a list of active video camera devices if the connection has been established and is active. For better presentation in PSOM, you can optionally add information about the camera's view range angle (in degrees), view distance (in feet), and view direction (in degrees). You will need to collect this information for each video camera you are adding to PSOM.

Appendix A, "Planning Worksheets," includes a planning table you can use for this video camera planning purpose—Table A-4 on page A-5.

Note Camera view direction moves counter-clockwise (0 to 359 degrees); 0 degrees means the camera is pointing to the right, 180 degrees indicates the camera is pointing to the left.

Adding New Sensors for Access Control Devices

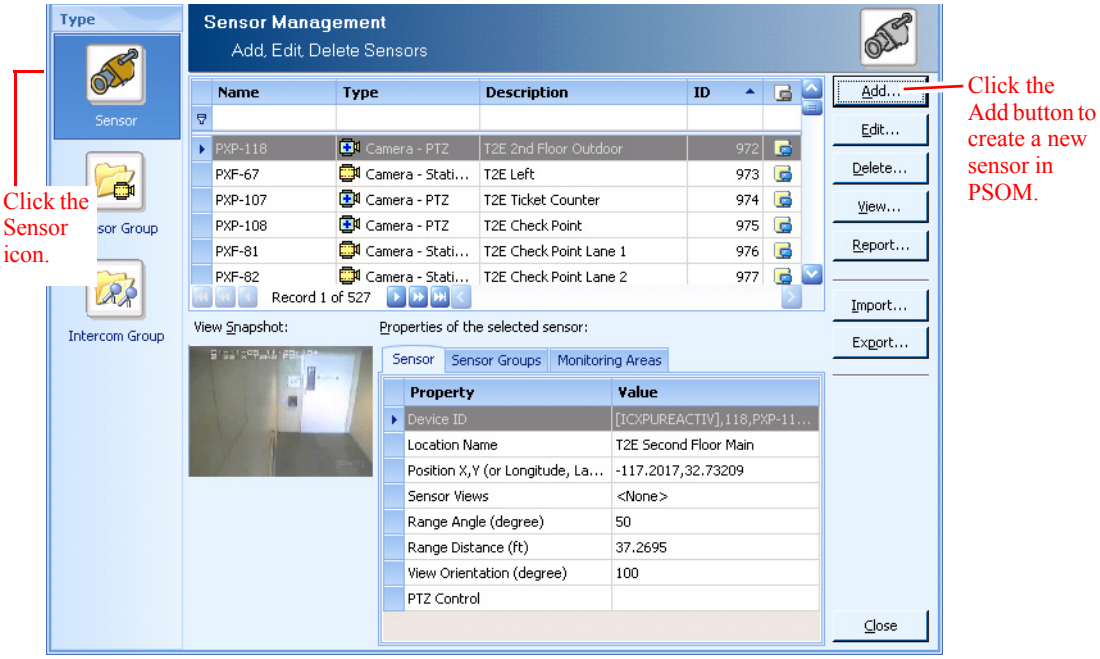
To add a new sensor for an access control device:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

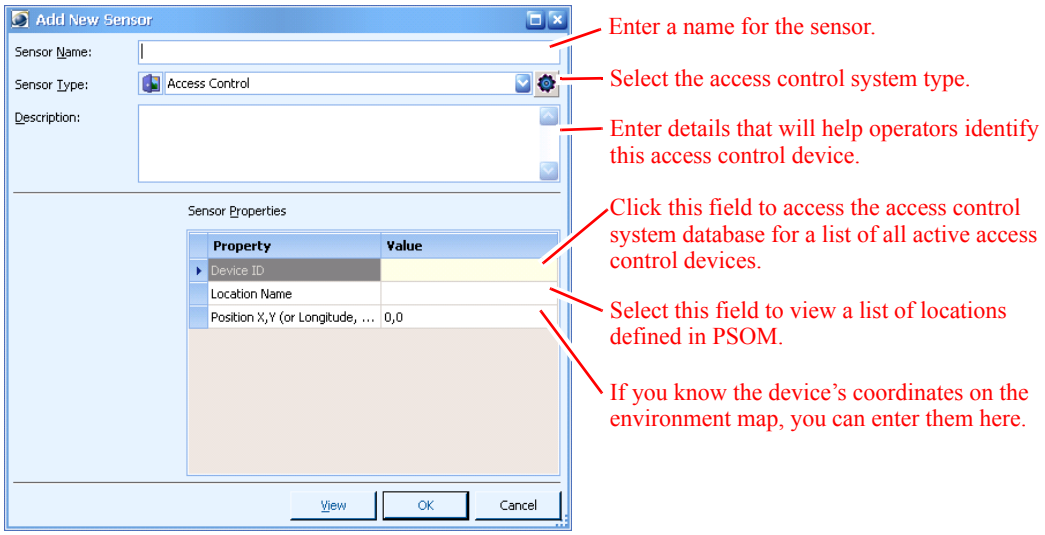
The Sensor Management window appears.



Step 3 Click the **Sensor** icon to display a list of all sensors defined for PSOM.

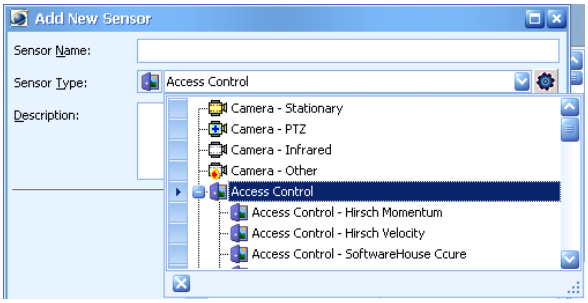
Step 4 Click the **Add** button to create a new sensor definition.

The Add New Sensor window appears.



Step 5 In the **Sensor Name** field, enter the name you want displayed for this sensor on the maps in the Map View Pane and in the Alert Details window of the Operation Console.

Step 6 From the **Sensor Type** field, select the type of your access control system, for example **Access Control - Cisco Physical Access Control**.



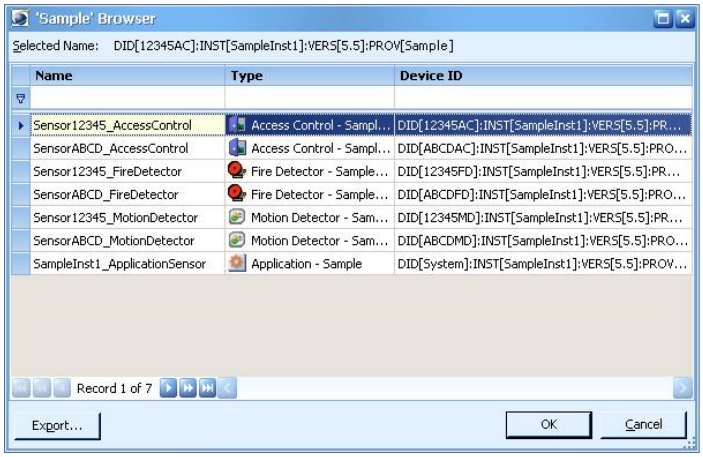
If you want to sort the sensor types by vendor, click the button and select the access control sensor from the **Sensor Type** field according to vendor.

Step 7 In the **Description** field, enter details that will help operators identify this access control device quickly when an alert condition happens.

Step 8 Click the button in the **Device ID** field to connect to the access control system's database and view a list of all access devices.

A window opens with a list of all devices.

If you've clicked the button in the Sensor Type field and selected a vendor, then clicking the button in the **Device ID** field opens a window similar to this.



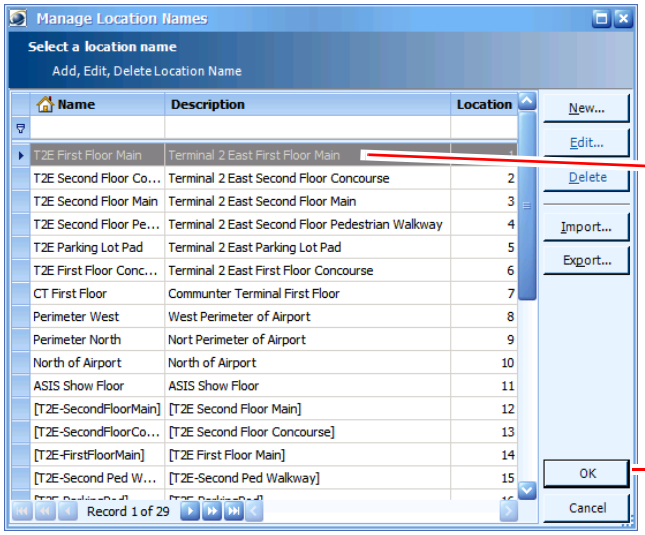
Step 9 Select the device you want to associate with the PSOM sensor.

Step 10 Click **OK**.

Note If you know the device ID, you can manually enter it into the **Device ID** field without having to access the access control's database. However, the name you enter must exactly match the device's ID in the access control database.

Step 11 Back in the Add New Sensor window, select the **Location Name** field.

The Manage Location Names window appears with a list of all locations defined for PSOM. See Chapter 4, "Defining Locations," for information.

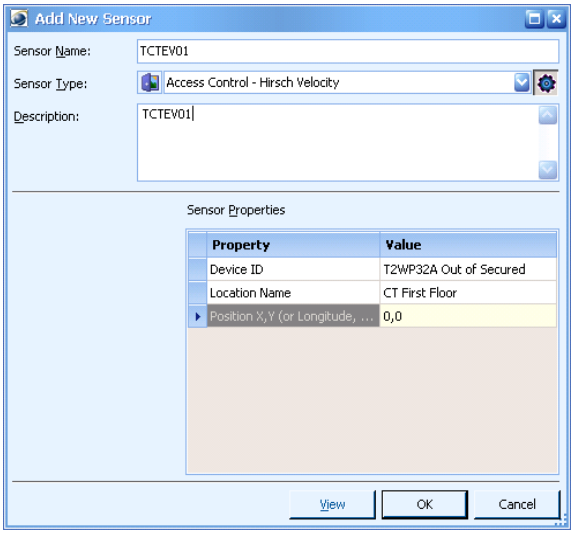


Step 12 Select the location with which you want to associate this sensor.

Step 13 Click **OK**.

Step 14 Back in the Add New Sensor window, you can enter the sensor's placement within the environment map into the **Position (X,Y)** field. If you do not know this value, you can leave it as [0,0] for now. The sensor's coordinates will be automatically updated once the sensor is placed on the environment map.

The final Add New Sensor window should appear similar to the following.



Step 15 Click **OK** to save the new sensor.

Adding new Sensors for Video Cameras

PSOM supports these types of video cameras: stationary, PTZ, infrared and other. When adding a sensor for a video camera, you complete the same information for each type of video camera.

There are special settings to configure EZ-Track. See Chapter 12, "Setting Up EZ-Track."

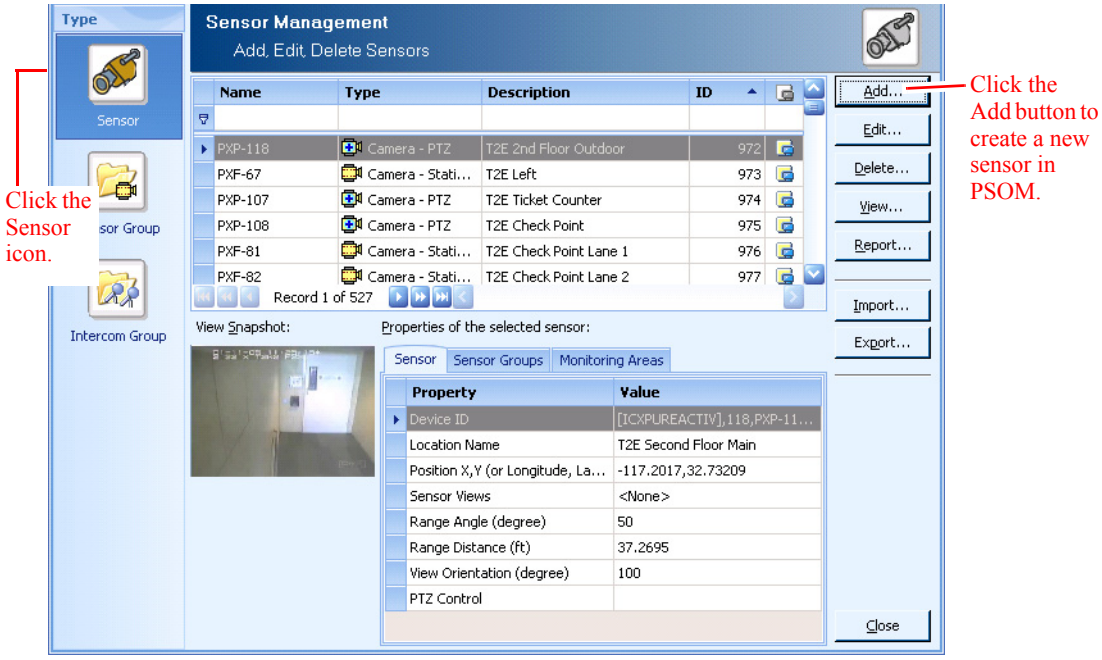
To add a new sensor for a video camera:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

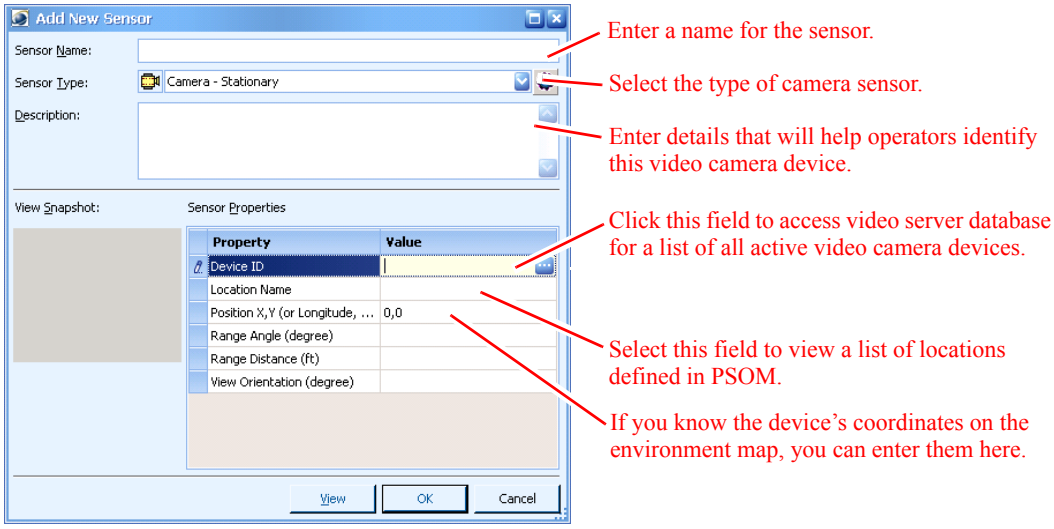
The Sensor Management window appears.



Step 3 Click the **Sensor** icon to display a list of all sensors currently defined for PSOM.

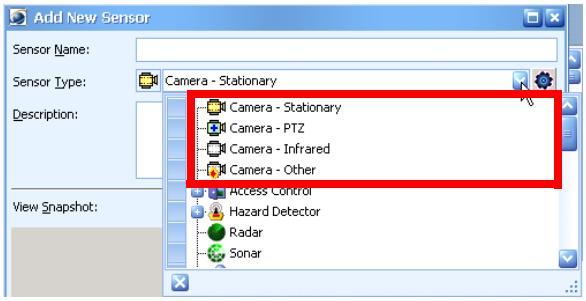
Step 4 Click the **Add** button to create a new sensor definition.

The Add New Sensor window appears.



Step 5 In the **Sensor Name** field, enter the name you want displayed for this sensor on the maps in the Map View Pane and in the Alert Details window of the Operation Console.

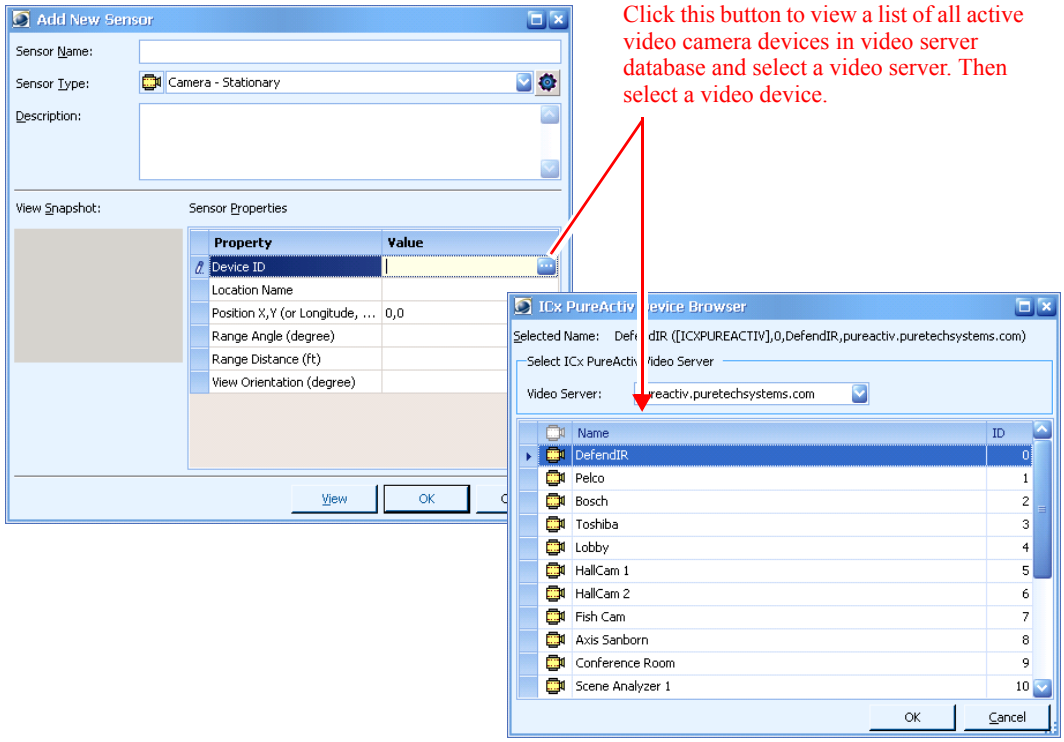
Step 6 From the **Sensor Type** field, select one of the video camera types. For example, select **Camera - Stationary**, **Camera - PTZ**, **Camera - Infrared**, or **Camera - Other**.



Step 7 In the **Description** field, enter details that will help operators identify this video camera quickly when an alert condition happens.

Step 8 Click the button in the **Device ID** field to connect to the video server's database and view a list of all video cameras.

A window opens with a list of all video cameras in the video server's database.



Click this button to view a list of all active video camera devices in video server database and select a video server. Then select a video device.

Note If PSOM cannot access the video server to display a list of camera sensors, you will need to manually enter the camera information into the Add New Sensor window.

Step 9 Select the video camera device you want to associate with the PSOM sensor.

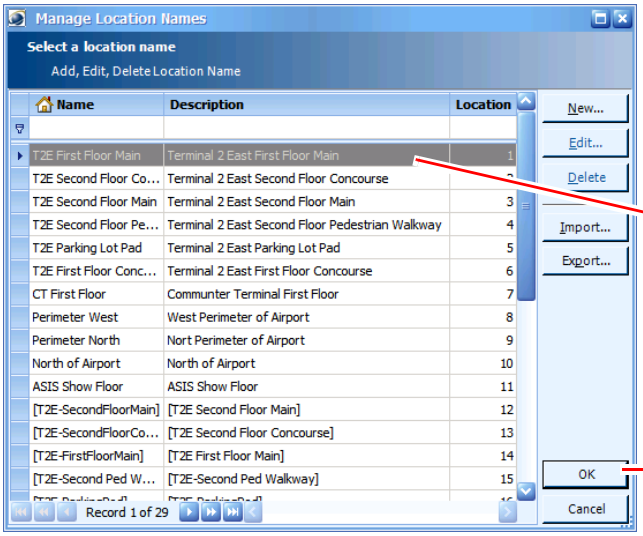
Step 10 Click **OK**.

Note If you know the device ID, you can manually enter it into the **Device ID** field without having to access the video server's database. The camera sensor's device ID is different from the device name and each vendor has a different format.

Note If the video server supports it, you can export the sensor list to XML, modify the sensor information, and then re-import the XML into PSOM. See the "Importing and Exporting Sensors, Sensor Groups, and Intercom Groups with PSOM" section on page 6-36.

Step 11 Back in the window, select the **Location Name** field.

The Manage Location Names window appears with a list of all locations defined for PSOM. See Chapter 4, "Defining Locations," for information.

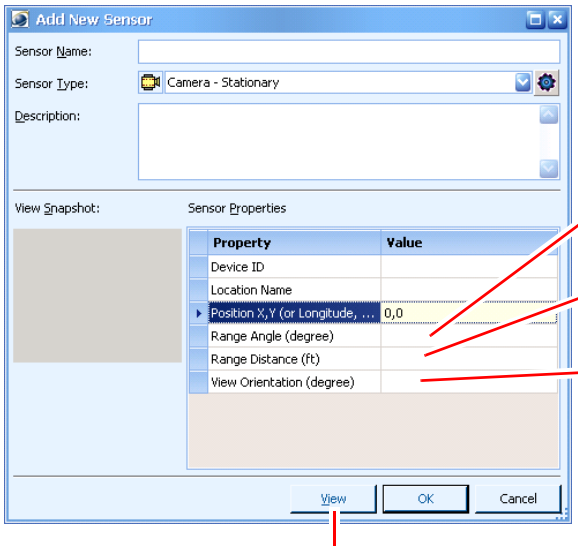


Step 12 Select the location with which you want to associate this sensor.

Step 13 Click **OK**.

Step 14 Back in the Add New Sensor window, you can enter the sensor's placement within the environment map into the **Position (X,Y)** field.

Note If you do not know this value, you can leave it as [0,0] for now. The sensor's coordinates will be automatically updated once the sensor is placed on the map.



Note You can enter the camera's range angle, distance and orientation in this dialog box, or you can visually provide this information when you add the camera sensor to a map. See the "Adding Sensors to a Map" section on page 7-21 for details.

Step 15 In the **Range Angle (degree)** field, enter the width of the camera's viewing area in degrees.

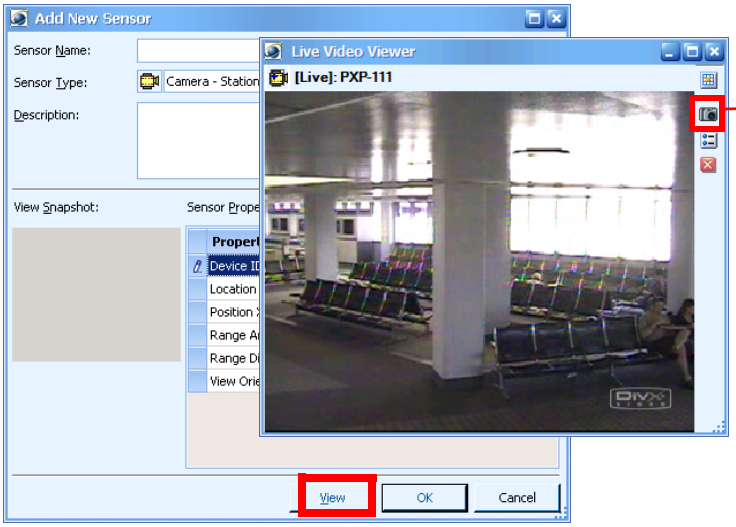
Step 16 In the **Range Distance (ft)** field, enter the distance from the camera to the furthest point it can accurately view.

Step 17 In the **View Orientation (degree)** field, enter the angle of the camera view in degrees (counter-clockwise from 0-359 degrees). 0 degrees indicates the camera is pointing to the right, 180 degrees indicates the camera is pointing to the left.

Note All of these settings are important for setting up EZ-Track. See Chapter 12, "Setting Up EZ-Track."

Step 18 To add a field of view (FOV) image to the sensor definition, click the **View** button.

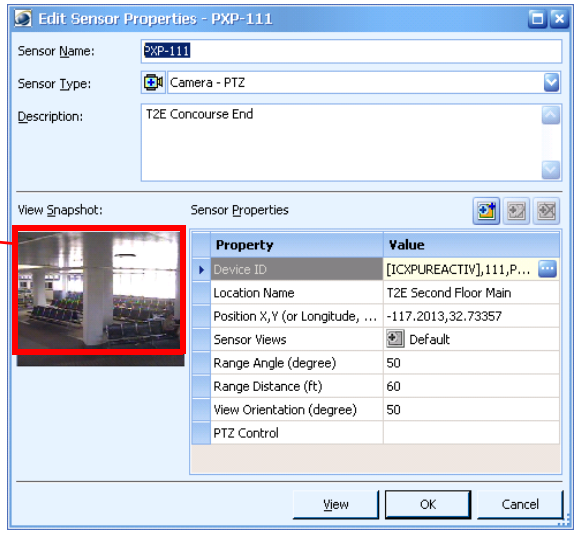
The Live Video Viewer window appears.



Click the Take Snapshot button to take a still image of the video feed from this camera that will be added to the sensor's definition in PSOM.

Step 19 Click the **Take Snapshot** button in the **Live Video Viewer** to capture a still image.

The camera FOV is displayed in the Add New Sensor window.



This image shows operators the view from this video camera.

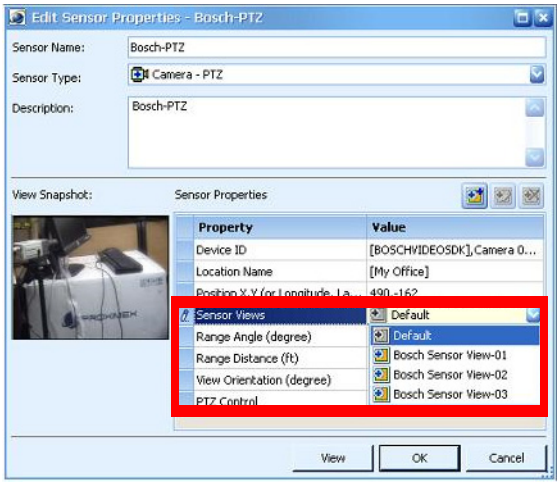
If you're configuring a PTZ camera, see the "Setting Up PTZ Preset Positions" section on page 6-12.

Step 20 Click **OK** to save the new sensor.

Setting Up PTZ Preset Positions

By defining *sensor views* for a PTZ camera sensor, you can enable PTZ cameras in PSOM to visually move between actual preset positions that are defined in the video management system.

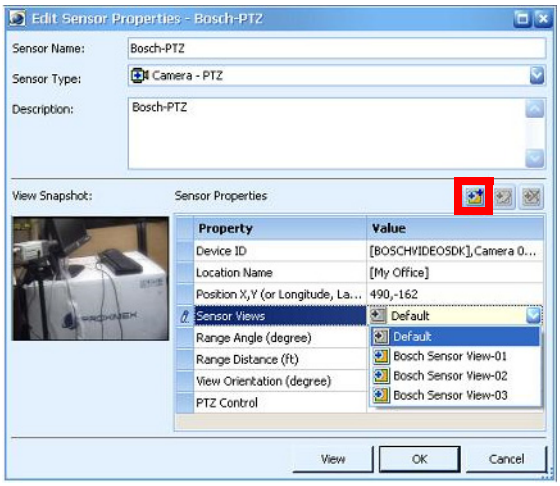
The following PTZ sensor has three sensor views defined for it.



Each of these sensor views corresponds to a camera preset position obtained from the DVR/NVR.

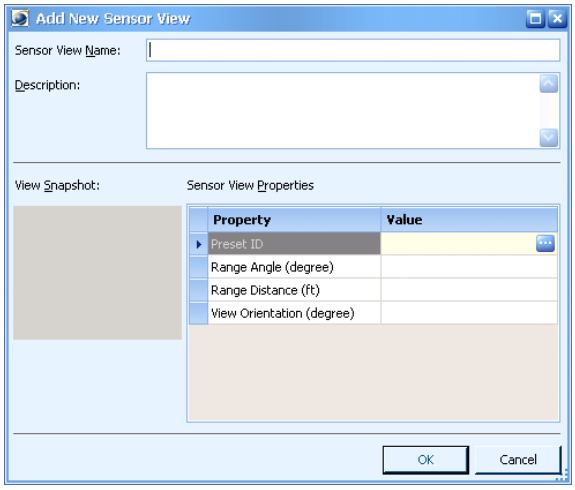
To add a sensor view:

Step 1 Edit the sensor for the PTZ camera by selecting it in the **Sensor** tab in the Sensor Management window and clicking **Edit**.



Step 2 Click the button to add a new sensor view.

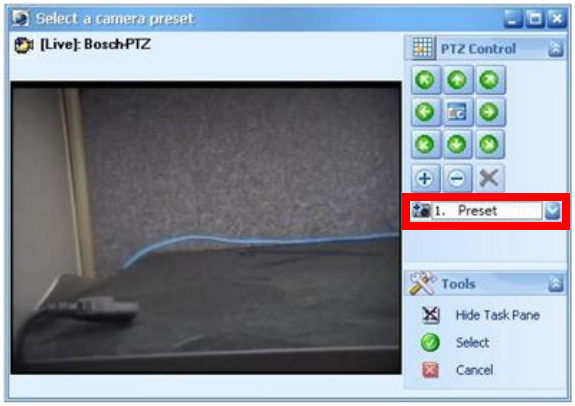
The Add New Sensor View window appears.



Step 3 Enter a name for the sensor view in the Sensor View Name field.

Step 4 In the **Preset ID** field, click the ... button.

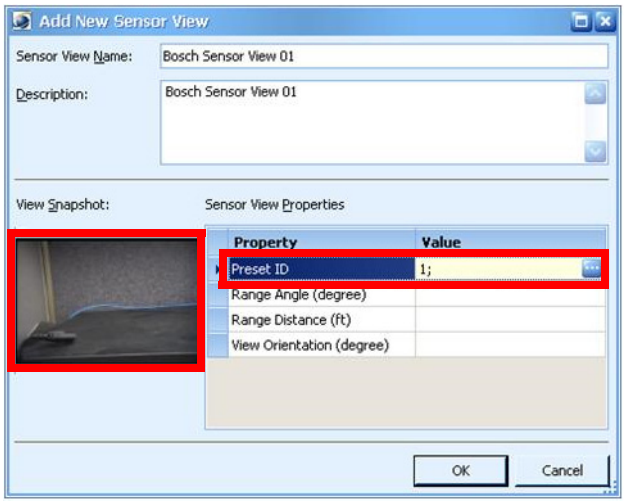
The Select a camera preset window appears.



Step 5 Select a preset view from the drop-down menu on the right side of the window.

Step 6 Click **Select**.

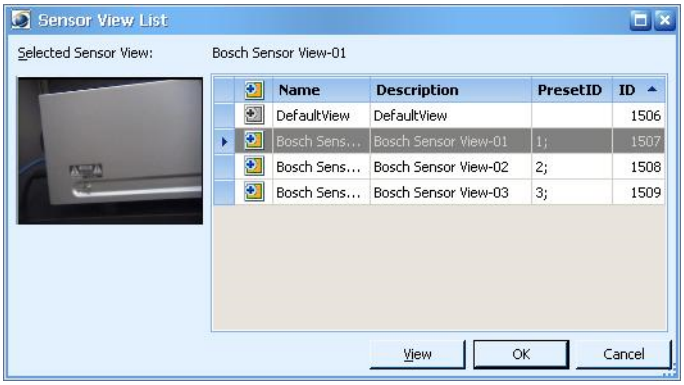
The preset camera position is added as a sensor view and given a pre-defined name; for example, {ID};{Name}. A snapshot is taken and automatically assigned to the sensor view.



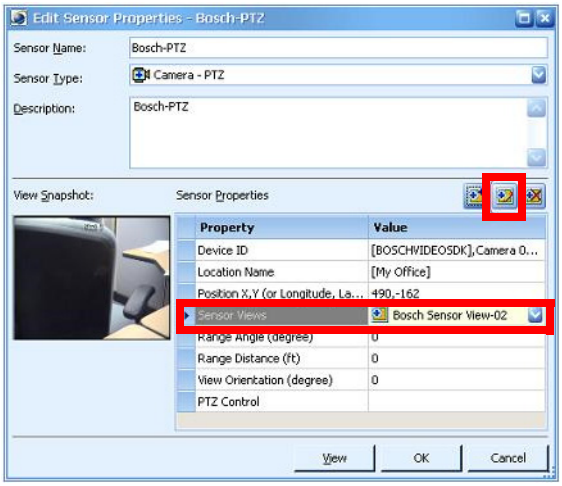
Step 7 Click **OK** to add the sensor view.

Step 8 To see the sensor views that have been configured for a sensor, double-click the **Sensor Views** field in the Edit Sensor Properties window.

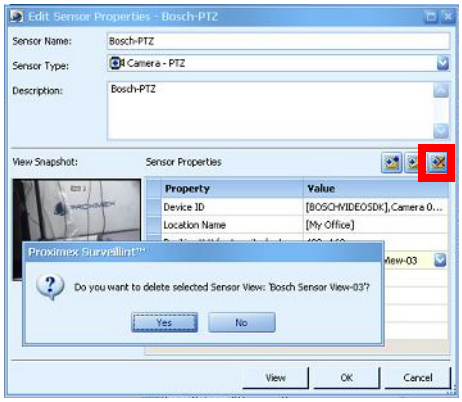
The Sensor View List window appears.



Step 9 To edit an existing sensor view, select it from the **Sensor Views** field and click the **Edit Sensor View** button.



Step 10 To delete an existing sensor view, select it from the **Sensor Views** field and click the **Delete Sensor View** button. Click **Yes** when prompted.

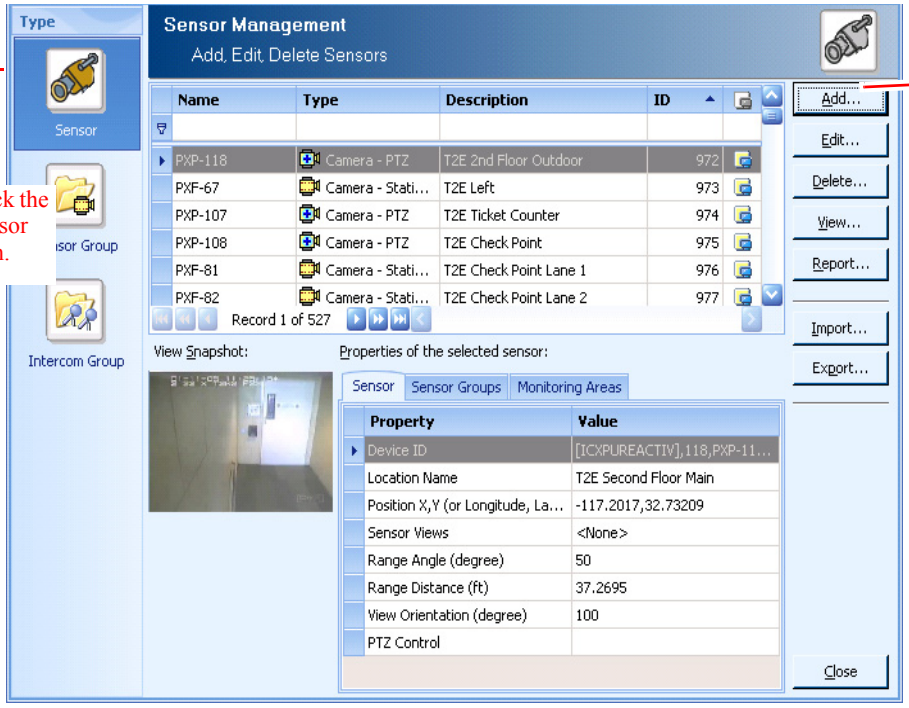


Adding New Sensors for Other Types of Devices

Adding new sensors for devices other than access control and video cameras is essentially the same, and instructions are covered in this section.

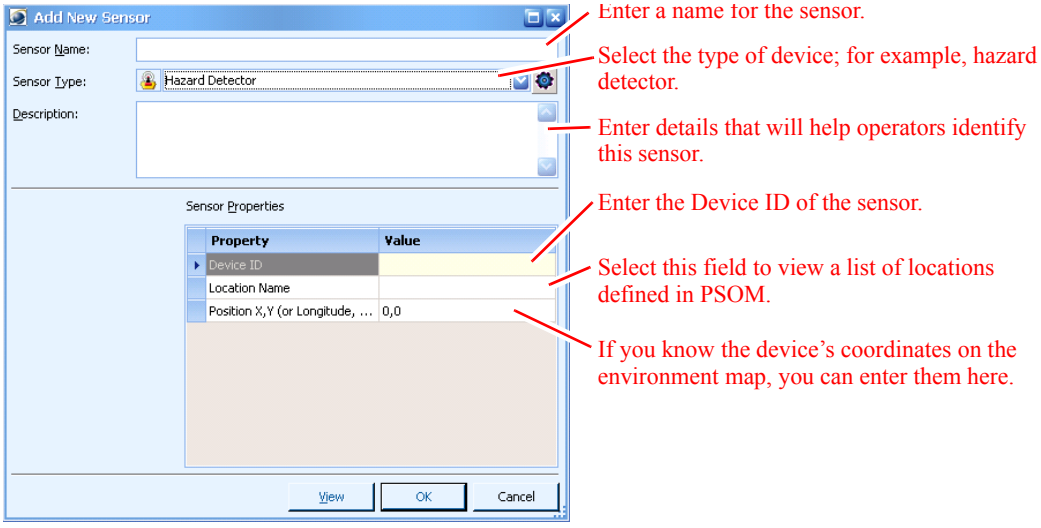
To add a new sensor for a device in your environment:

Step 1 In the Sensor Management window, click the **Sensor** icon.



Step 2 Click the **Add** button to create a new sensor definition.

The Add New Sensor window appears.



Step 3 In the **Sensor Name** field, enter the name you want displayed for this sensor on the maps in the Map View Pane and in the Alert Details window of the Operation Console.

Step 4 From the **Sensor Type** field, select the type of device for which you want to add a sensor; for example **Hazard Detector**.

Choices in the **Sensor Type** field are shown in Table 6-1.

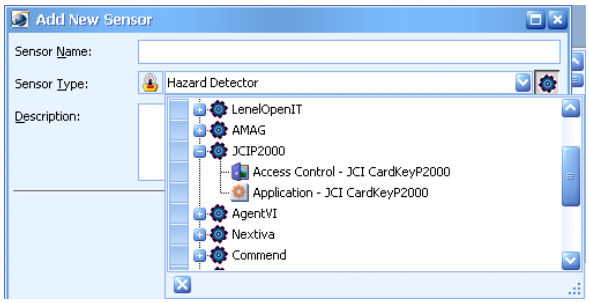
Table 6-1 Sensor Type Filed Choices

Sensor Icon	Description
	Hazard detector. Integrates with hazard detection systems like RaeSystems.
	Radar. Integrates with radar devices that are used to detect, range (determine the distance of), and map various types of targets.
	Sonar. Integrates with sonar devices that are used for acoustic location.
	Intercom. Integrates with Public Announcement (PA) systems such as Intercom-Commend.
	Digital signage. Integrates with electronic displays that are installed in public spaces.
	Digital signage—Cisco Digital Media Player. Integrates with electronic displays powered by Cisco Digital Media Player.
	Monitor-area. Assigns the alert to a monitoring area rather than a sensor.
	Fire detector. Integrates with devices that detect smoke and issue alarms.
	Microwave. Integrates with reconfigurable microwave networks; for example, reconfigurable wireless communication, wireless network, and reconfigurable phase array antenna.
	Fence. Integrates with electronic fence security systems.
	Intrusion detector. Integrates with software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.
	Emergency duress. Integrates with emergency communication systems such as panic alarms.
	AED. Integrates with automated external heart defibrillators.
	Computer. Integrates with computers on the network.
	Video systems. Integrates with intelligent video systems such as Agent VI or Verint Nextiva.
	IP device. Integrates with instrumented components such as those that provide information and notification via Windows Management Instrumentation (WMI).
	HVAC device. Integrates with heating, ventilating and air conditioning systems.
	BAC device. Integrates with Basic Access Control (BAC) systems used to read passports.
	Glass break detector. Integrates with devices that detect a break in a pane of glass, alerting a burglar alarm.
	Seismic detector. Integrates with systems that detect seismic activity.
	UPS device. Integrates with Universal Power Supply (UPS) systems.
	Gas detector. Integrates with systems that detect the presence of various gases within an area, usually as part of a system to warn about gases which might be harmful to humans or animals.
	Computer aided dispatch. Integrates with systems that dispatch taxicabs, couriers, field service technicians, or emergency services assisted by computer.
	Carbon monoxide detector. Integrates with systems that detect the presence of carbon monoxide within an area.

Table 6-1 Sensor Type Filed Choices (continued)

Sensor Icon	Description
	Motion detector. Integrates with systems that quantifies motion that can be either integrated with or connected to other devices that alert the user of the presence of a moving object within the field of view.
	Application. Sends an alert if a PSOM Integration Module encounters systematic problems with a third-party sensor, such as loss of connection or initialization problems. Use of the Application sensor is specific to the Integration Module and covered in the relevant documentation.

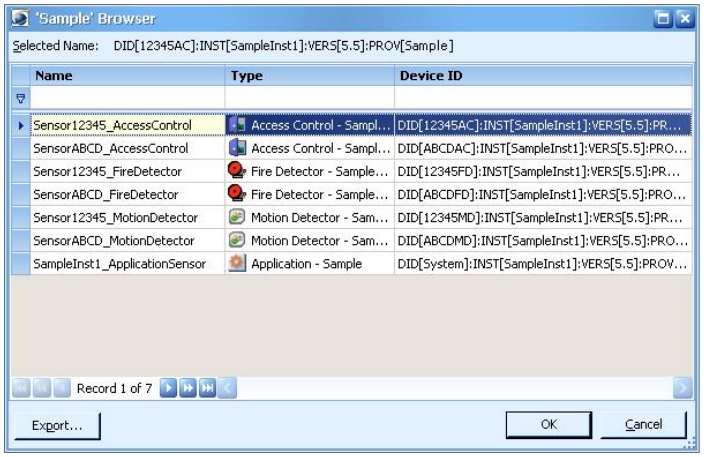
If you would prefer, you can click the button and select the sensor from the **Sensor Type** field according to vendor.



Step 5 In the **Description** field, enter details that will help operators identify this device quickly when an alert condition happens.

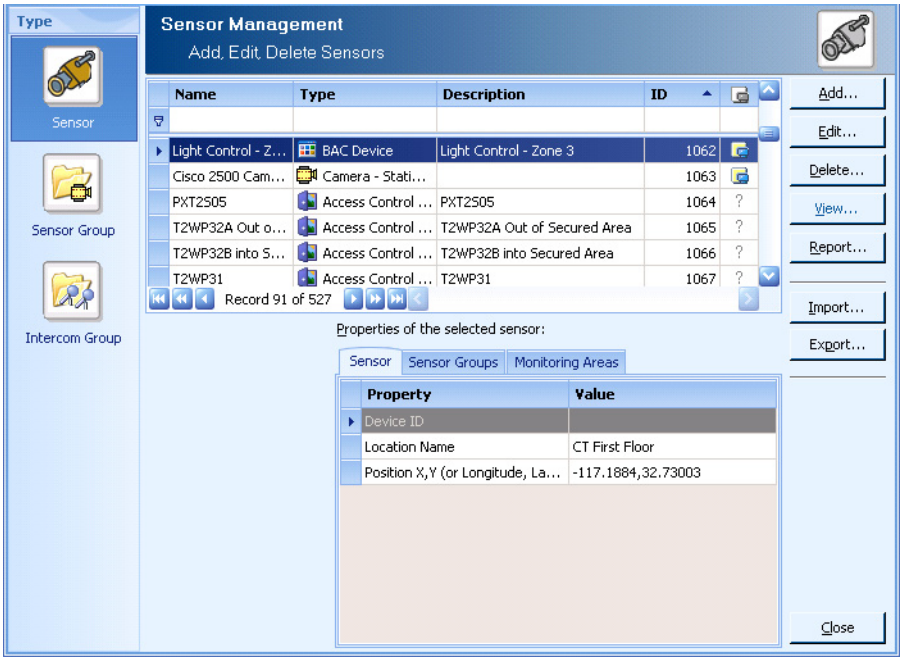
Step 6 In the **Device ID** field, enter the device ID. Check with your system integrator to get the necessary information.

If you've clicked the button in the Sensor Type field and selected a vendor, then clicking the button in the **Device ID** field opens a window similar to this.



Step 7 Click **OK** to save the new sensor.

The Sensor Management window appears with the new sensor added.



Editing Sensors

You can view sensor properties, the sensor groups to which a sensor belongs, and the monitoring areas in which the sensor is active, from the Sensor Management window. You can also edit a sensor's properties from this window.

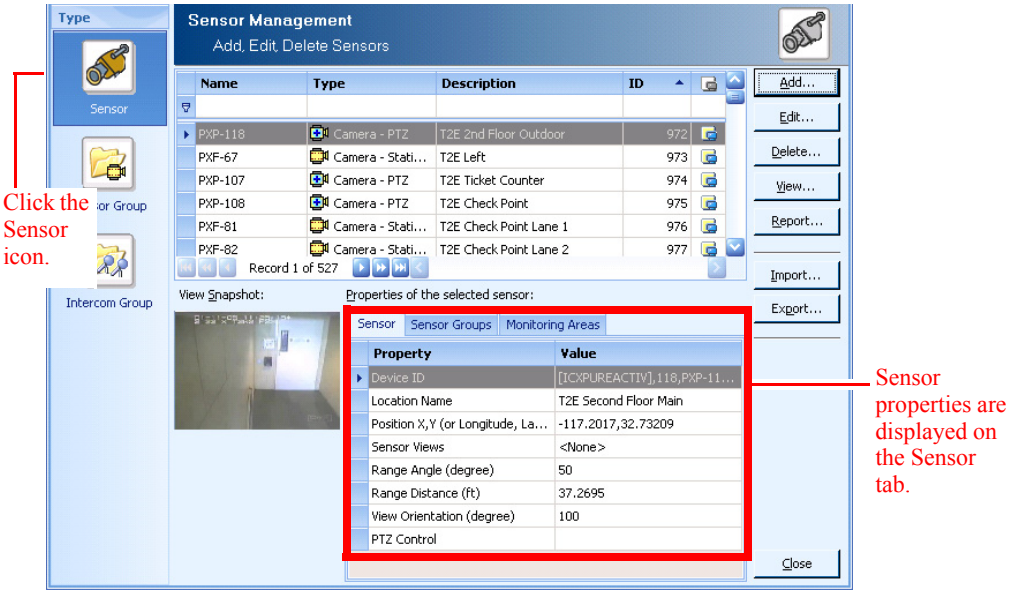
To edit a sensor's properties:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

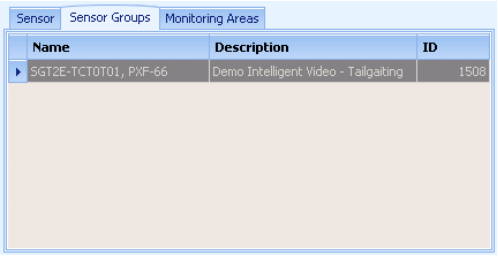
The Sensor Management window appears.



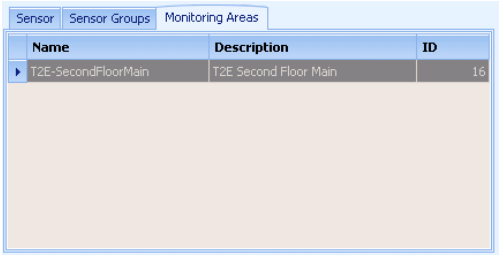
Step 3 Click the **Sensor** icon to display a list of all sensors currently defined for PSOM.

Step 4 Select the sensor you want to view or edit. It's sensor properties are displayed on the **Sensor** tab.

Step 5 Click the **Sensor Groups** tab to show the groups to which the sensor belongs.

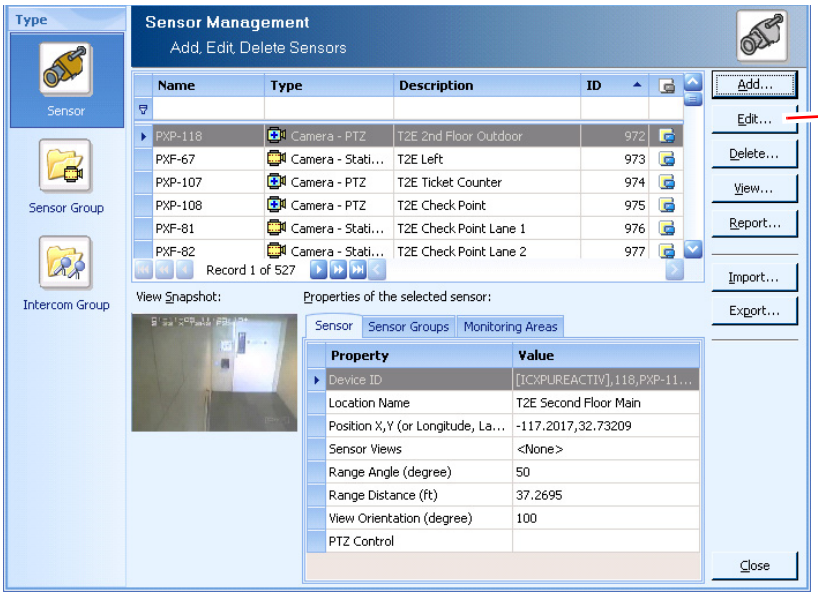


Step 6 Click the **Monitoring Areas** tab to show the locations where the sensor is active.



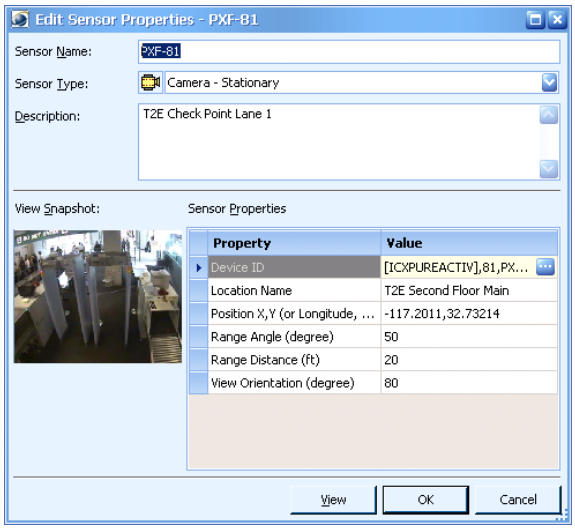
If the sensor is active in one or more monitoring areas, the sensor list indicates this with a monitoring area icon in the last column.

Step 7 Click the **Edit** button to change the sensor's definition.



Select the sensor you want to change and click the Edit button.

The Edit Sensor window appears.



Step 8 Edit properties as desired and click **OK** to save changes.

Grouping Sensors

A sensor *group* is a logical association of sensors designed to collect information about incidents occurring in a certain location. For example, you might associate a video camera sensor with an access control door so that when an alarm occurs at the door, you capture the incident on the associated video camera.

Types of Sensor Groups

You can create the following types of sensor groups.

Icon	Sensor Group	Description
	General Group	This group contains any types of sensors which have no associated rule.

Adding a Sensor Group

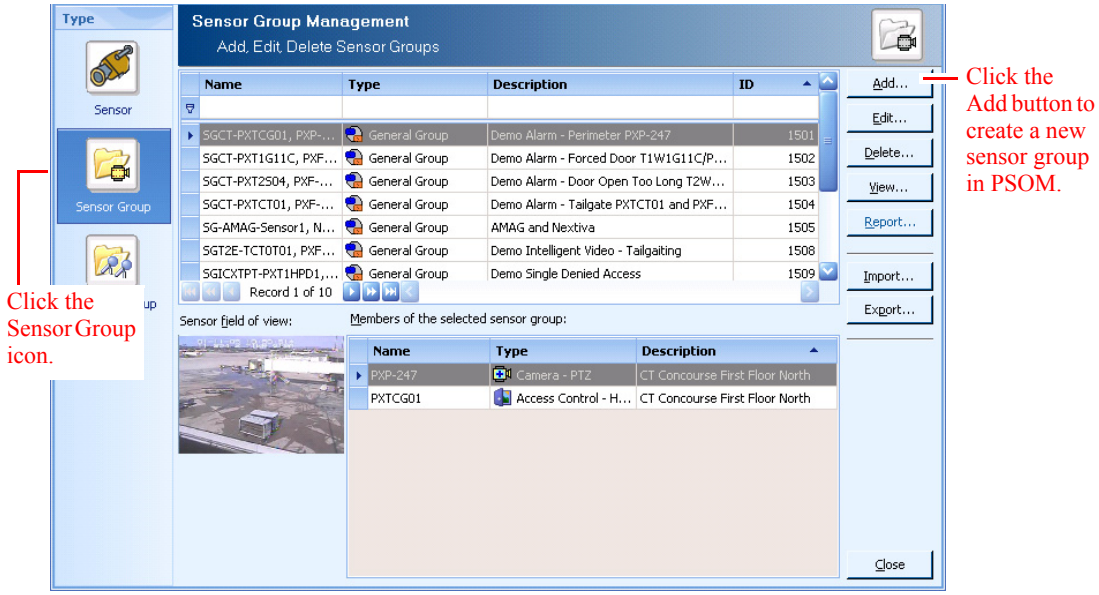
To add a new sensor group:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

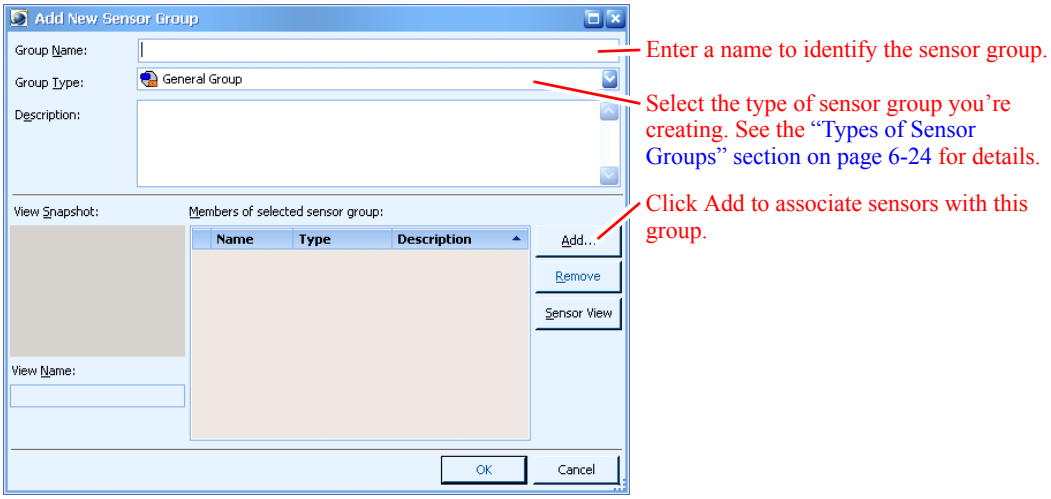
The Sensor Management window appears.



Step 3 Click the **Sensor Group** icon to display a list of all sensor groups currently defined for PSOM.

Step 4 Click the **Add** button to add a new sensor group.

The Add New Sensor Group window appears.



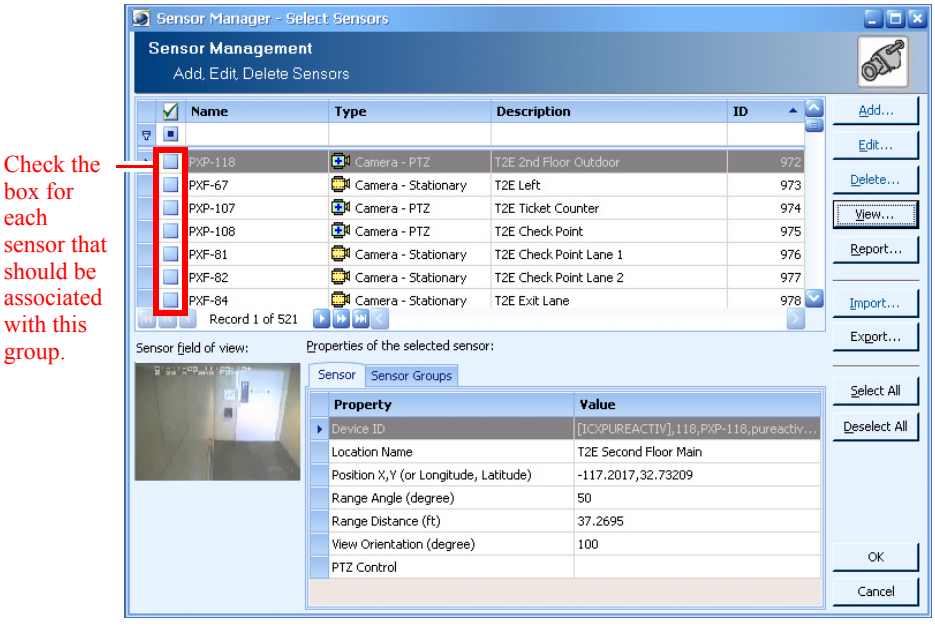
Step 5 In the **Group Name** field, enter the name you want to assign to this collection of sensors.

Step 6 From the **Group Type** field, select the type of sensor group you want to create. For example, select **General Group**.

Step 7 In the **Description** field, enter details about this sensor group that will help operators determine the location, the access control devices that are being monitored, and the video cameras that are involved.

Step 8 Click the **Add** button to select sensors that should be associated with this group.

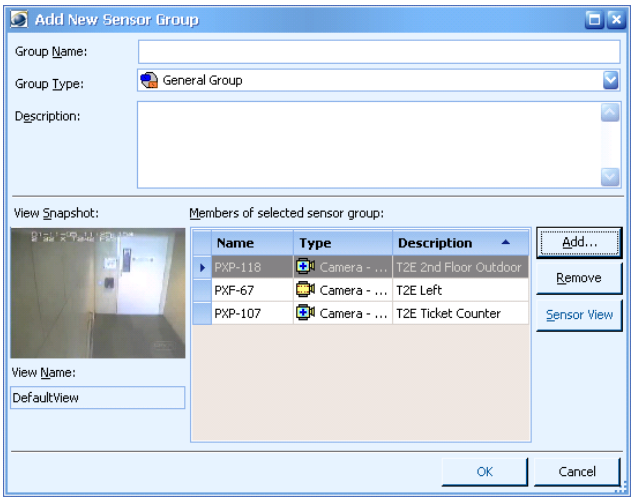
The Select Sensors window appears.



Step 9 Check the boxes for each sensor in the list that should be added to this group.

Step 10 Click **OK** to save your selections.

The selected sensors are added to the "Members" area of the Add New Sensor Group window.



Note If your sensor group includes a PTZ camera, the primary sensor view configured for the PTZ camera appears under **View Name**.

Step 11 Click **OK** to save your sensor group.

Editing a Sensor Group

You may want to edit a sensor group to change its member sensors, or to modify its description.

Note If you add or remove members in a sensor group, you need to first remove the sensor group from its monitoring area. Once you've modified membership to the sensor group, you can re-assign the sensor group to the monitoring area. See the "Editing or Deleting Monitoring Areas" section on page 5-20 for instructions.

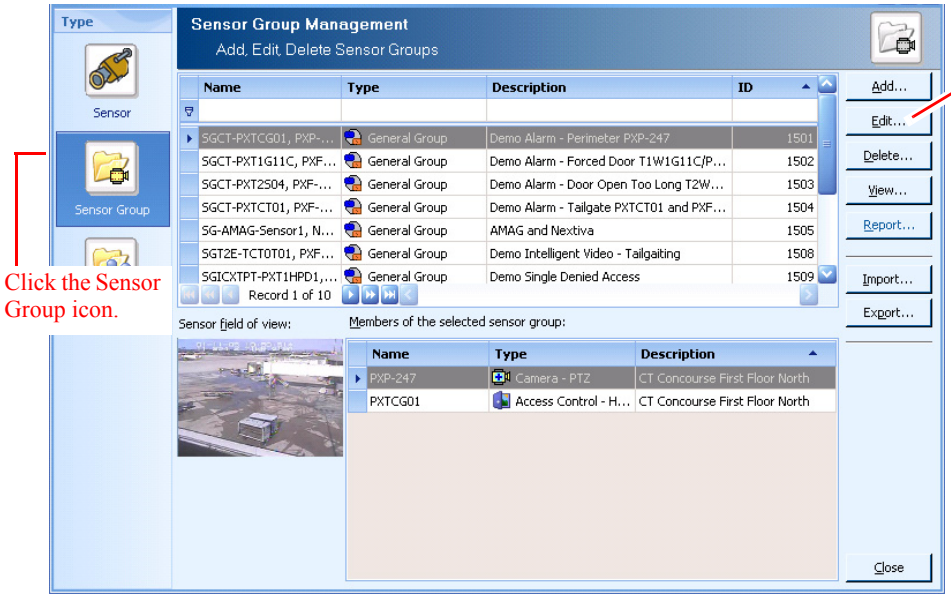
To edit a sensor group:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

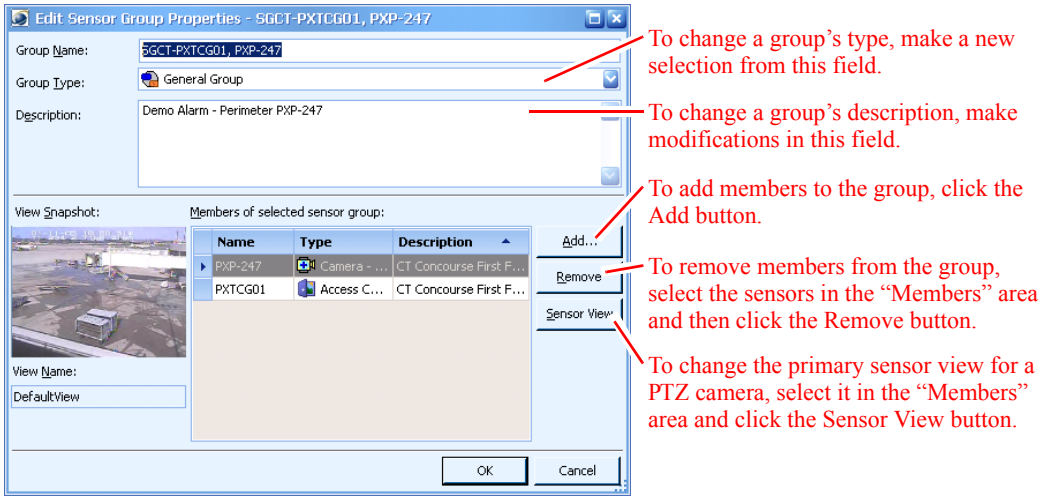
The Sensor Management window appears.



Step 3 Click the **Sensor Group** icon to display a list of all sensor groups currently defined for PSOM.

Step 4 Select the group from the list and click the **Edit** button to change it.

The Edit Sensor Group Properties window appears.



Step 5 To change the group's type, make a different selection from the **Group Type** field.

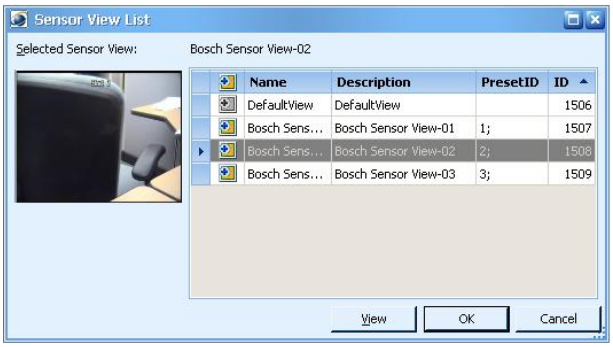
Step 6 To change the description, enter modifications in the **Description** field.

Step 7 To add new members to the sensor group, click the **Add** button. When the Select Sensors window appears, check boxes for the sensors you want to add to the group, and click **OK**.

Step 8 To remove a member from the sensor group, select the sensor from the list under "Members..." and click the **Remove** button.

Step 9 To change the primary sensor view for a PTZ camera in the sensor group, select the PTZ camera from the "Members..." list and click **Sensor View**.

The Sensor View List window appears.



Select the view you want to assign to the PTZ camera for this sensor group and click **OK**.

Click **View** to define a new view for the sensor group. The **Live Video Viewer** appears to allow you to select the new view.

Step 10 Click **OK** to save your changes.

Deleting a Sensor Group

To remove a sensor group:

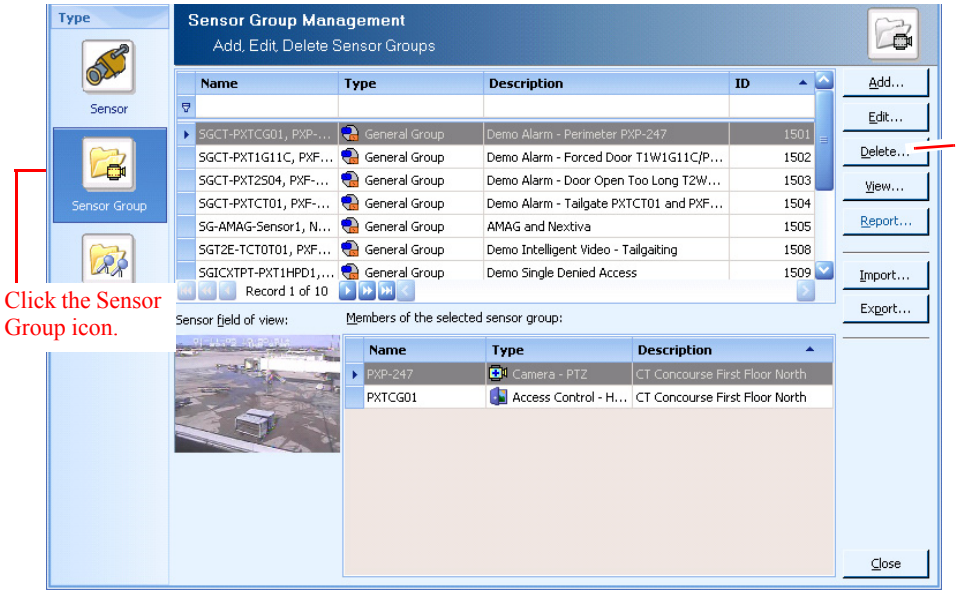
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

Step 3 Click the **Sensor Group** icon.

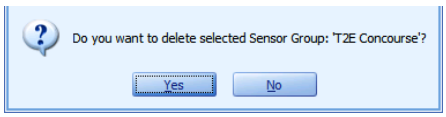
The Sensor Management window appears.



Step 4 Click the **Sensor Group** icon to display a list of all sensor groups.

Step 5 Select the sensor group you want to remove, and click the **Delete** button.

A confirmation dialog box appears.



Step 6 Click **Yes** to verify the deletion.

Managing Intercom Device Groups

You can group intercom devices together in PSOM so that you can broadcast announcements to these devices from PSOM.

Adding an Intercom Device Group

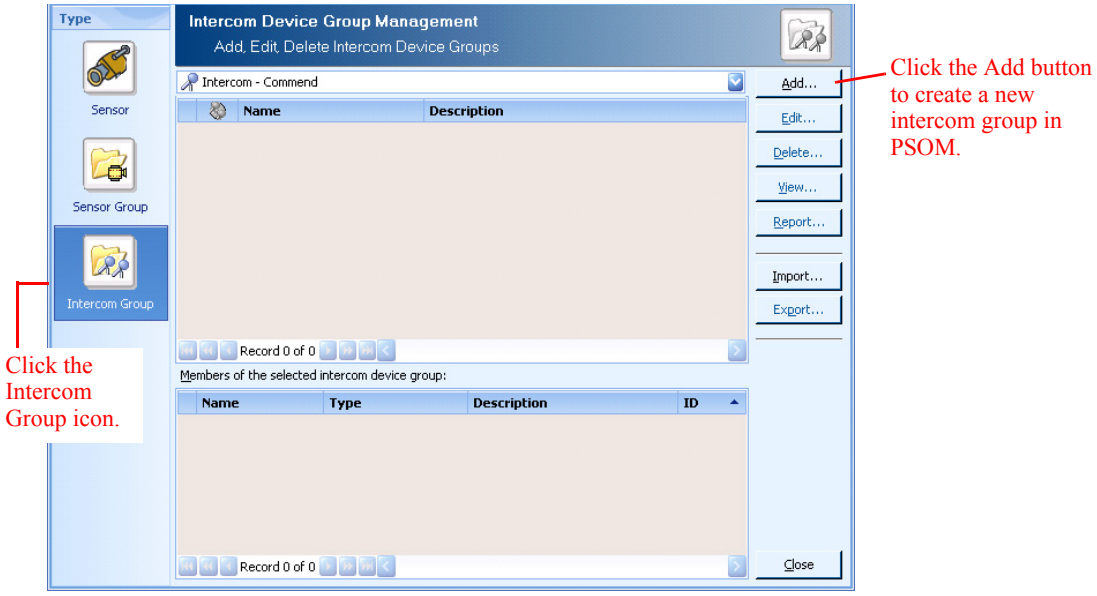
To add a new intercom device group:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

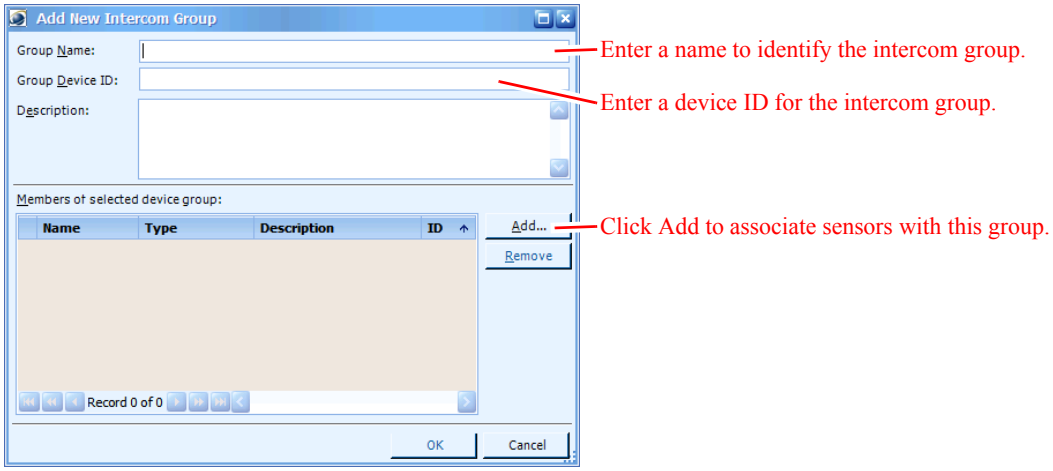
The Sensor Management window appears.



Step 3 Click the **Intercom Group** icon to display a list of all intercom groups currently defined for PSOM.

Step 4 Click the **Add** button to add a new intercom group.

The Add New Intercom Group window appears.



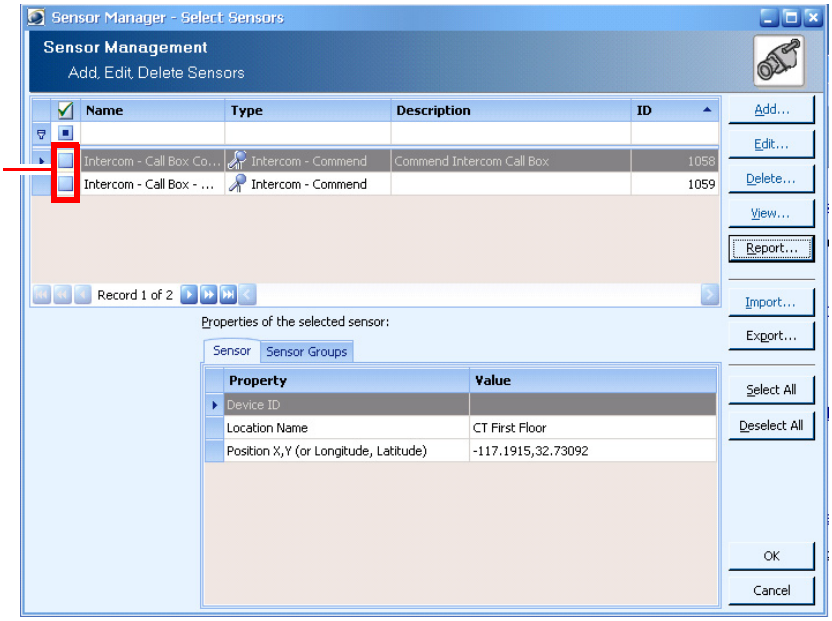
Step 5 In the **Group Name** field, enter the name you want to assign to this collection of intercom devices.

Step 6 In the **Group Device ID** field, enter the device ID to associate with this group.

Step 7 In the **Description** field, enter details about this intercom device group that will help operators determine the location, the intercom devices that are being monitored.

Step 8 Click the **Add** button to select intercom devices to associate with this group.

The Select Sensors window appears.



Step 9 Check boxes for each intercom device in the list that should be added to this group.

Step 10 Click **OK** to save your selections.

The selected intercom devices are added to the "Members" area of the Add New Intercom Group window.

Step 11 Click **OK** to save your intercom device group.

Editing an Intercom Device Group

You may want to edit an intercom device group to change its members, or to modify its description.

Note If you add or remove members in an intercom group, you need to first remove the intercom device group from its monitoring area. Once you've modified membership to the intercom device group, you can re-assign the intercom device group to the monitoring area. See the "Editing or Deleting Monitoring Areas" section on page 5-20 for instructions.

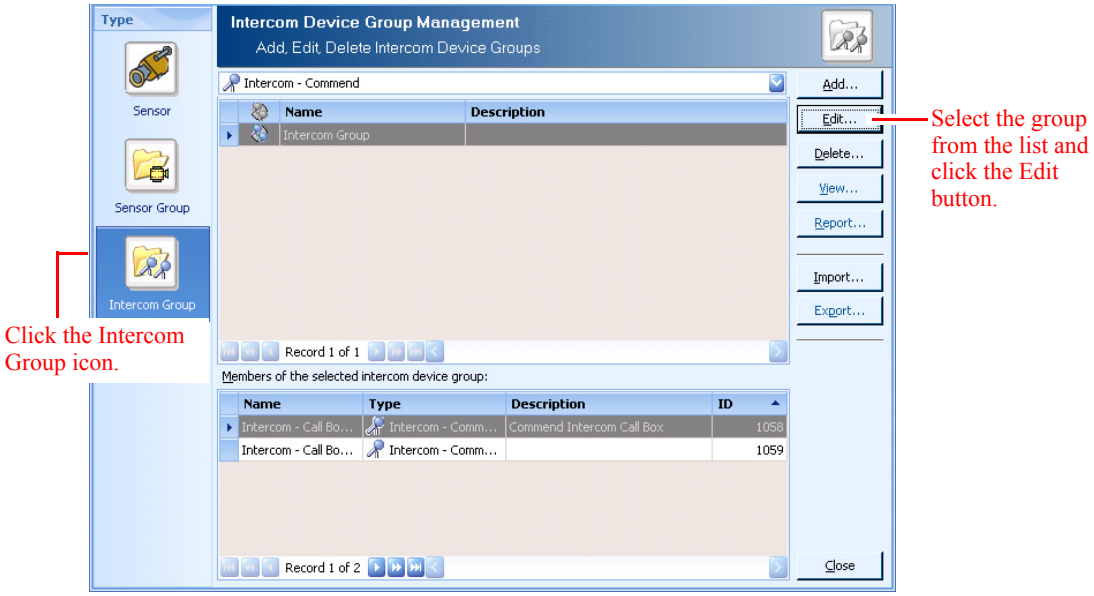
To edit an intercom device group:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

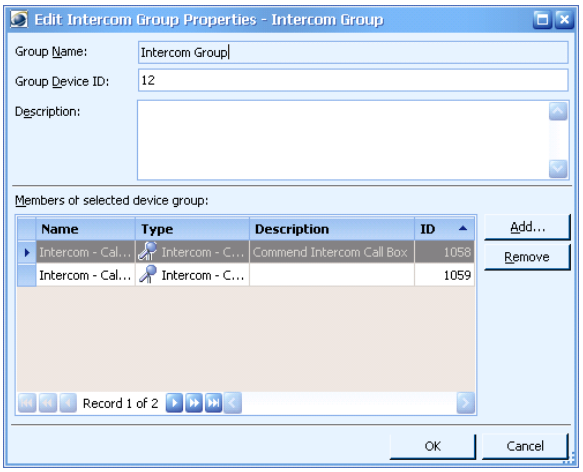
The Sensor Management window appears.



Step 3 Click the **Intercom Group** icon to display a list of all intercom device groups currently defined for PSOM.

Step 4 Select the group from the list and click the **Edit** button to change it.

The Edit Intercom Group Properties window appears.



Step 5 To change the group's device ID, enter a different ID in the **Group Device ID** field.

Step 6 To change the description, enter modifications in the **Description** field.

Step 7 To add new members to the intercom device group, click the **Add** button. When the Select Sensors window appears, check boxes for the intercom devices you want to add to the group, and click **OK**.

Step 8 To remove a member from the intercom device group, select the device from the list under "Members..." and click the **Remove** button.

Step 9 Click **OK** to save your changes.

Deleting an Intercom Device Group

To remove an intercom device group:

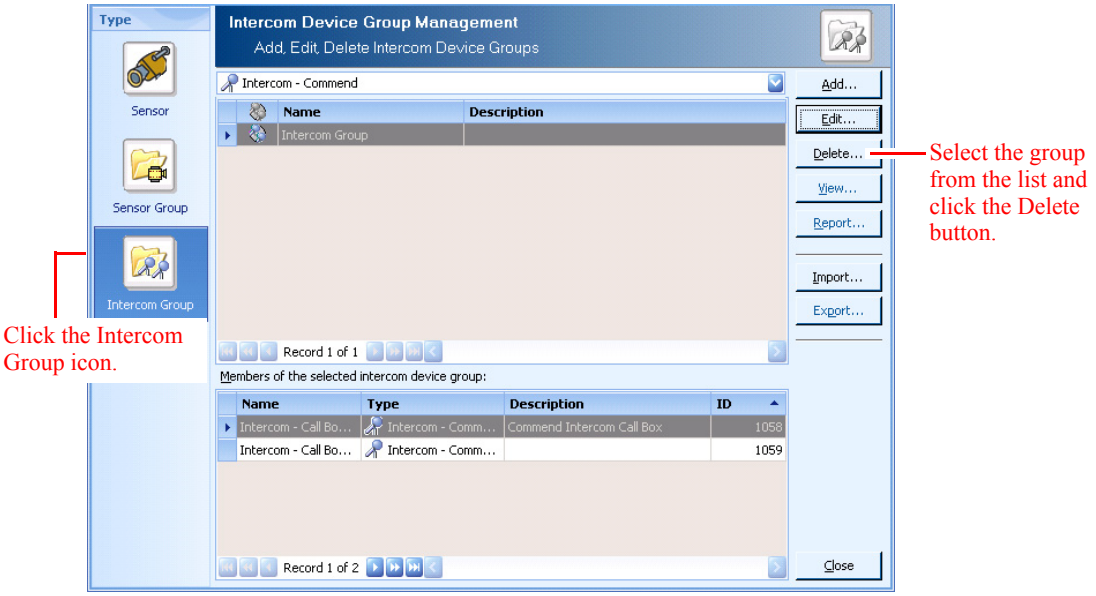
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

Step 3 Click the **Intercom Group** icon.

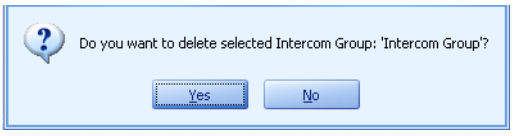
The Sensor Management window appears.



Step 4 Click the **Intercom Group** icon to display a list of all intercom groups currently defined for PSOM.

Step 5 Select the intercom device group you want to remove, and click the **Delete** button.

A confirmation dialog box appears.



Step 6 Click **Yes** to verify the deletion.

Importing and Exporting Sensors, Sensor Groups, and Intercom Groups with PSOM

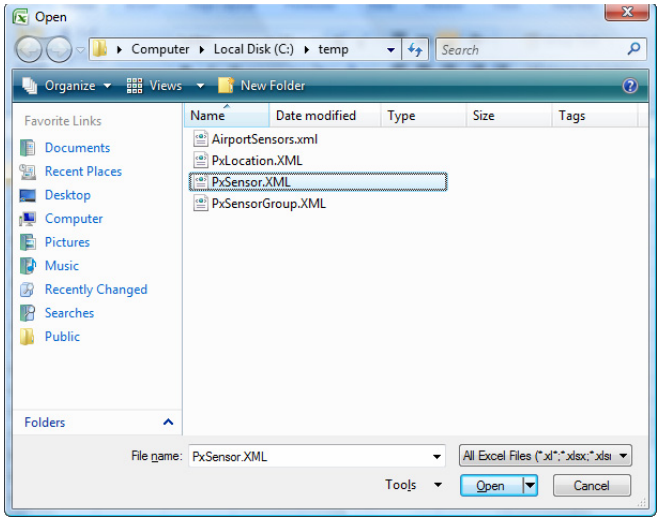
You can import sensors, sensor groups, intercom groups and locations to PSOM using Microsoft Excel; you can also export these definitions to Excel from PSOM.

Note These procedures have been verified using Excel 2007. If you are using Excel 2003 or later, you can save the XML file as XML Data for reimport to PSOM.

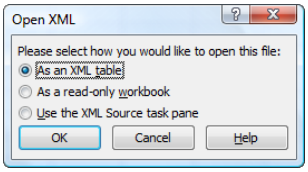
To import sensors to PSOM:

Step 1 Open the **PxSensor.XML** file in Excel 2007.

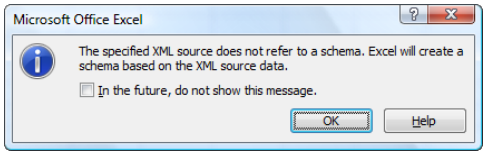
Note For sensor groups, open the **PxSensorGroup.XML** file, and for intercom groups, open the **PxIntercomGroup.XML** file.



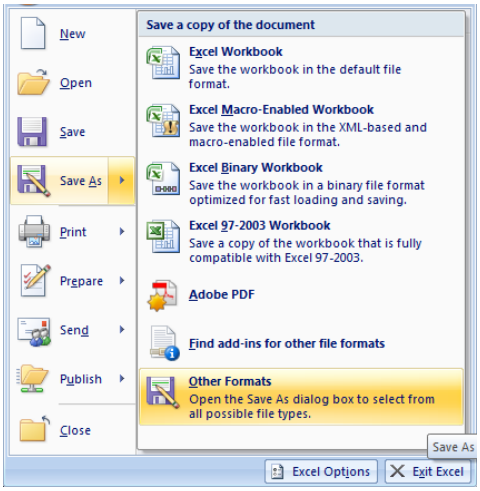
Step 2 When prompted, choose to open the XML file as an XML table; select **As an XML table** and click **OK**.



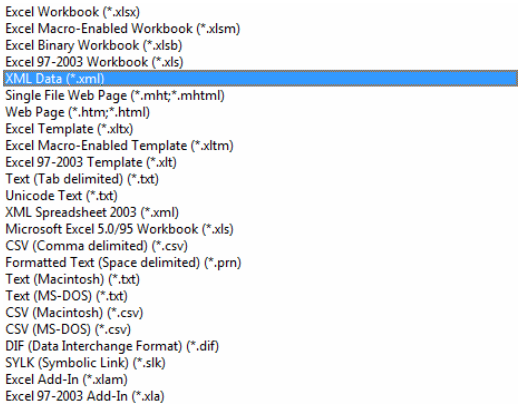
Step 3 When prompted, click **OK**.



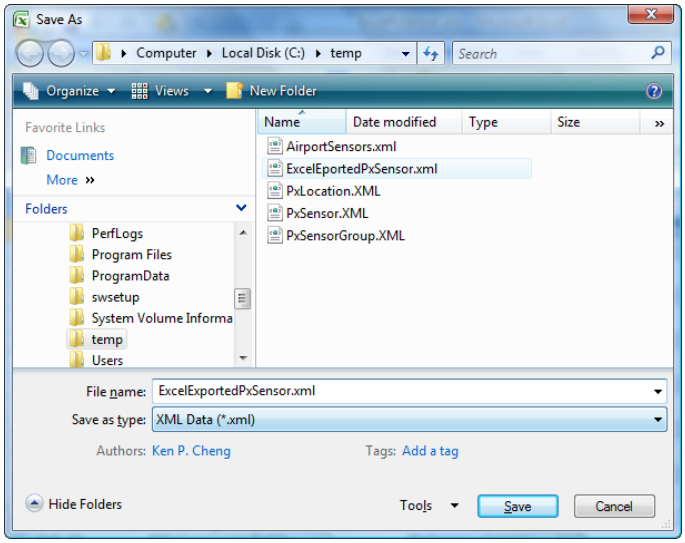
Step 4 In Excel, click **Save As > Other Formats**.



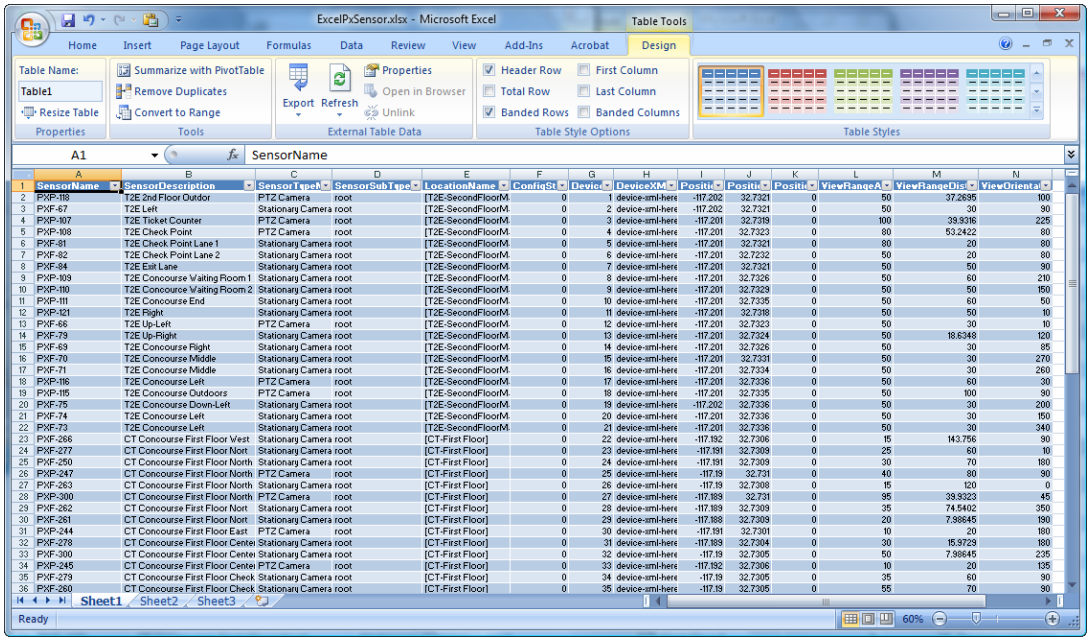
Step 5 From the list of formats that appears, select **XML Data (*.xml)**.



Step 6 In the window that appears, enter a name in the **File name** field and click **Save**.



Step 7 Modify the table to add your new sensors. You must provide values for each column for your new sensor.



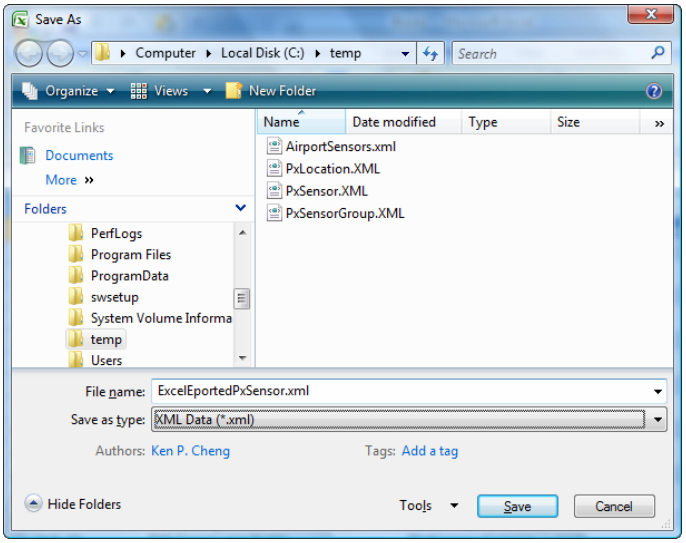
Be aware that characters cannot be used in XML strings. You can substitute the following syntax for special characters:

Character	Substitute
&	&
<	<
>	>

“	"
‘	'

For example, if you have a SensorDescription of “Area A & B”, you will use “Area A & B”.

Step 8 Save the XML table as an XML Data file; select **XML Data (*.xml)** from the **Save as Type** field.



Step 9 When prompted, click **Continue**.

Step 10 Save the XML file.

Now you can import the sensor definitions XML file into PSOM.

Step 11 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 12 Click **Sensors**.

The Sensor Management window appears.

Step 13 Click **Sensor** to view sensors.

Note Click **Sensor Group** to view sensor groups, or **Intercom Group** to view intercom groups.

Step 14 Click **Import** to import sensor definitions from an XML file, then select the XML file on your system that has the definitions.

Note You can also click **Export** to save an XML file with the sensor definitions stored in PSOM. It will save the file as **PxSensor.xml** for sensors, **PxSensorGroup.xml** for sensor groups, and **PxIntercomGroup.xml** for intercom device groups.

If the XML file size you are importing exceeds 2 MB (roughly 4000 sensors), the import process will either timeout or fail immediately without importing sensors. To avoid this problem, split the XML file into multiple files that are smaller than 2 MB each, and import the XML files one at a time.

Updating Sensors with a Web Service Call

You may wish to update sensor information in PSOM from your application using an XML file; conversely, you may wish to pull sensor information from PSOM into your application. PSOM provides these web service calls:

- ExportDBObject <LoginID>, <Object Type>, <File Name with full path>
- ImportDBObject <LoginID>, <Object Type>, <File Name with full path>

where *Object Type* can be a value from 1-3 representing the following:

- 1—Location
- 2—Sensor
- 3—SensorGroup

For example, the following syntax instructs PSOM to export all sensor information in XML to "C:\output\sensor.xml":

```
ExportDBObject myLogin, 2, "c:\output\sensor.xml"
```

When updating information in PSOM, the SensorName property is used to determine whether the sensor already exists and should be updated, or whether the sensor is new and should be created. For sensor groups, the `SensorGroupName` property is used. If a sensor exists in PSOM, but is not included in the XML you are uploading, then no change is made to that sensor in PSOM. In other words, XML for import operations only needs to contain changed and new sensors.

Structure of XML for Sensor Definitions

The structure of the XML for sensors is as follows.

```
<Sensor>
    <SensorName>Hirsch Expansion Input</SensorName>
    <SensorDescription>Expansion Input Access Control</SensorDescription>
    <SensorTypeName>Access Control</SensorTypeName>
    <LocationName>Office1</LocationName>
    <ConfigStatus>0</ConfigStatus>
    <DeviceID>&lt;![CDATA[AED Alarm CP5]]&gt;</DeviceID>
    <DeviceXML></DeviceXML>
    <PositionX>-1.216291</PositionX>
    <PositionY>3.6883777</PositionY>
```

```
    <PositionZ>0.0000000</PositionZ>
    <ViewRangeAngle>0</ViewRangeAngle>
    <ViewRangeDistance>0</ViewRangeDistance>
    <ViewOrientation>0 </ViewOrientation>
    <UIState>0</UIState>
</Sensor>
```

Structure of XML for Sensor Group Definitions

The structure of the XML for a sensor group is as follows.

```
<SensorGroup>
    <Name>CCure Grp2</Name>
    <Description></Description>
    <TypeName>Access Control-Camera</TypeName>
    <SubTypeName>SoftwareHouse-CCure</SubTypeName>
    <Member>
        <MemberName>NonDoor</MemberName>
        <MemberTypeName>Access Control</MemberTypeName>
        <MemberSubTypeName>SoftwareHouse-CCure</MemberSubTypeName>
        <LocationName>[CCure Area 1]</LocationName>
        <DeviceID>&lt;![CDATA[2087]]&gt;</DeviceID>
        <DeviceXML></DeviceXML>
    </Member>
</SensorGroup>
```

You can use the <PxSensorGroupImport> command to create a new sensor group, as well as create new sensors within it. In this case, the DeviceID must contain a value for the new member.

Return Values

Successful operations receive the following return value.

```
<WSSERVICE NAME="Export or Import DBObjects">
    <STATUS>0</STATUS>
    <RESULT COUNT="0">
        <REASON>Output written to file successfully</REASON>
    </RESULT>
</WSSERVICE>
```

If an output file and path is not specified by your call, the returned XML includes the structure of the sensor, sensor group, or location data that is being imported or exported. The following example shows an update to location data.

```
<WSSERVICE NAME="Export or Import DB Objects">
    <STATUS>0</STATUS>
    <RESULT COUNT="0">
     <ExportDBObject>
        <Location>
            <LocationName>dummyloc</LocationName>
            <LocationDescription>dummyloc</LocationDescription>
        </Location>
        <Location>
            <LocationName>Office10</LocationName>
            <LocationDescription>Office10</LocationDescription>
        </Location>
    </ExportDBObject>
    </RESULT>
</WSSERVICE>
```

CHAPTER 7

Designing Maps

To enable the view provided in the Map View Pane of the Operation Console, you must design the maps shown for each monitoring zone and area within PSOM.

This chapter covers how to use the Map Design Mode to:

- Provide background images for maps that offer an aerial view or building floor plan.
- Configure the origin and scale for a map. Optionally, configure GPS coordinates for maps.
- Add sensors to a map for each video camera and access control device in the environment.

This chapter includes these topics:

- Entering Map Design Mode, page 7-1
- Adding Background Map Images, page 7-5
- Configuring Origin and Scale for a Map, page 7-6
- Setting Display Options for a Map, page 7-14
- Drawing a Monitoring Zone or Area on a Map, page 7-16
- Adding Sensors to a Map, page 7-21
- Adding Navigation to Maps, page 7-24
- Adding URL Links to Maps, page 7-27
- Editing and Deleting Items from the Map, page 7-29
- Setting the Sort Order of the Monitoring Hierarchy, page 7-30
- Integrating GIS Maps with PSOM, page 7-31

Entering Map Design Mode

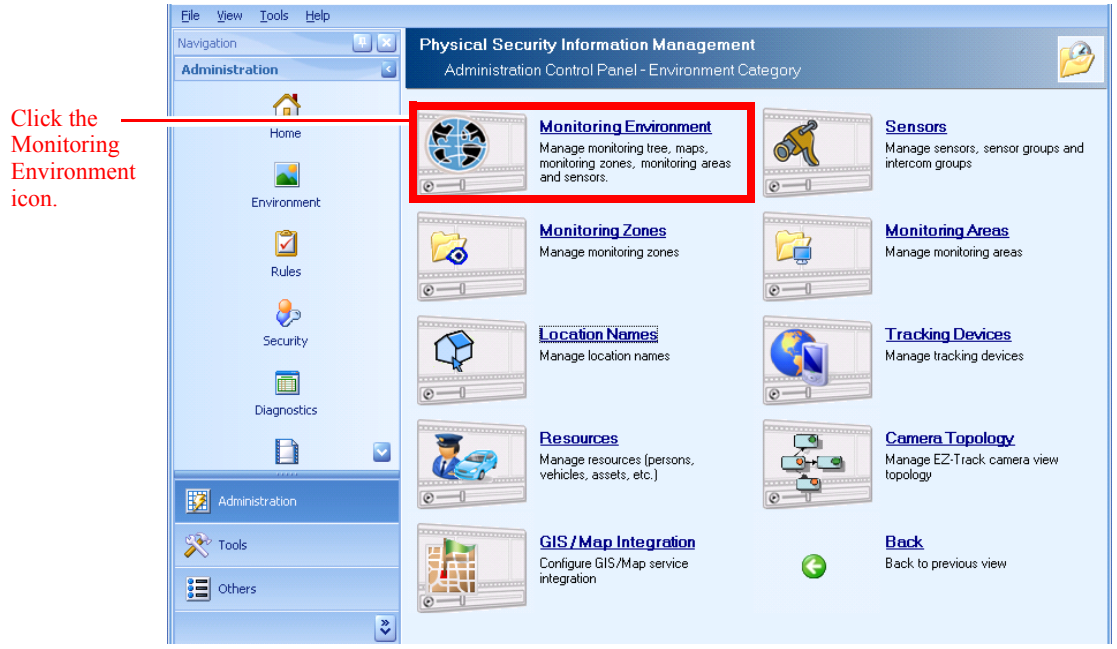
You need to design maps for each monitoring zone and area within PSOM, including the top-level "global zone" node. The process for configuring maps and their properties is the same for all levels of nodes in the Monitoring Tree—from the Map Design Mode, you perform all actions in this chapter for each node.

To enable Map Design Mode for all nodes in the Monitoring Tree at once, follow the instructions below to enter Map Design Mode for the global zone node.

To enter Map Design Mode for a node:

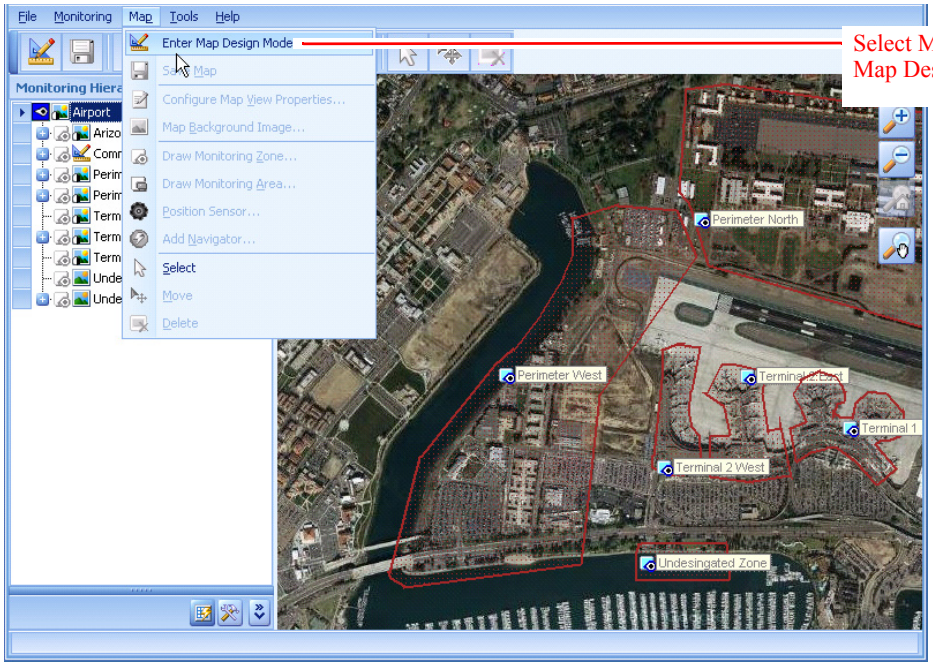
Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.



Step 2 Click the **Monitoring Environment** icon.

The PSOM Environment Management window appears.



Step 3 Select the global zone node, the top-most node, in the Monitoring Tree; in this case, the "Airport" node.

Step 4 From the menu bar, select **Map > Enter Map Design Mode**.

In the map design mode, the Design Mode icon is selected and enables you to modify maps for each monitoring node in the Monitoring Tree.

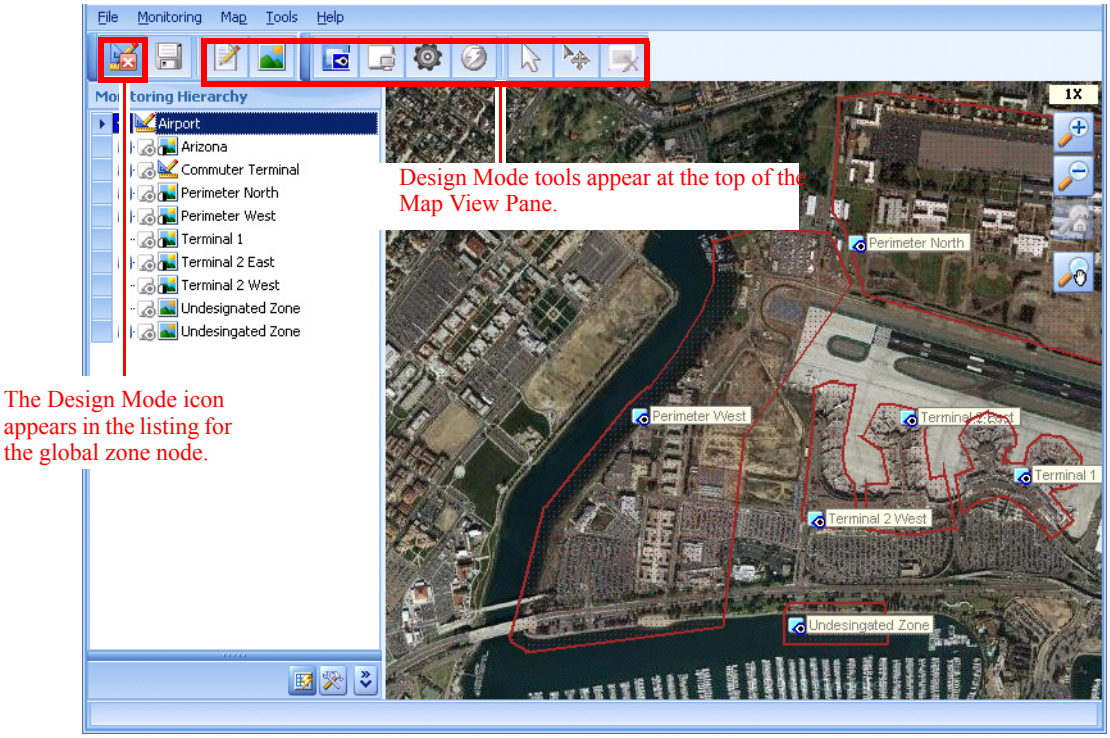
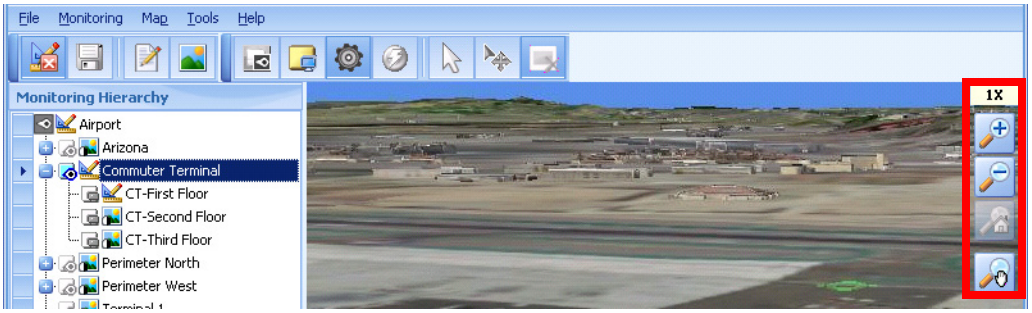


Table 7-1 explains what the Design Mode icons are used for. There are additional tools that appear in the Design Mode toolbar when a camera sensor is selected on the map; see Table 7-3 on page 7-24.

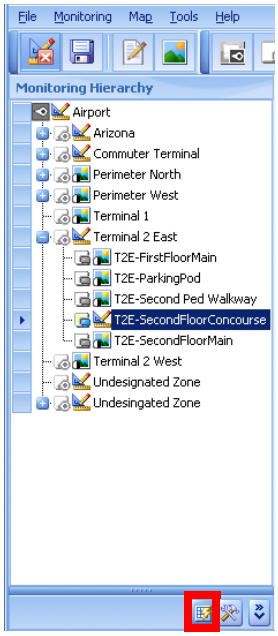
Table 7-1 Design Mode Tools

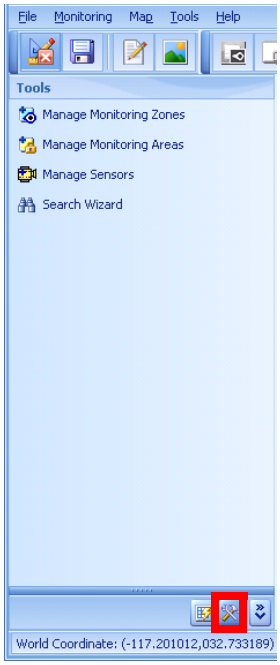
This icon...	Does this to the map area...
	Enables Map Design Mode.
	Saves the changes to the map design.
	Configures the view properties for a map design such as whether sensor icons are displayed.
	Allows you to select a background map image for the current node.
	Allows you to draw a monitoring zone on a map design.
	Allows you to draw a monitoring area on a map design.
	Places a sensor icon on the visible map: video camera, access door, hazard detection device, and so on.
	Places a link on the map so you can allow users to jump to a map for a different node from the Map View Pane.
	Allows you to select an object in the map design.
	Moves the selected object in the map area.
	Deletes the selected object from the map design.

You can use the icons at the far right of the map to zoom in, zoom out, and pan.



And you can display the Monitoring Hierarchy or Tools in the left navigation bar using the icons at the bottom of the navigation bar.





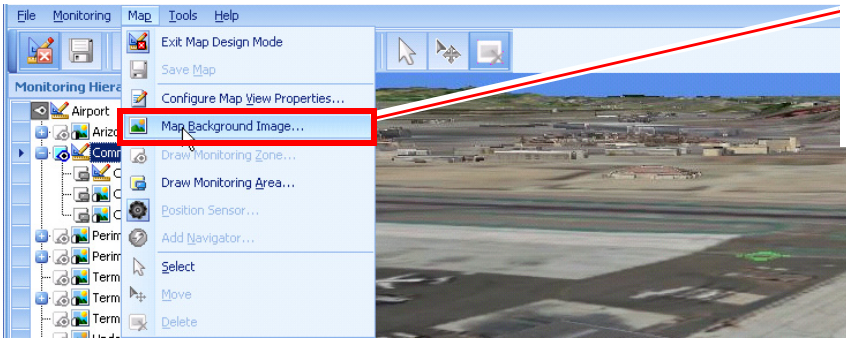
Adding Background Map Images

To add a background image to a monitoring node:

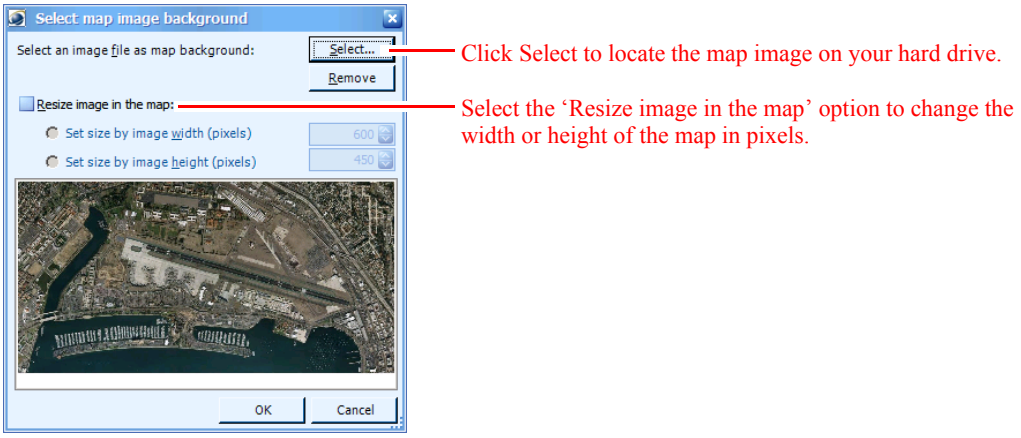
Step 1 Select the node's listing in the Monitoring Tree.

Step 2 Select **Map > Background Image...** from the menu bar at the top of the window.

Note Alternatively, you can click the **Background Image** icon from the Design toolbar.



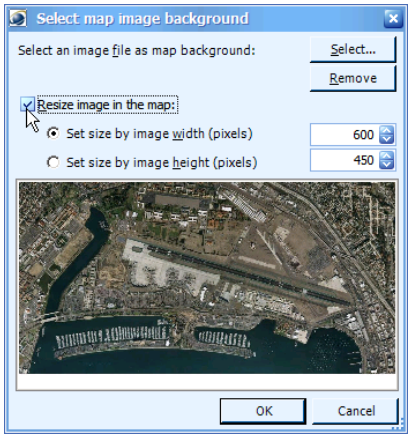
The **Select map image background** dialog box appears.



Step 3 Click **Select** to locate the background image file on your computer's hard drive.

Note If you want to remove the background image that is currently selected for map, click the **Remove** button.

Step 4 If you want to change the size of the image, click the **Resize image in the map** option. You can now set the width or height of the map in pixels using the fields below; the aspect ratio of the map is retained.



Step 5 Click **OK**.

The background image is now displayed in the **Map View Pane**.

Step 6 If you are done modifying the map, exit from the Design Mode to save your changes.

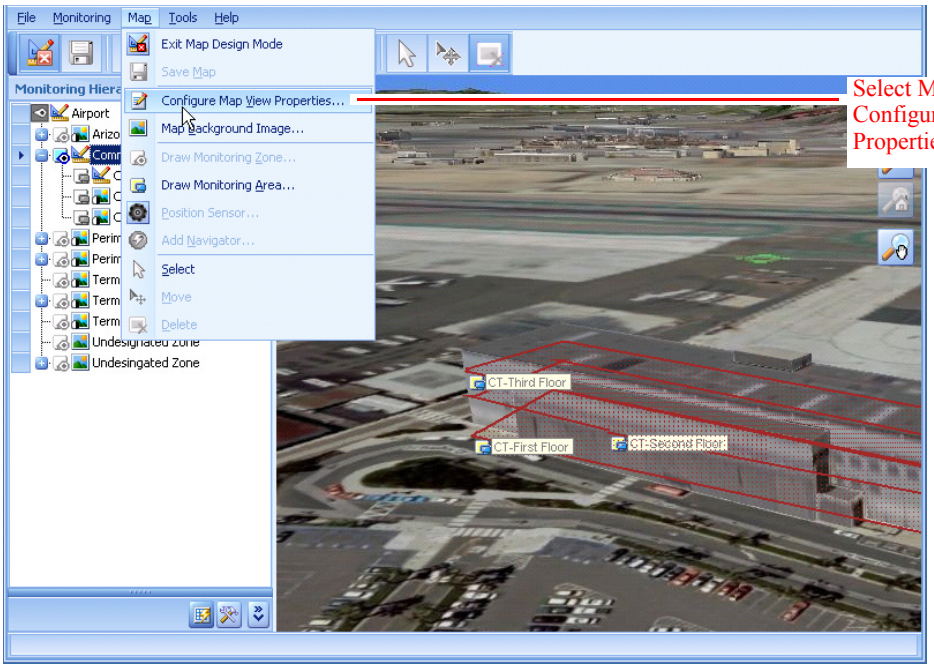
Configuring Origin and Scale for a Map

For each map, you can configure the origin coordinates, provide a reference point for map scale, and set the orientation of the x-axis on the map. You can either use map coordinates generated by PSOM, or you can use actual GPS coordinates.

To configure origin and scale for a map:

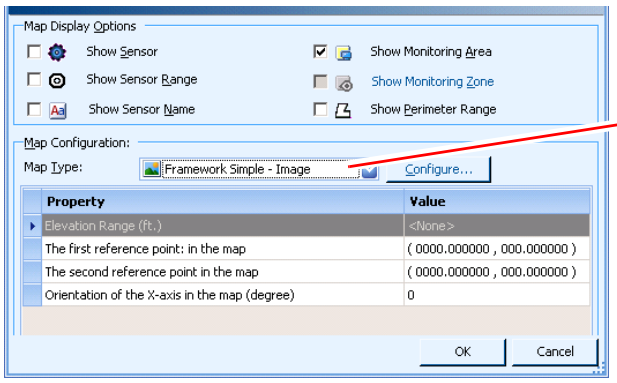
Step 1 Select the node's listing in the Monitoring Tree. This should be a node that has a background map image assigned to it.

Step 2 Select **Map > Configure Map View Properties** from the menu bar.



Alternatively, you can right-click the node and select **Properties** from the right-click menu. Then select the **View** tab in the **Properties** window.

The Map View Properties Configuration window appears.



Step 3 If you want to configure coordinates for a two-dimensional image map, select **Framework Simple – Image** from the **Map Type** field and click the **OK** button. You are done with configuration.

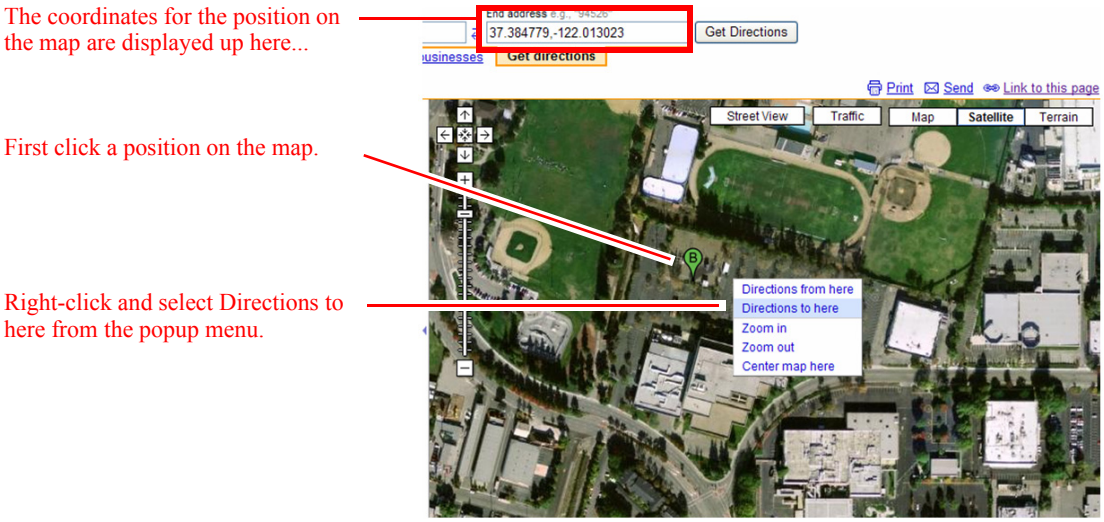
Note To use GPS-based coordinates, see the "Configuring Coordinates using GPS" section on page 7-8.

Step 4 If you are done modifying the map, exit from the Design Mode to save your changes. Select **Map > Exit Map Design Mode**.

Configuring Coordinates using GPS

Before you configure coordinates using GPS, you need to obtain the coordinates for the reference points in your map. You can obtain latitude/longitude using a web-based map (such as Google Map or Microsoft Virtual Earth).

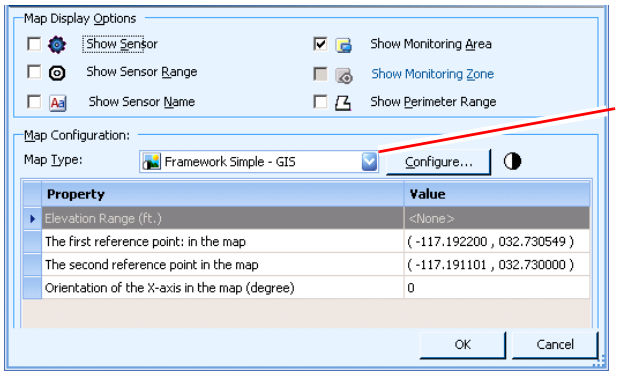
In Google Map, bring up a map of the area in question, then right-click and select **Direction to here** from the popup menu. This creates a marker on the map, and also displays coordinates at the top of the window in the address field.



Another resource is ITouchMap, which is based on Google Map: http://itouchmap.com/latlong.html.

To configure origin and scale using GPS coordinates:

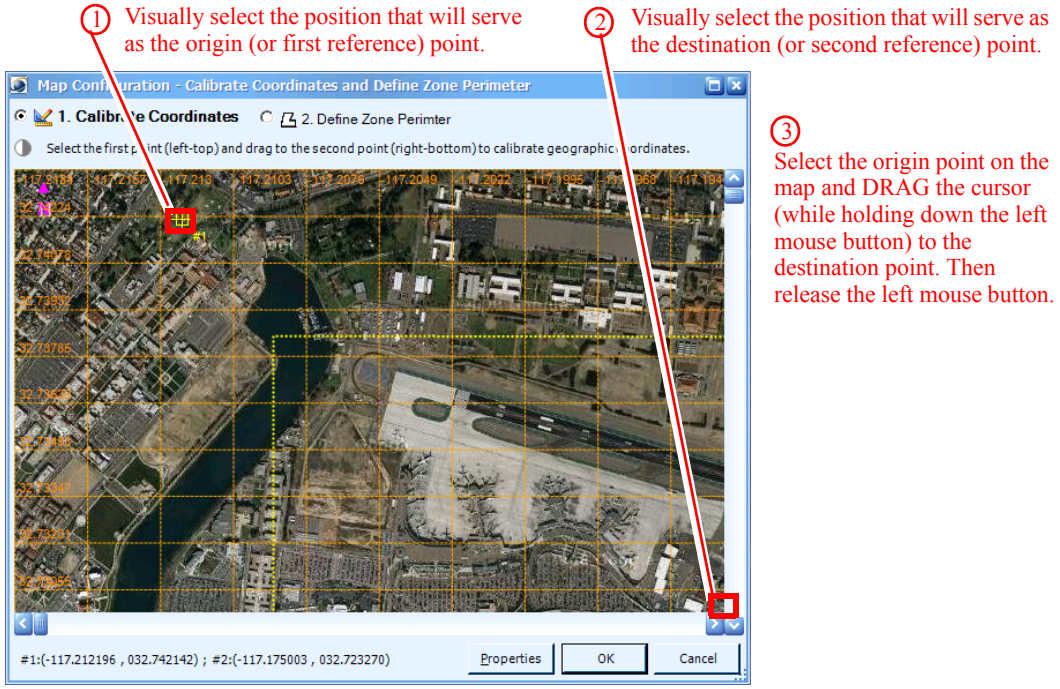
Step 1 From the Map View Properties Configuration window, select **Framework Simple – GIS** from the **Map Type** field.



Note If you have enabled different GIS/map software, it will appear in the **Map Type** field as a choice. See the "Integrating GIS Maps with PSOM" section on page 7-31.

Step 2 Click the **Configure** button.

The Map Configuration window appears.

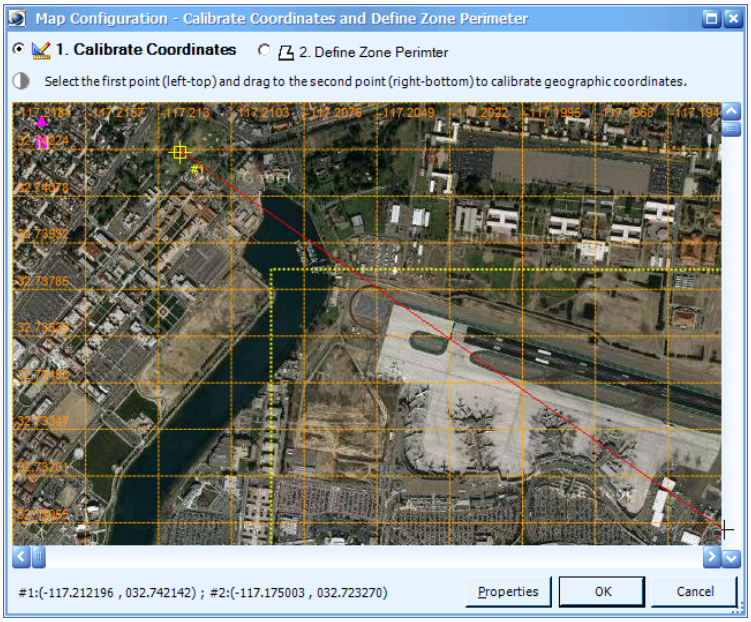


Step 3 First, expand the window size so that the entire map is shown within the window (e.g., there are not any scroll bars).

Step 4 Visually select an *initial* position on the background map that will serve as the *origin* or first reference point. The origin should be the top-left of the area.

Step 5 Visually select a *second* point on the map to be the *destination* or second reference point. The destination should be the bottom-right of the area.

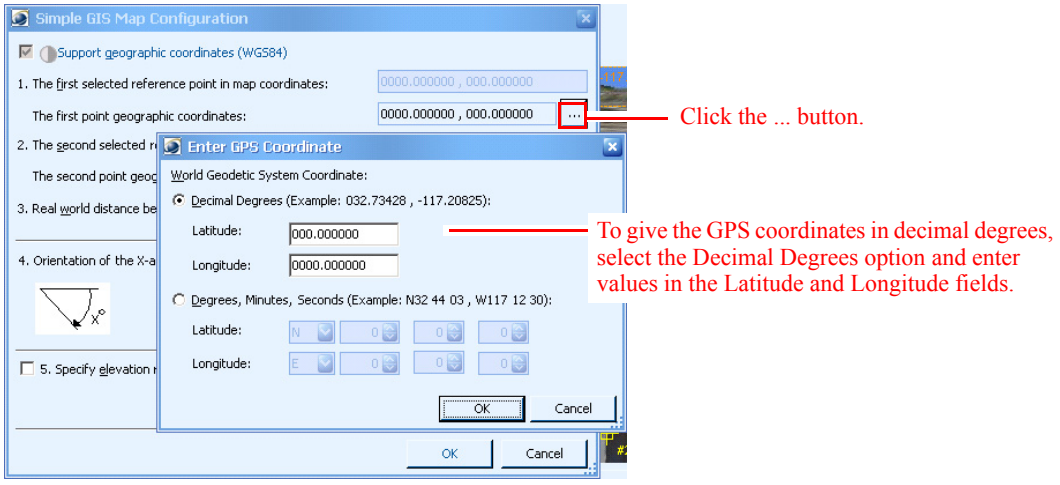
Step 6 Select your origin position on the map (point #1) and drag the mouse (while holding down the left mouse button) towards your destination point (point #2). Release the left mouse button at the destination point (point #2).



The Simple GIS Map Configuration window appears.

Step 7 Click the ... button to the right of the **The first point geographic coordinates** field.

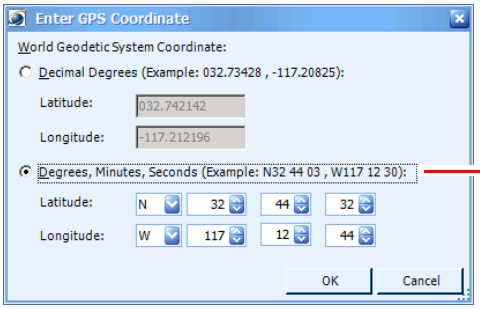
The Enter GPS Coordinate window appears.



Step 8 You can either select the GPS coordinate using decimal degrees for the latitude and longitude, or direction plus degrees, minutes and seconds.

The screen above shows the GPS coordinate given in decimal degrees.

Shown next is the GPS coordinate given in direction, degrees, minutes and seconds.



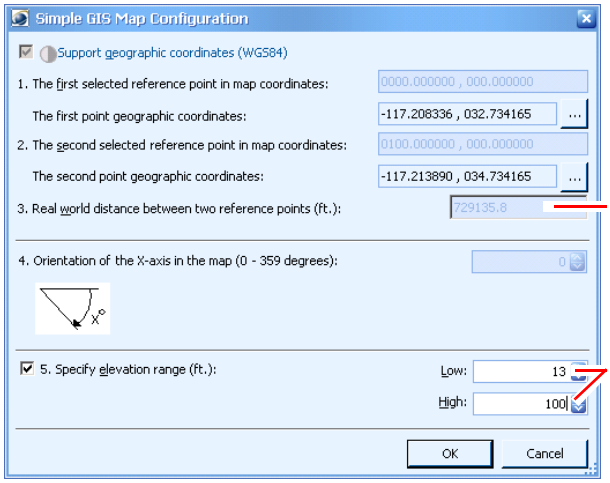
To give the GPS coordinates in direction plus degrees and time, select the Degrees, Minutes, Seconds option and select values from the Latitude and Longitude fields.

Step 9 Click **OK**.

Step 10 In the Simple GIS Map Configuration window, click the … button to the far right of the **The second point GPS coordinates** field.

Step 11 In the Enter GPS Coordinate window, enter the coordinates for the second position on the map and click **OK**.

The Simple GIS Map Configuration window appears similar to the following. Note that the real world distance between the two reference points is automatically calculated based on the GPS coordinates you selected.



The real-world distance between the two reference points is automatically calculated.

If your map shows a location that is higher or lower than ground level, you can enter the elevation range (in feet) using these fields.

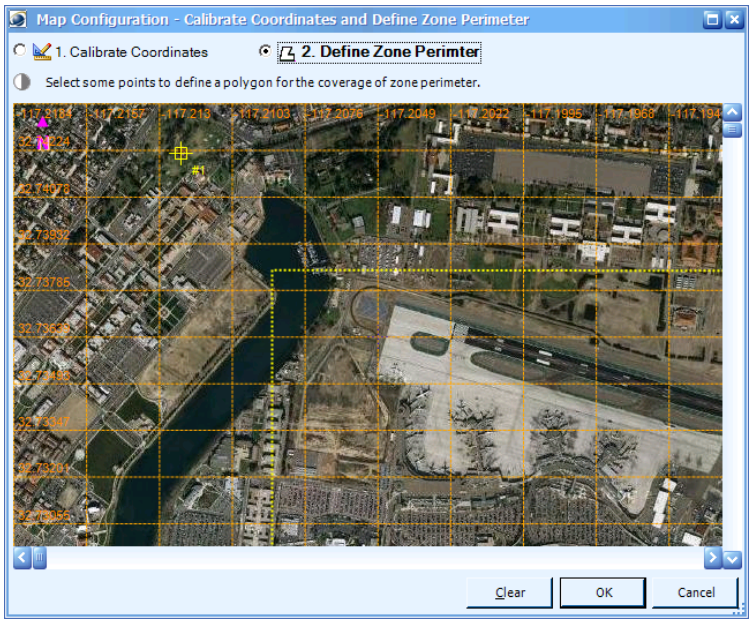
Note For GPS coordinates to work correctly, the GPS map must have North facing directly upwards; in other words, the map cannot be tilted or angled. Therefore, the **Orientation on the X-axis in the map** option is disabled.

Step 12 If your map shows a space that is elevated—for example, a second floor in a building—you can enter the elevation information in the **Specify elevation range** area. Enter the bottom of the elevation range in the **Low** field (e.g., the floor), and the top of the elevation range in the **High** field (e.g., the ceiling).

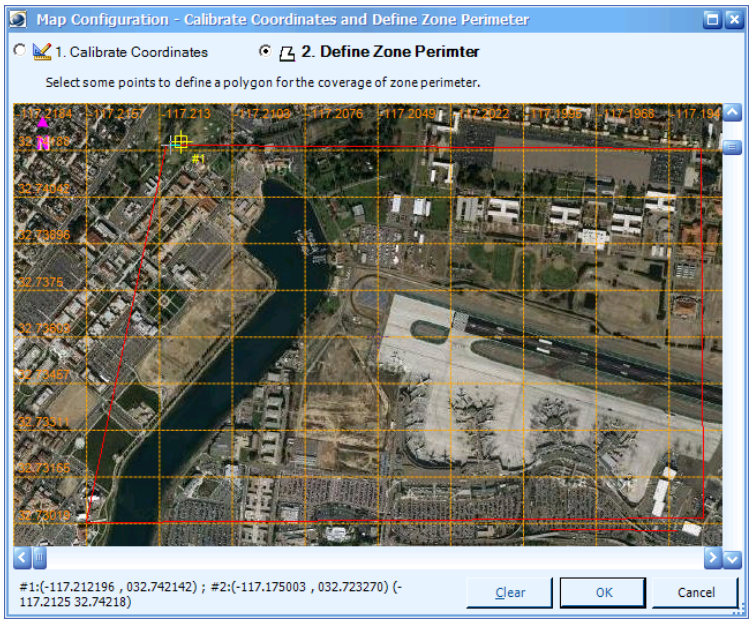
Note The elevation information is displayed on maps when locating resources, as shown next.

Step 13 Click **OK** when finished.

The Map Configuration window reappears. Configured coordinates appear in an orange grid pattern, and the **Define Zone Perimeter** option is selected.



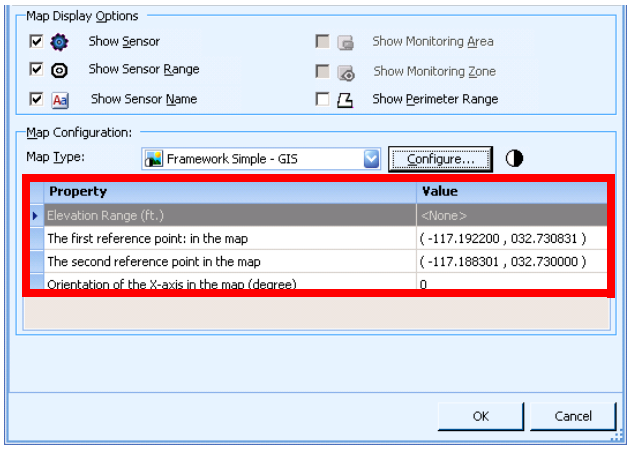
Step 14 Define the perimeter of the monitoring zone by first clicking anywhere in the map to place the first point of the polygon. Then keep clicking to create lines to create a closed polygon shape that defines the area covered by the monitoring zone.



Step 15 When finished, right-click on the map.

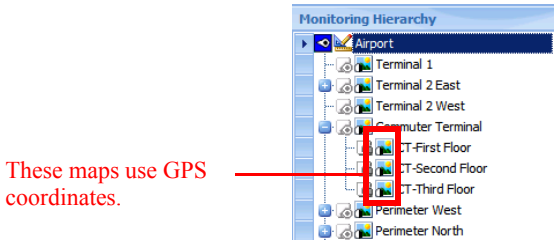
Step 16 Click **OK**.

The **Map View Properties Configuration** window displays your settings.



Step 17 Click **OK** to save your settings.

When viewing the Navigation Pane in the Operation Console, the maps that use geographic coordinates are displayed with a black/white circle on the map icon.



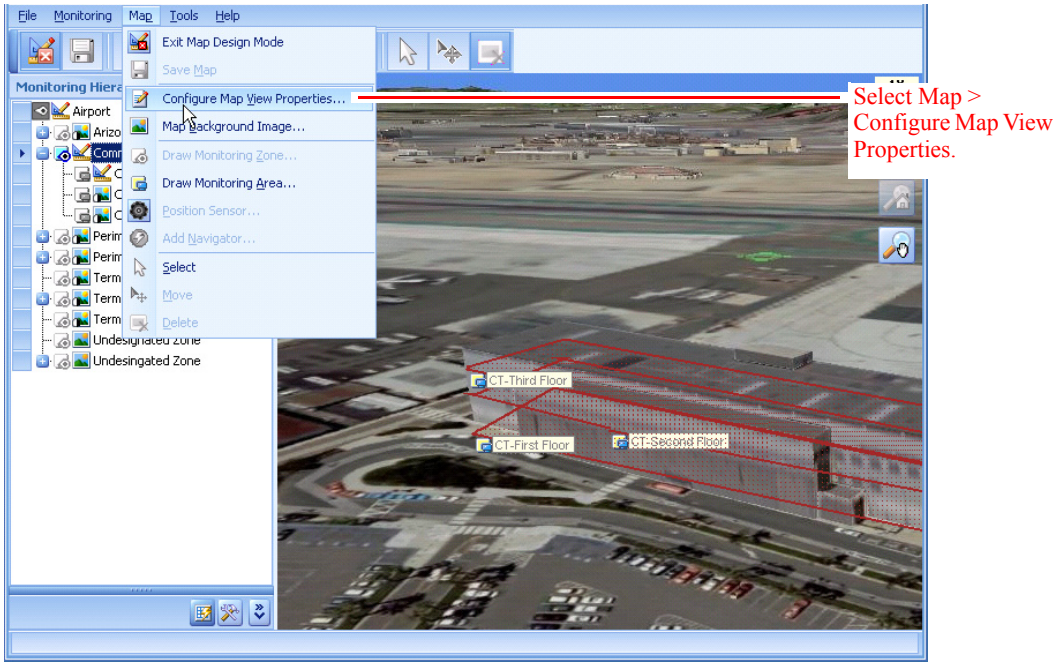
Setting Display Options for a Map

For each map, you can decide whether to show sensor icons, the range of these icons, the sensor names, and monitoring areas or zones that are defined for the map.

To set display options for a map:

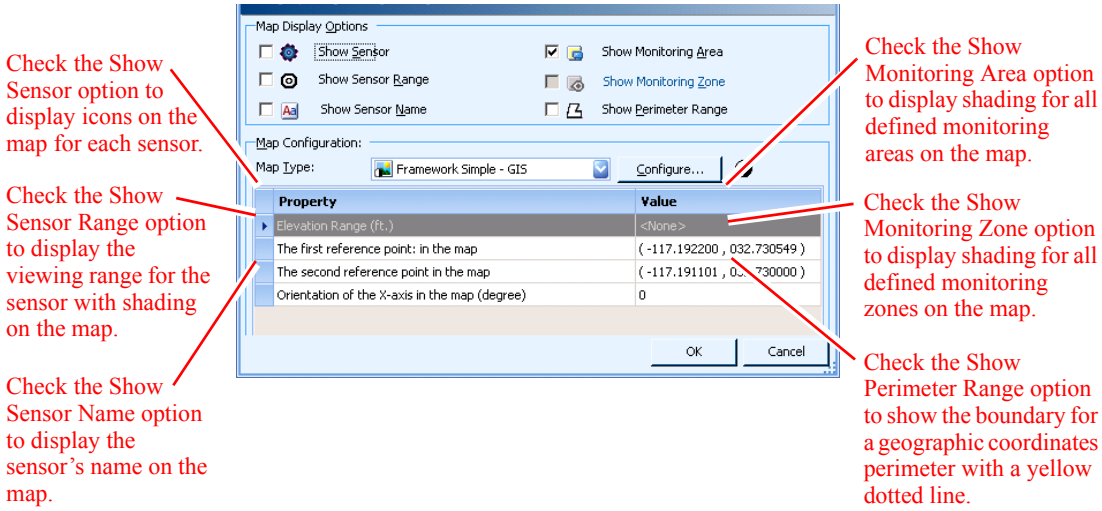
Step 1 Select the node's listing in the Monitoring Tree. This should be a node that has a background map image assigned to it, and that is in Map Design Mode.

Step 2 Select **Map > Configure Map View Properties** from the menu bar.



Alternatively, you can right-click the node and select **Properties** from the right-click menu. Then select the **View** tab in the **Properties** window.

The Map View Properties Configuration window appears.



Step 3 To display icons on the map for each sensor in the environment, check the **Show Sensor** option.

Step 4 To display the viewing range for a camera sensor (a shaded area that represents the area it can capture with video), check the **Show Sensor Range** option.

Step 5 To display the name of each sensor next to its location on the map, check the **Show Sensor Name** option.

Step 6 To display a shaded area on the map that represents the boundary of a monitoring area, check the **Show Monitoring Area** option. If this option is not valid for this map, it will be greyed out. See the "Drawing a Monitoring Zone or Area on a Map" section on page 7-16 for instructions on how to define a monitoring area on the map.

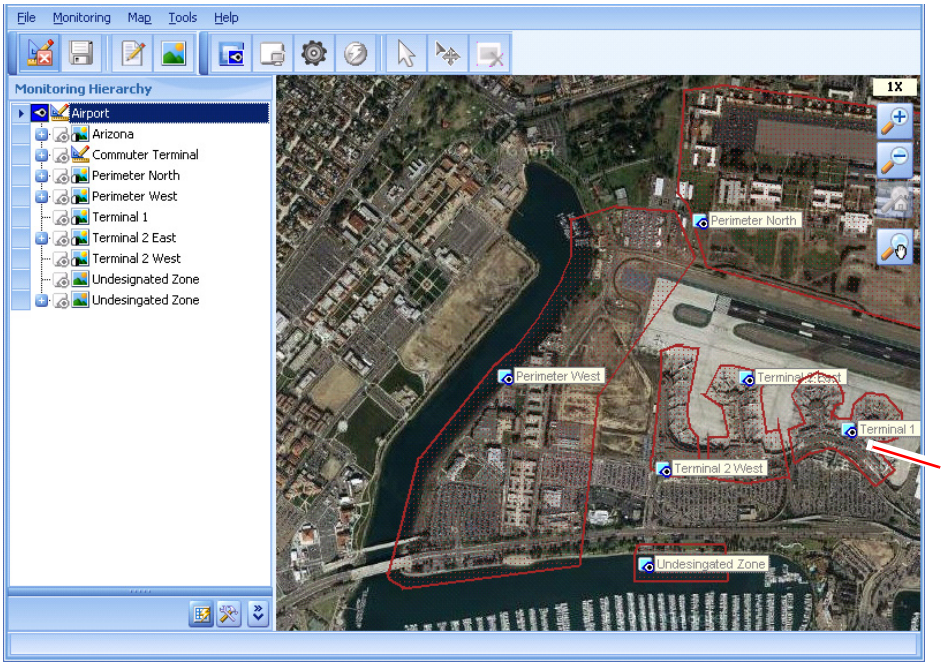
Step 7 To display a shaded area on the map to represent the boundary of a monitoring zone, check the **Show Monitoring Zone** option. If this option is not valid for this map, it will be greyed out. See the "Drawing a Monitoring Zone or Area on a Map" section on page 7-16 for instructions on how to define a monitoring zone on the map.

Step 8 To display the perimeter polygon that was configured on the Geographic Coordinates Map, check the **Show Perimeter Range** option. If this option is selected, the perimeter boundary is displayed using a yellow dotted line.

Step 9 Click **OK** to save your settings.

Drawing a Monitoring Zone or Area on a Map

You can draw a shaded area on a map to represent a monitoring zone or monitoring area. For example, the map for the global zone will have shaded areas representing different monitoring zones within the overall security zone.



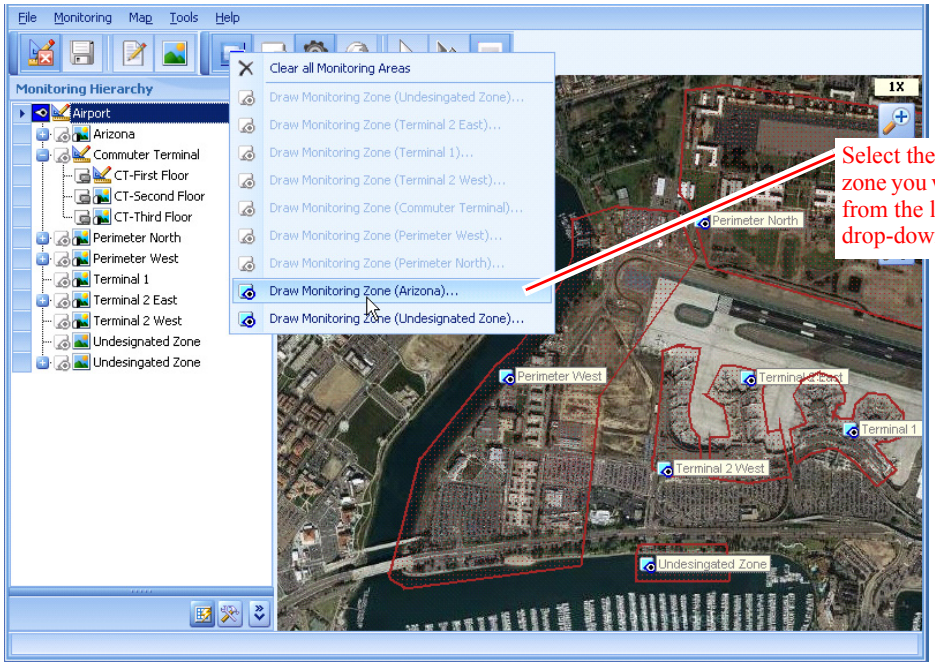
To draw a monitoring zone on a map:

Step 1 Navigate to the correct map by selecting the node's listing in the Monitoring Tree.

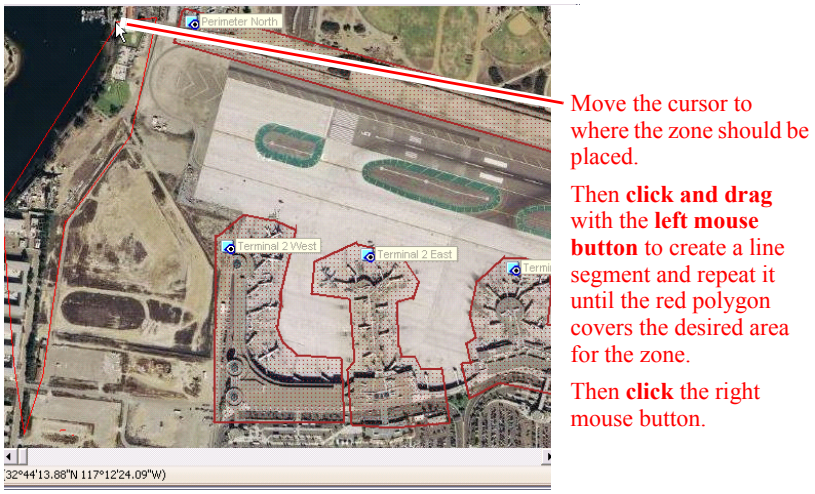
Step 2 Enter drawing mode using one of these methods:

- Select **Map > Draw Monitoring Zone** from the menu bar.
- Click the **Draw Monitoring Zone** icon in the Design toolbar. A list of all monitoring zones appears in a drop-down menu. Select the monitoring zone you will be drawing from the list.

Note You can only select a monitoring zone that has not yet been drawn (these appear in black text). If a monitoring zone has already been drawn, its name is greyed out in the drop-down menu.



Step 3 Move the cursor to where the zone should be placed, then click and drag with the left mouse button to create a line segment and repeat it until the red polygon covers the desired area for the monitoring zone. Then click the right mouse button.



The new monitoring zone is created on the map.

Step 4 To save changes, exit Design Mode. Select **Map > Exit Map Design Mode**.

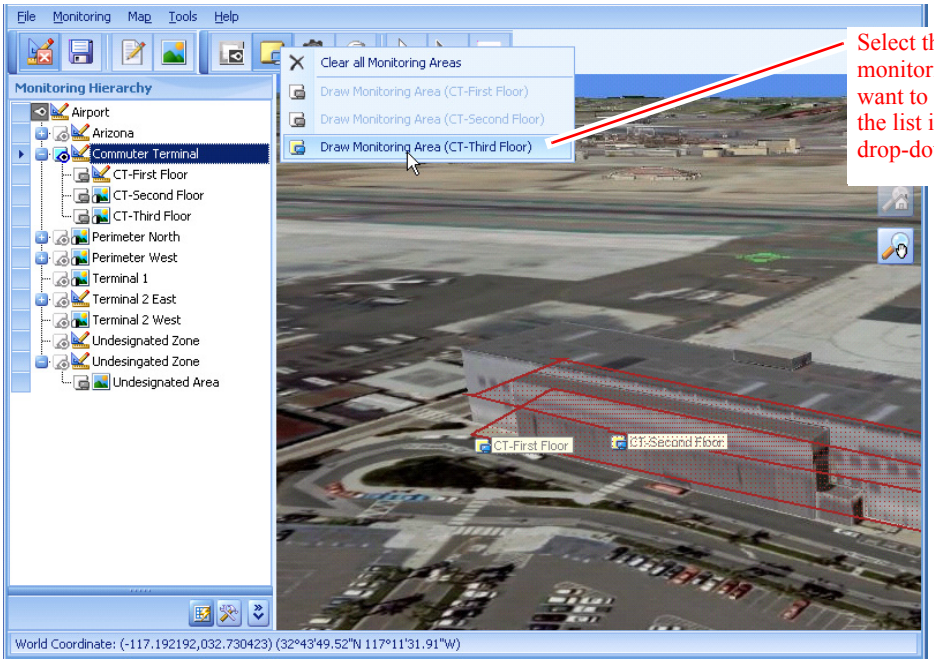
To draw a monitoring area on a map:

Step 1 Navigate to the correct map by selecting the node's listing in the Monitoring Tree. Make sure the node is in Map Design Mode.

Step 2 Select **Map > Draw Monitoring Area** from the menu bar.

Step 3 Select the **Draw Monitoring Area** icon from the Design toolbar. A list of all monitoring areas appears in a drop-down menu. Select the monitoring area you will be drawing from the list.

Note You can only select a monitoring area that has not yet been drawn (these appear in black text). If a monitoring area has already been drawn, its name is greyed out in the drop-down menu.



Step 4 Move the cursor to where the monitoring area should be placed, then click and drag with the left mouse button to create a line segment and repeat it until the red polygon covers the desired area. Then click the right mouse button.

The new monitoring area is created on the map.

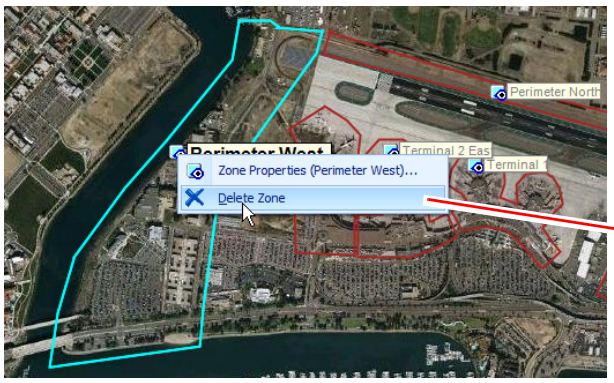
The new monitoring area is created on the map.

Step 5 To save changes, exit Design Mode. Select **Map > Exit Map Design Mode**.

To delete a monitoring zone from the map design:

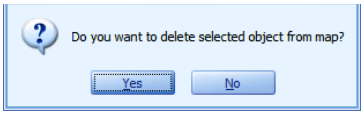
Step 1 Left click the icon and select monitoring zone on the map (it will become bold).

Step 2 Right click the icon and select **Delete Zone** from the right-click menu.



Right-click the monitoring zone's icon on the map and select Delete Zone from the right-click menu.

A confirmation dialog box appears.



Step 3 Click **Yes** to confirm the deletion.

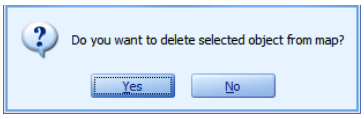
To delete a monitoring area from the map design:

Step 1 Select the icon for the monitoring area on the map (it will become bold).

Step 2 Right click the icon and select **Delete Area** from the right-click menu.

Right-click the monitoring area's icon on the map and select Delete Area from the right-click menu.

A confirmation dialog box appears.



Step 3 Click **Yes** to confirm the deletion.

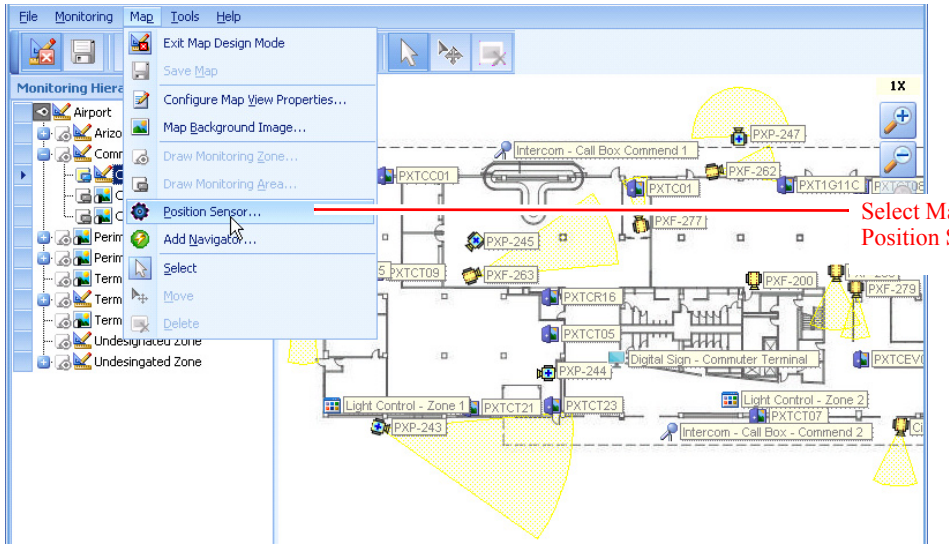
Adding Sensors to a Map

The next step is to place sensor icons on the map to show where actual video cameras and access control devices are located in the actual physical environment.

To position a sensor on the map:

Step 1 Select the node's listing in the Monitoring Tree.

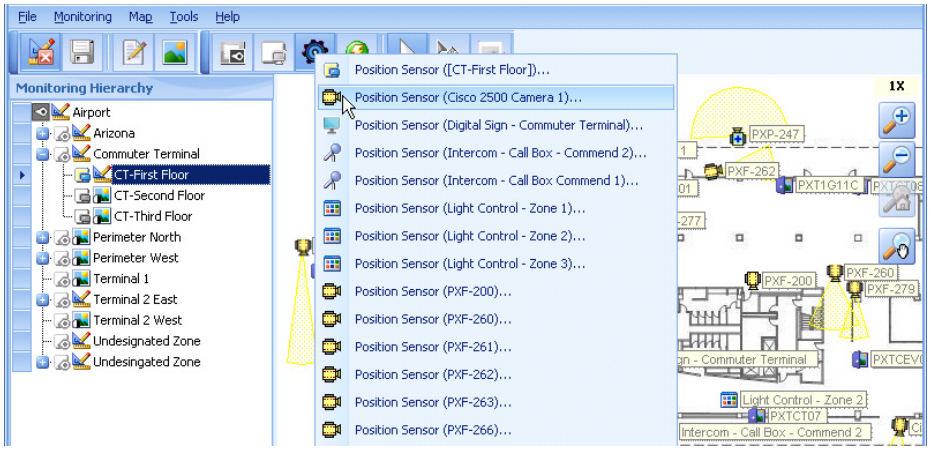
Step 2 Select **Map > Position Sensor** from the menu bar at the top of the window.



Select Map > Position Sensor.

Alternatively, select the **Position Sensor** icon in the Design Toolbar.

A list of sensors associated with the node appears in a menu. Only those sensors that are associated with the node appear in the menu.



Note If you select a sensor that is already on the map, you simply re-position it.

The sensor list includes the sensor's name and an icon representing its type, as shown in Table 7-2.

Table 7-2 Icons Displayed for Sensors

Icon	What the icon means...
	Stationary video camera icon.
	PTZ camera icon.
	Infrared camera icon.
	Access control device icon.
	Hazard detector icon. Integrates with hazard detection systems like RaeSystems.
	Radar icon. Integrates with radar devices that are used to detect, range (determine the distance of), and map various types of targets.
	Sonar icon. Integrates with sonar devices that are used for acoustic location.
	Intercom icon. Integrates with Public Announcement (PA) systems such as Intercom-Commend.
	Digital signage icon. Integrates with electronic displays installed in public spaces.
	Monitor-area icon. Allows alarms to be raised on a monitoring area instead of on a particular sensor.
	Fire detector icon. Integrates with devices that detect smoke and issue alarms.
	Microwave icon. Integrates with reconfigurable microwave networks; for example, reconfigurable wireless communication, wireless network, and reconfigurable phase array antenna.
	Fence icon. Integrates with electronic fence security systems.
	Intrusion detector icon. Integrates with software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.
	Emergency duress icon. Integrates with emergency communication systems such as panic alarms.

Table 7-2 Icons Displayed for Sensors (continued)

Icon	What the icon means...
	AED icon. Integrates with automated external heart defibrillators.
	Computer icon. Integrates with computers on the network.
	Video systems icon. Integrates with intelligent video systems such as Agent VI or Verint Nextiva.
	IP Device icon. Integrates with instrumented components such as those that provide information and notification via Windows Management Instrumentation (WMI).
	HVAC device icon. Integrates with heating, ventilating and air conditioning systems.
	BAC device icon. Integrates with Basic Access Control (BAC) systems used to read passports.
	Glass break detector icon. Integrates with devices that detect a break in a pane of glass, alerting a burglar alarm.
	Seismic detector icon. Integrates with systems that detect seismic activity.
	UPS device icon. Integrates with Universal Power Supply (UPS) systems.
	Gas detector icon. Integrates with systems that detect the presence of various gases within an area, usually as part of a system to warn about gases which might be harmful to humans or animals.
	Computer aided dispatch icon. Integrates with systems that dispatch taxicabs, couriers, field service technicians, or emergency services assisted by computer.
	Carbon monoxide detector icon. Integrates with systems that detect the presence of carbon monoxide within an area.
	Motion detector icon. Integrates with systems that quantifies motion that can be either integrated with or connected to other devices that alert the user of the presence of a moving object within the field of view.
	Application icon. Sends an alert if a PSOM Integration Module encounters systematic problems with a third-party sensor, such as loss of connection or initialization problems. Use of the Application sensor is specific to the Integration Module and covered in the relevant documentation.

Step 3 Select the sensor you want to add to the map, and click **OK**.

Step 4 Click the map on the location where the sensor should be positioned (using the left mouse button). You can continue clicking on the map to change the position of the sensor; when it is placed where you want it, right-click on the map.

Note Devices with position (0,0) are displayed with a small version of their sensor icon in the top left corner of the map.

Step 5 Save the map by clicking the **Save** button .

Step 6 If you are adding a camera sensor, you can configure its range angle, distance and orientation using graphical tools. To change the angle or field of view (FOV) for the camera, select the camera icon in the map. New icons appear in the Design Mode toolbar as shown in Table 7-3.

Note If you are still "positioning" the sensor, these new toolbar options will not appear. Right-click the map to stop positioning the sensor, and then select the sensor's icon on the map. The new toolbar options should now appear.

Table 7-3 Camera Sensor Angle and Field of View Design Tools

This icon...	Does this to the camera sensor...
	Rotate the camera angle clockwise.
	Rotate the camera angle counter-clockwise.
	Widen the camera's field of view (FOV).
	Shrink (or make more narrow) the camera's field of view (FOV).
	Increase the distance that can be viewed within the camera's field of view (FOV).
	Decrease the distance that can be viewed within the camera's field of view (FOV).

Step 7 Use the camera sensor design tools to adjust the camera's angle and field of view.

Step 8 Repeat these steps to place all sensors for this node on the corresponding map.

Step 9 Once you've placed a sensor on the map you can move it by clicking .

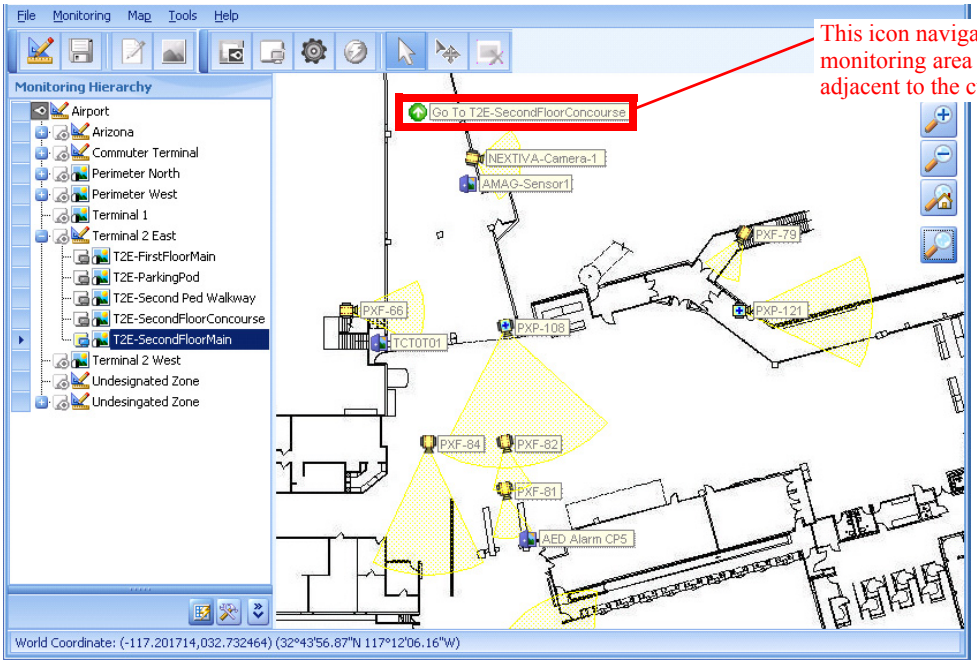
Step 10 If you are done modifying the map, exit from the Design Mode to save your changes. Select **Map > Exit Map Design Mode**.

You can also adjust the angle, range or direction of the camera's field of view by right-clicking the video camera sensor icon on the map and selecting **Properties** from the right-click menu. The Sensor Properties window appears where you can make these changes. See the "Adding new Sensors for Video Cameras" section on page 6-7 for details on the fields in this window.

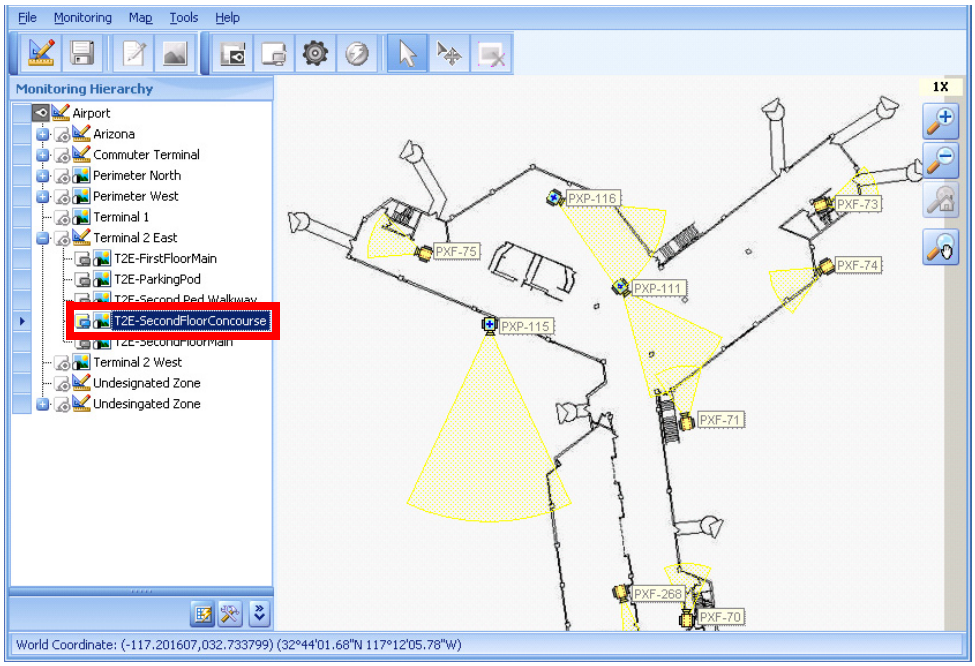
Adding Navigation to Maps

You can add Navigator icons to maps that allow operators to traverse from the current map view to a map for an adjacent monitoring area.

For example, the following map shows a Navigate Up icon that goes to the T2E-SecondFloorConcourse monitoring area.



When the operator double-clicks the Navigate icon, the map view for the T2E-SecondFloorConcourse area is displayed in the Map View Pane.

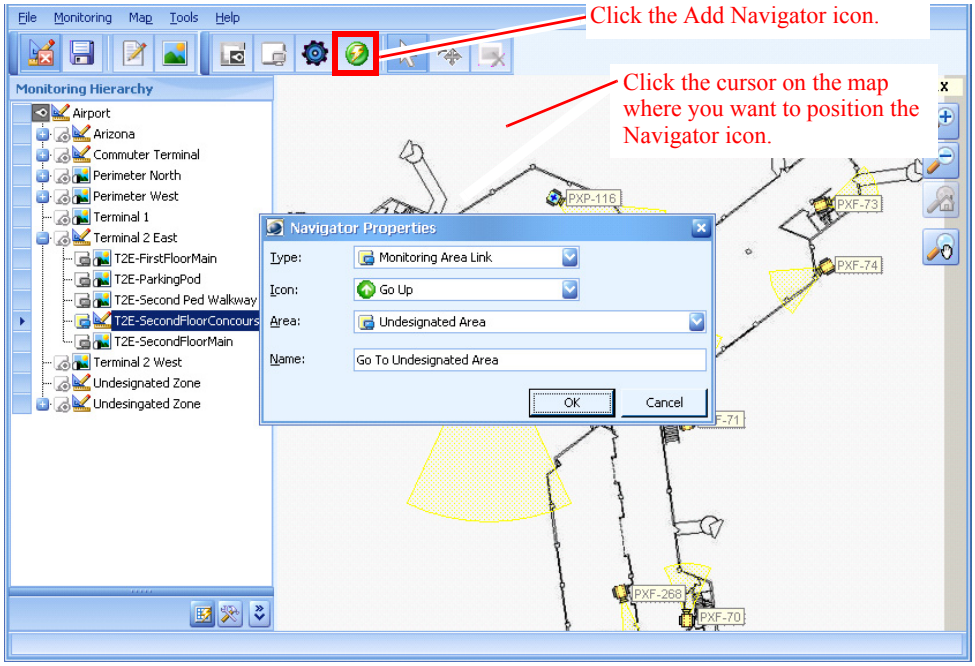


To add Navigator icons to a map:

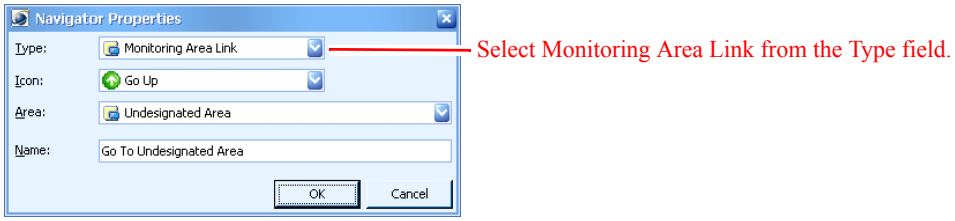
Step 1 Select the node's listing in the Monitoring Tree.

Step 2 Click the **Add Navigator** icon in the Design Mode toolbar.

Step 3 Click the location in the map where you want the Navigator icon positioned.

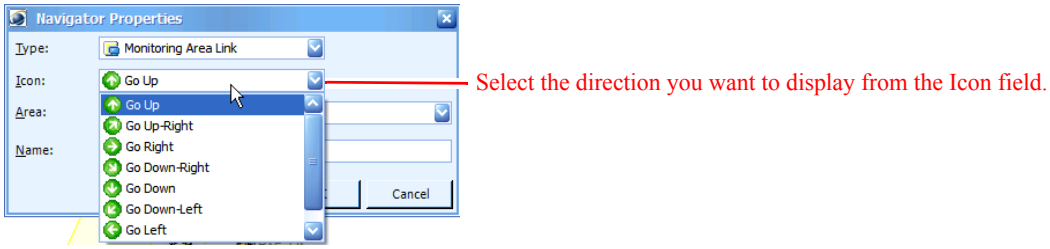


The Navigator Properties window appears.



Step 4 From the **Type** field, select **Monitoring Area Link**.

Step 5 From the **Icon** field, make a selection depending on the logical direction in which you're navigating.

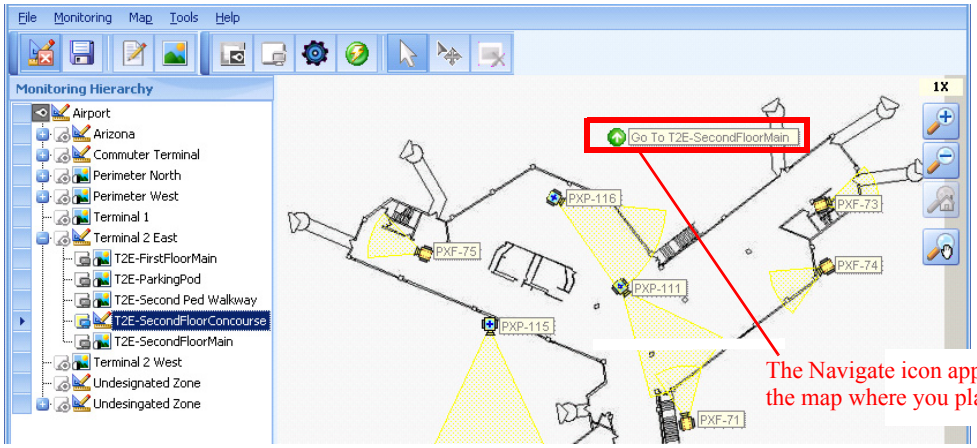


Step 6 From the **Area** field, select the monitoring area to which the operator will navigate when the Navigator icon is clicked.

Step 7 In the **Name** field, enter text that should appear on the map next to the Navigator icon. This text could explain what will happen when the icon is clicked.

Step 8 Click **OK**.

A green Navigator icon appears on the map where it was positioned.



Step 9 Once you've placed a navigator on the map you can move it by clicking .

Step 10 If you are done modifying the map, exit from the Design Mode to save your changes. Select **Map > Exit Map Design Mode**.

Adding URL Links to Maps

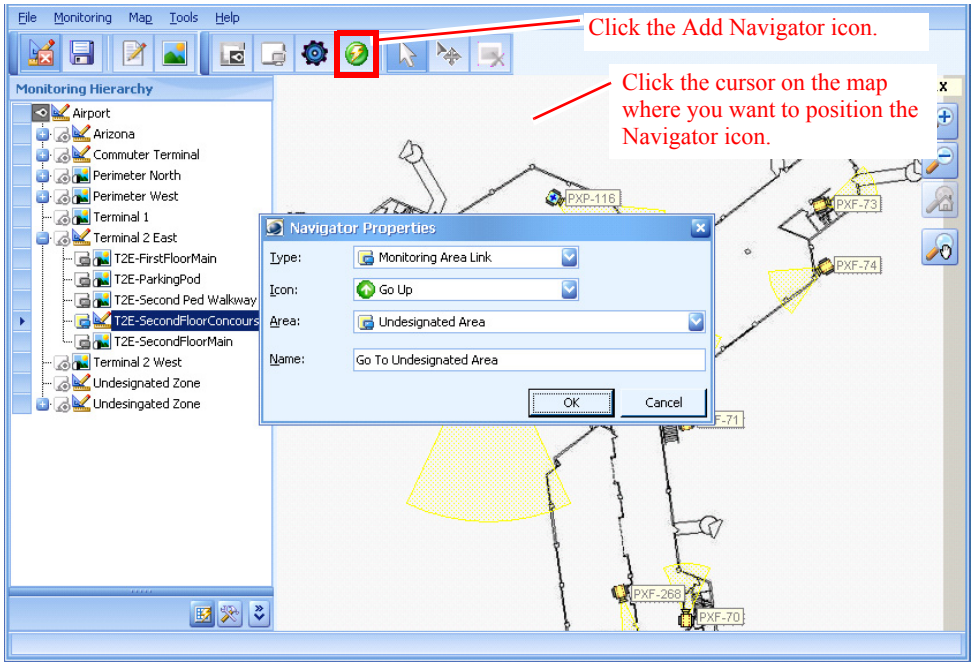
You can add a URL link to a map so that the user can launch a Web browser to view a web page—directly from a map.

To add a URL icon to a map:

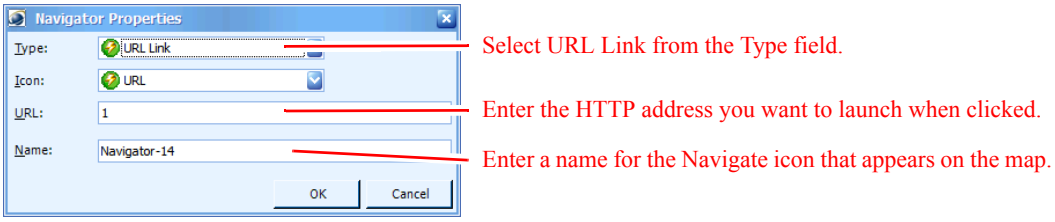
Step 1 Select the node's listing in the Monitoring Tree.

Step 2 Click the **Add Navigator** icon in the Design Mode toolbar.

Step 3 Click the location in the map where you want the Navigator icon positioned.



The Navigator Properties window appears.



Step 4 From the **Type** field, select **URL Link**.

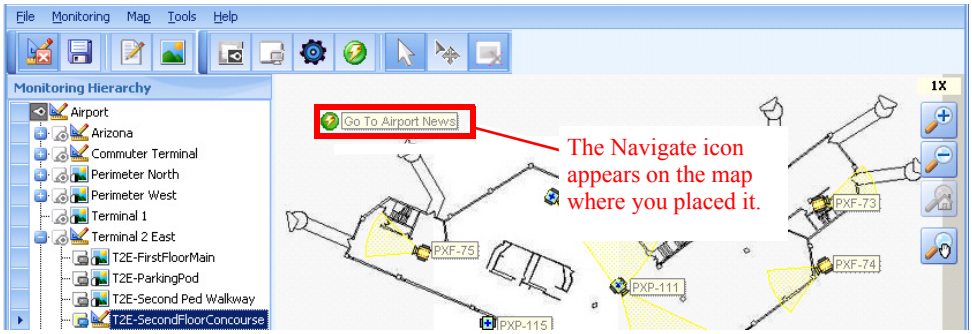
Step 5 From the **Icon** field, select **URL**.

Step 6 In the **URL** field, enter the HTTP address where the web page is located.

Step 7 In the **Name** field, enter text that should appear on the map next to the URL icon. This text could explain what will happen when the icon is clicked.

Step 8 Click **OK**.

A green Navigator icon appears on the map where it was positioned.



Step 9 Once you've placed a URL icon on the map you can move it by clicking .

Step 10 If you are done modifying the map, exit from the Design Mode to save your changes. Select **Map > Exit Map Design Mode**.

Editing and Deleting Items from the Map

To edit an icon on a map:

Step 1 Right-click the icon in the map view.

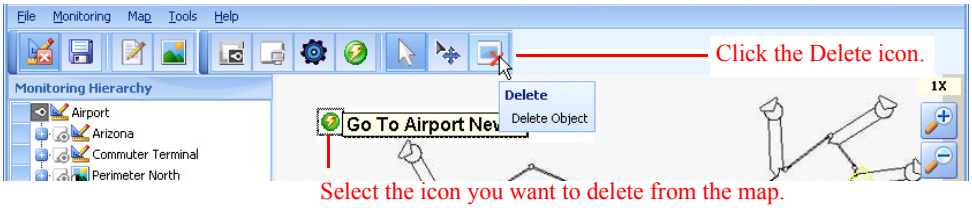
Step 2 Select **Properties** from the right-click menu.

The Properties window appears.

Step 3 Make necessary changes and click **OK** to save them to the database.

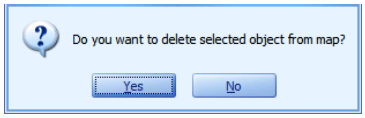
To remove an icon from a map:

Step 1 Select the icon so that it is highlighted on the map.



Step 2 Click the **Delete** icon in the Design Toolbar.

A confirmation dialog box appears.



Step 3 Click **Yes** to confirm the deletion.

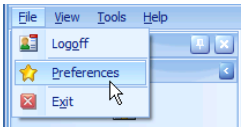
Step 4 If you are done modifying the map, exit from the Design Mode to save your changes. Select **Map > Exit Map Design Mode**.

Setting the Sort Order of the Monitoring Hierarchy

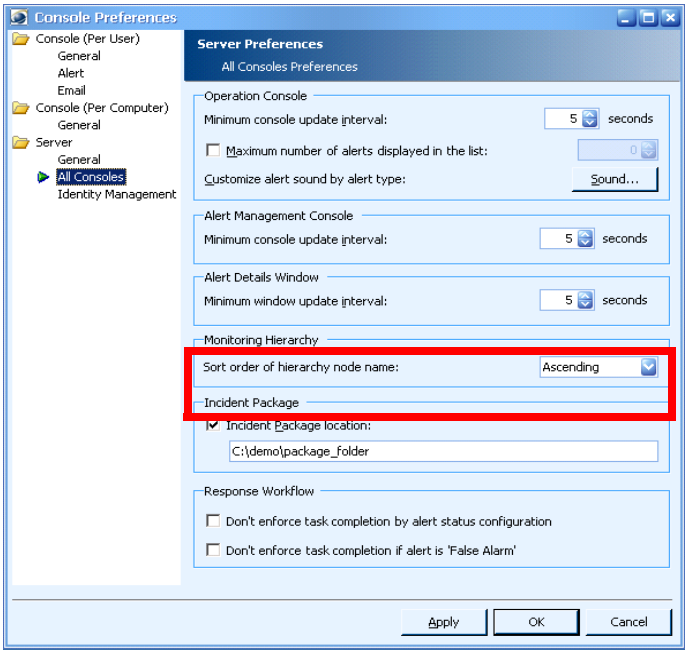
You can set the sort order for the Monitoring Hierarchy in server Preferences.

To set the sort order:

Step 1 Select **File > Preferences**.



Step 2 Select **All Consoles** under **Server**.

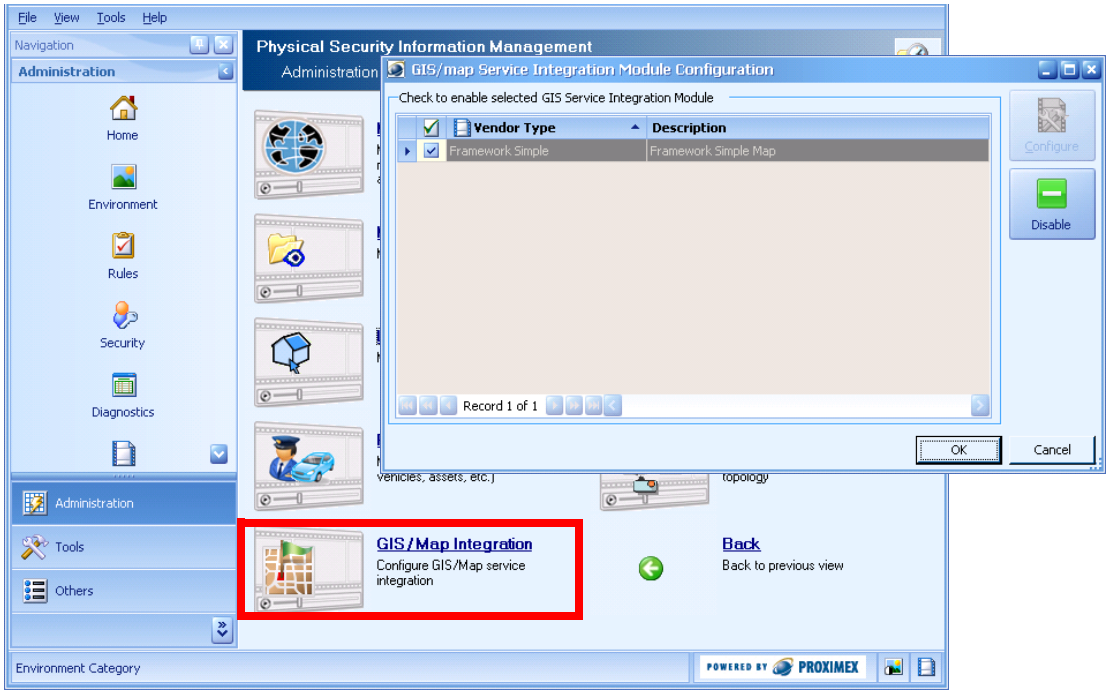


Step 3 Make a selection from the **Sort order of hierarchy node name** field: No Order, Ascending or Descending.

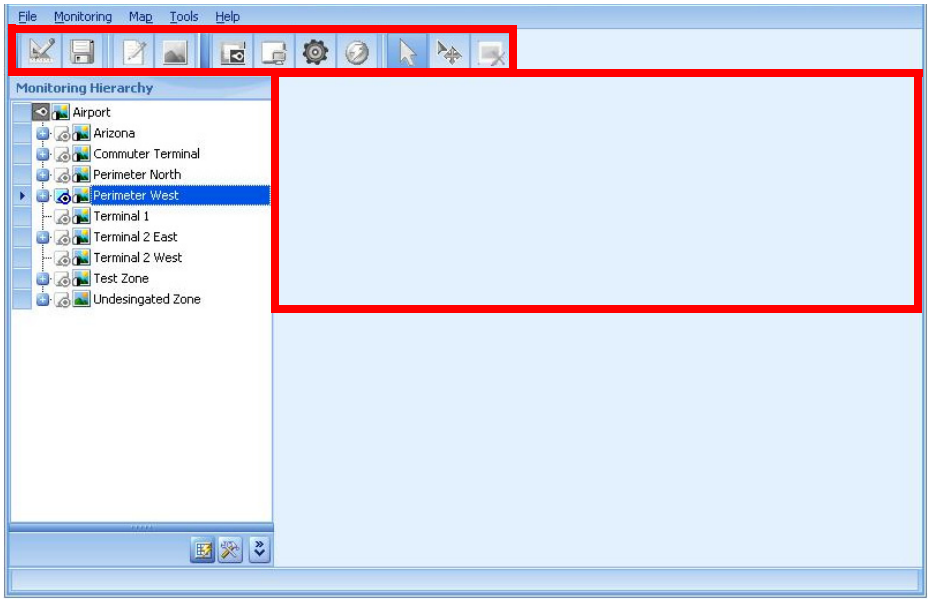
Step 4 Click **OK** to save your changes.

Integrating GIS Maps with PSOM

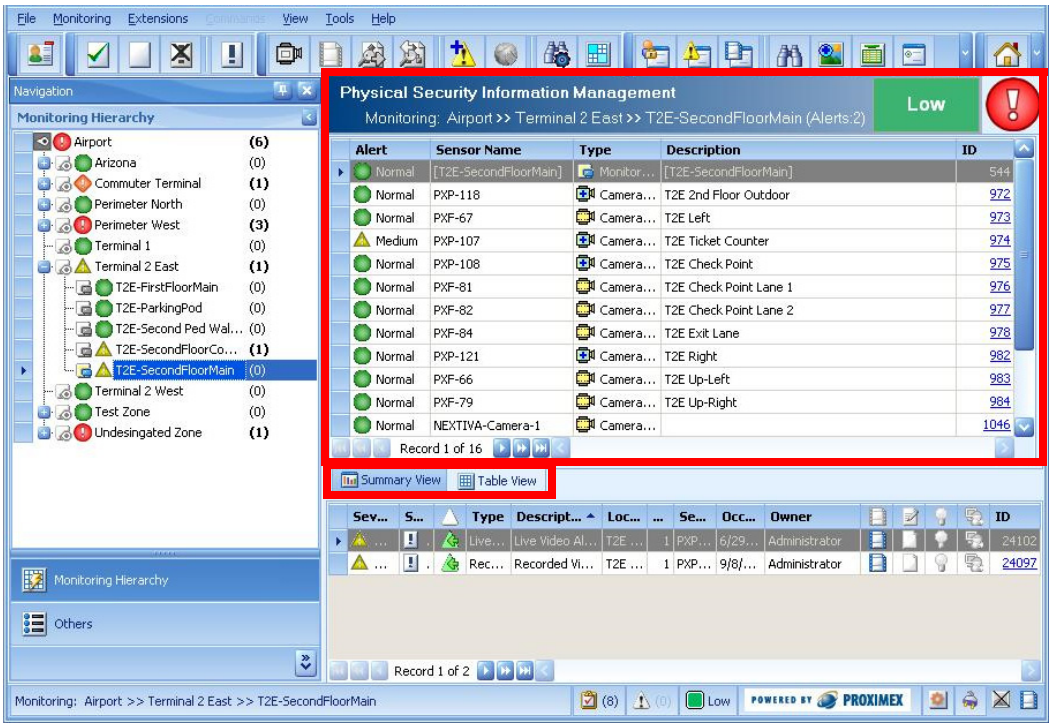
In future releases of PSOM, you will be able to integrate third-party GIS map software with PSOM using the **GIS Map Integration** feature from the **Environment** area of the Administration Console.



Currently, the only GIS map integration module that appears in the GIS/map Service Integration Module Configuration window is the one supplied with PSOM called **Framework Simple**. If you disable this module (by selecting it and clicking Disable), then all map-related features will be disabled in all PSOM Consoles. For example, the Environment Management window in the Administration Console will not show maps in the right pane and the map toolbar will be disabled.



In the Operation Console, the Map View Pane will not appear, as shown next.



CHAPTER 8

Managing Response Task Items and Response Workflow Rules

You can configure *response task items* that specify "best practices" for the actions that an operator should take to resolve alerts. You can then configure *response workflow rules* that generate checklists of actions operators must take when certain types of alerts are raised. With these rules in place, it is easy for operators to follow standardized procedures which leads to fewer errors in response and more importantly a faster time to response.

This chapter describes:

- How response tasks work in the Operation Console
- How to add, modify, or delete response task items
- How to add, modify, or delete response workflow rules
- How to apply response workflow rules to different types of alerts

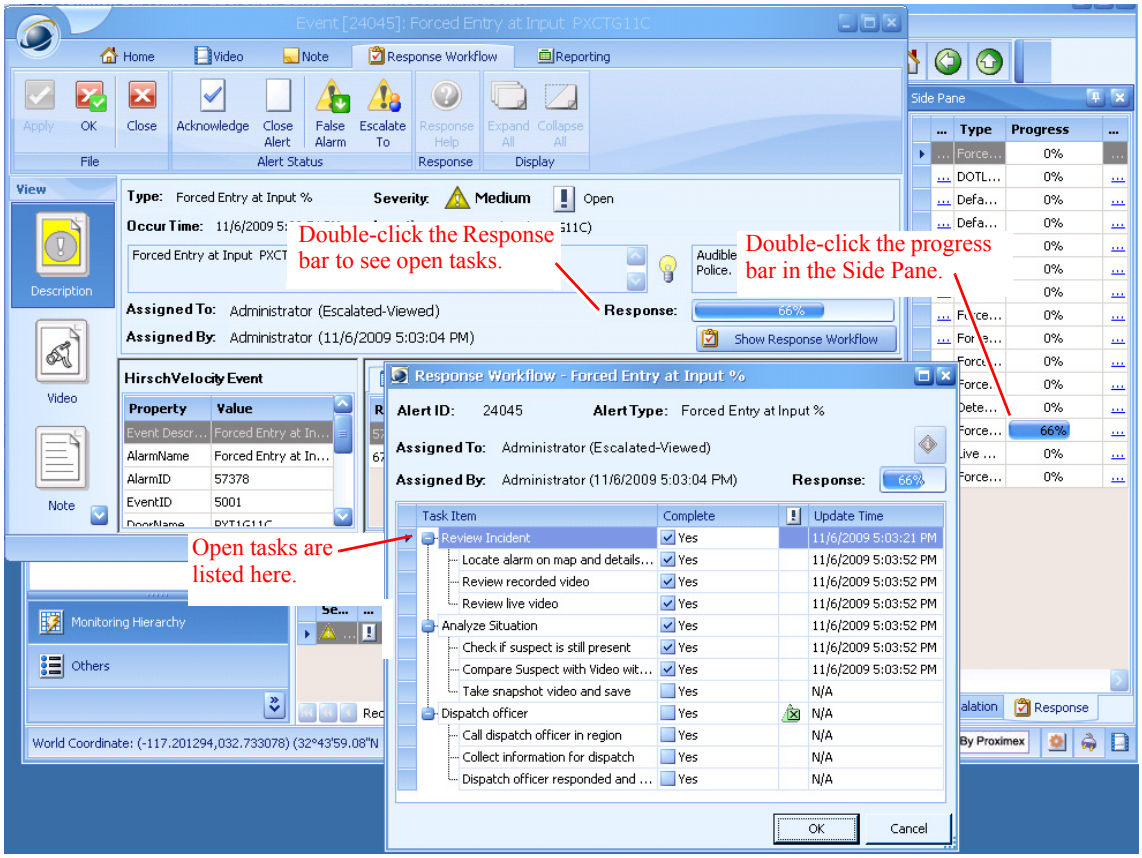
This chapter includes these topics:

- Response Tasks within the Operation Console, page 8-1
- Managing Response Task Items, page 8-2
- Managing Response Workflow Rules, page 8-9
- Applying a Response Workflow Rule to an Alert Type, page 8-15
- Enforcing Task Completion in the Operation Console, page 8-19

Response Tasks within the Operation Console

Within the Operation Console, operators can be assigned specific tasks to complete before an alert can be acknowledged or closed. Configuring task checklists for alerts helps ensure that operators take appropriate action when an alert occurs, as defined by the security experts at your company. Within the Operation Console, the Response Workflow Pane on the right side of the window shows operators their progress towards fulfilling their responsibilities for various alerts.

Operators can access response task checklists by double-clicking a progress bar in the Response Workflow Pane to bring up the Alert Details window. Then they can double-click the **Response** bar to view the task checklist for the alert.



A task checklist in the Operation Console is comprised of *response task items* that you configure using the Administration Console. For example, “Notify Police” in the above screen is a response task item. The *response workflow rule* defines which response task items must be completed for certain types of alerts before the alert can be acknowledged or closed.

When response workflow rules are applied along with escalation business logic, then response task items are only associated with alerts when the alerts are escalated (“new,escalated” and “escalated,viewed”). For example, escalation is applied to the system to redirect alerts after a set amount of time to a user/user group. Then response workflow rules are applied to select alert types. Under these conditions, response task items are associated with alerts when newly-created alerts are escalated by the system or un-escalated alerts are viewed for the first time.

If you subsequently remove the applied response workflow rule, and then open an alert to view it, even if the alert has been escalated there will not be any response tasks associated with the alert. If you change the response workflow rule and reapply it, then existing non-escalated and non-viewed alerts will assume the new response task items when the alert is escalated.

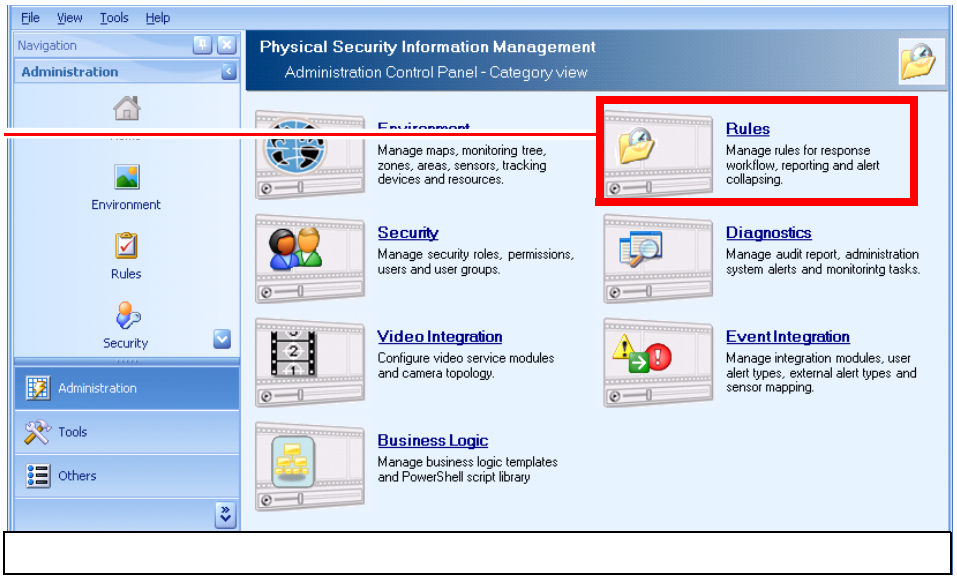
Managing Response Task Items

Response task items are the specific steps that appear in the response task checklists for operators. Response workflow rules are comprised of several response task items.

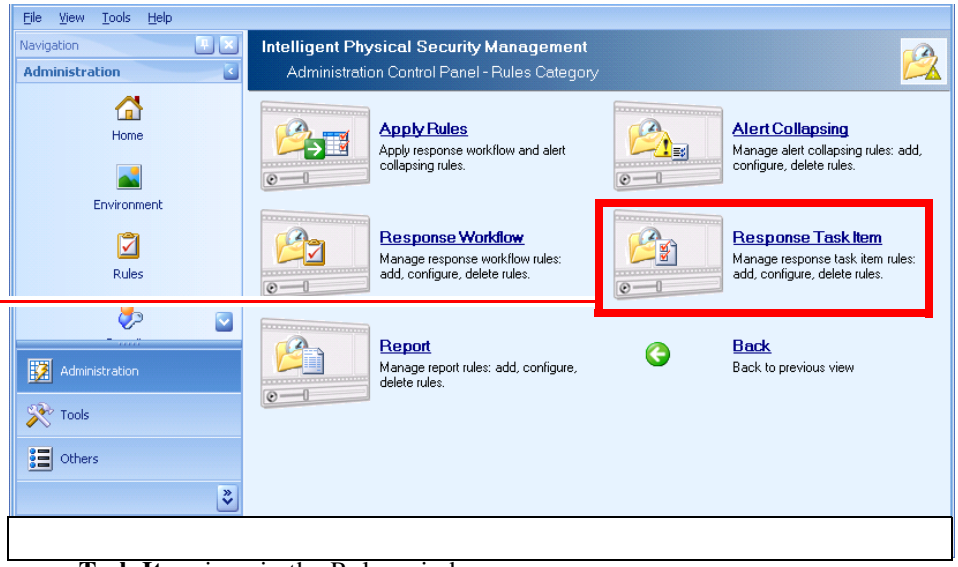
Adding a New Response Task Item

To add a response task item:

Step 1 Click the **Rules** icon in the Administration Console.

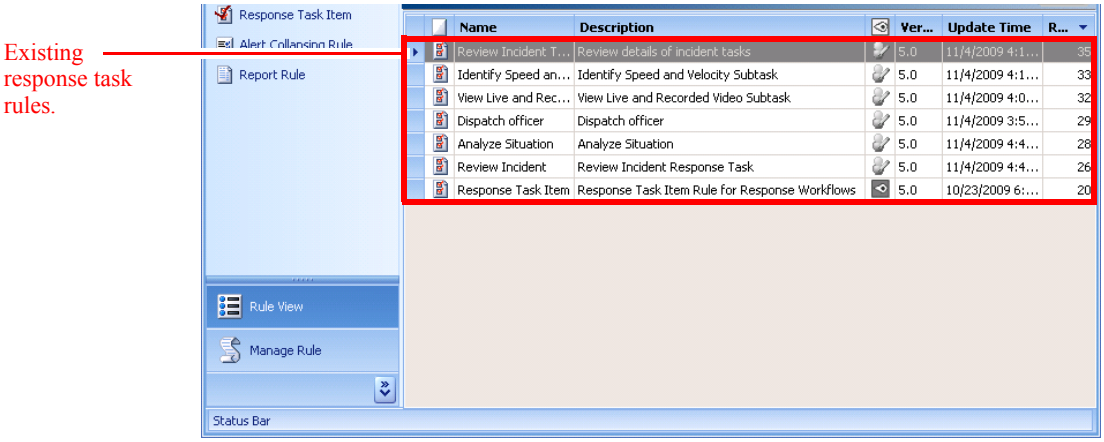


The Rules window appears.

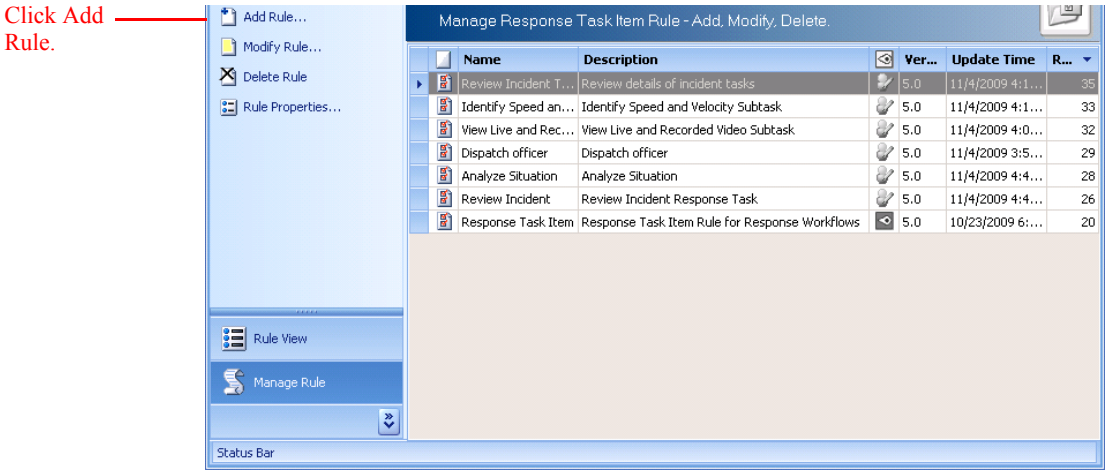


Step 2 Click the **Response Task Item** icon in the Rules window.

The Response Task Item Rule window appears.

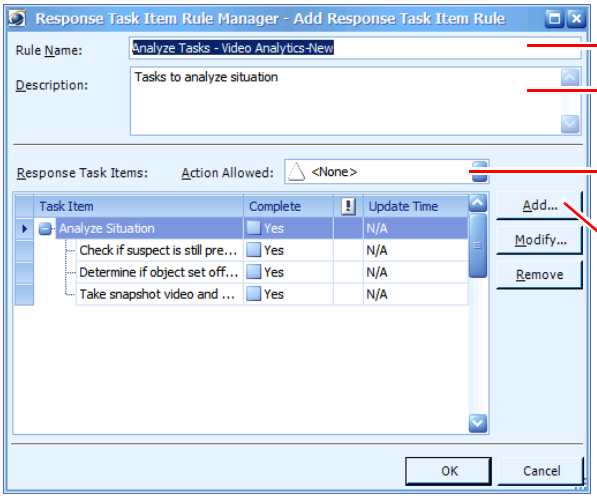


Step 3 Click **Manage Rule** in the left navigation pane.



Step 4 Click **Add Rule** under **Manage Rule** in the left pane.

The Add Task Item Rule window appears.



Enter a name for the task item.

Provide a description of the task item.

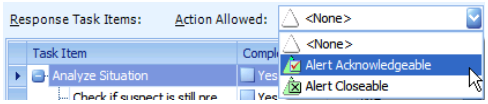
Make a selection to assign importance to this alert.

Click Add to define the task's checklist item.

Step 5 In the **Rule Name** field, enter a name for this new task item.

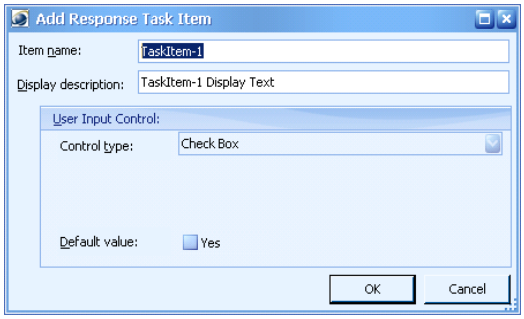
Step 6 In the **Description** field, enter information about this task item.

Step 7 From the **Action Allowed** field, make a selection to assign importance to this task item. For example, if the operator should complete this task before being allowed to acknowledge the alert, then select **Alert Acknowledgeable**.



Step 8 Click **Add**.

The Add Response Task Item window appears.

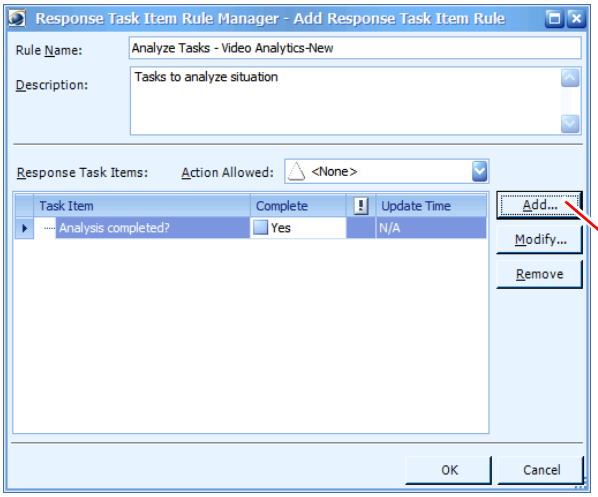


Step 9 In the **Item name** field, enter the name of the checklist item.

Step 10 In the **Display description** field, enter more information about the checklist item.

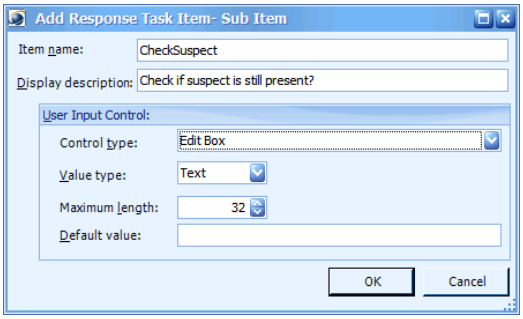
Step 11 Click **OK**.

The Add Task Item Rule window re-appears.



Step 12 If you want to add a sub-item to the primary task item, select the primary task item in the list and click **Add**.

The Add Response Task Item - Sub Item window appears.



Step 13 In the **Item name** field, enter the sub-task checklist item you want displayed.

Step 14 In the **Display description** field, enter an explanation of this field.

Step 15 From the **Control type** field, select the type of field you want to create: **Edit Box** or **Check Box**.

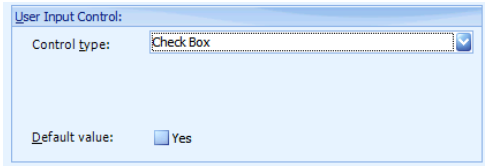
Step 16 For edit boxes:

a. Select the type of information to be captured by the field from the **Value type** field. Choices are **text** or **integer**.

b. Enter the maximum characters that can be entered in the field in the **Maximum length** field.

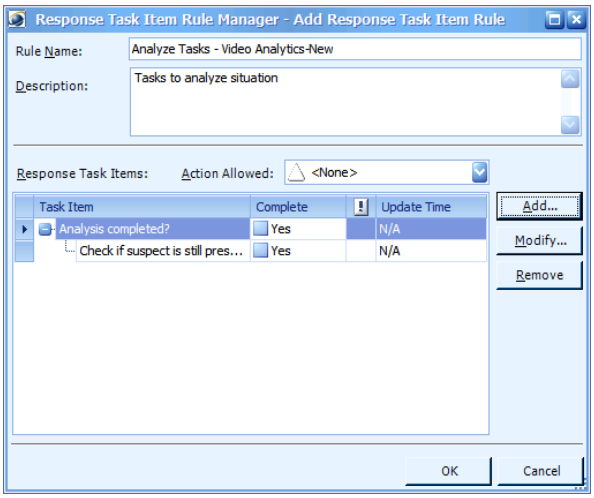
c. Enter the text that should be displayed initially in the field in the **Default value** field.

Step 17 For check boxes, determine whether to put a check in this checklist item by default, or leave the item unchecked, using the **Default value** field.



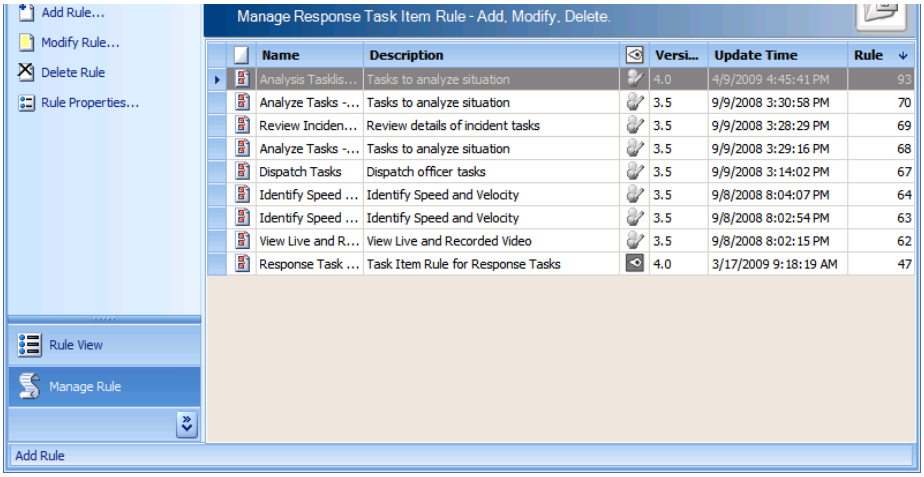
Step 18 Click **OK**.

The Add Task Item Rule window re-appears.



Step 19 Click **OK** to save your new task item.

Your new task item now appears in the Response Task Item Rule window.



Once you've added the task items you need, the next step is to define *response workflow rules* that incorporate multiple task items to define a standard operating procedure for alert response. See the "Managing Response Workflow Rules" section on page 8-9.

Modifying a Response Task Item

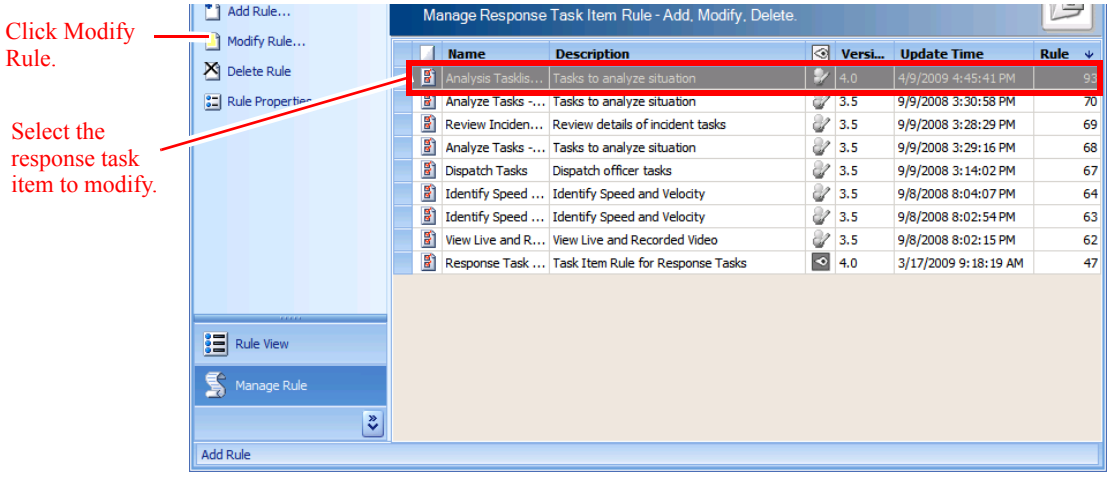
Step 1 Click the **Rules** icon in the Administration Console.

The **Rules** window appears.

Step 2 Click the **Response Task Item** icon in the Rules window.

The Response Task Item Rule window appears.

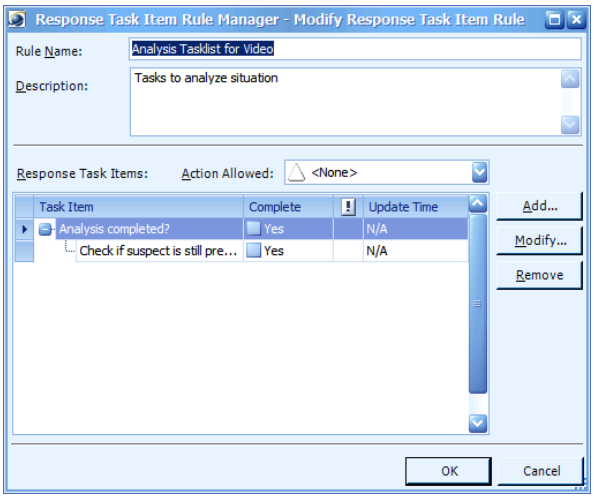
Step 3 Click **Manage Rule** in the left navigation bar.



Step 4 Select the response task item you want to modify from the list.

Step 5 Click **Modify Rule** under **Manage Rule** in the left pane.

The Modify Response Task Item window appears.



Step 6 Change the properties of the task item as desired. See the "Adding a New Response Task Item" section on page 8-3 for information.

Step 7 Click **OK**.

Deleting a Response Task Item

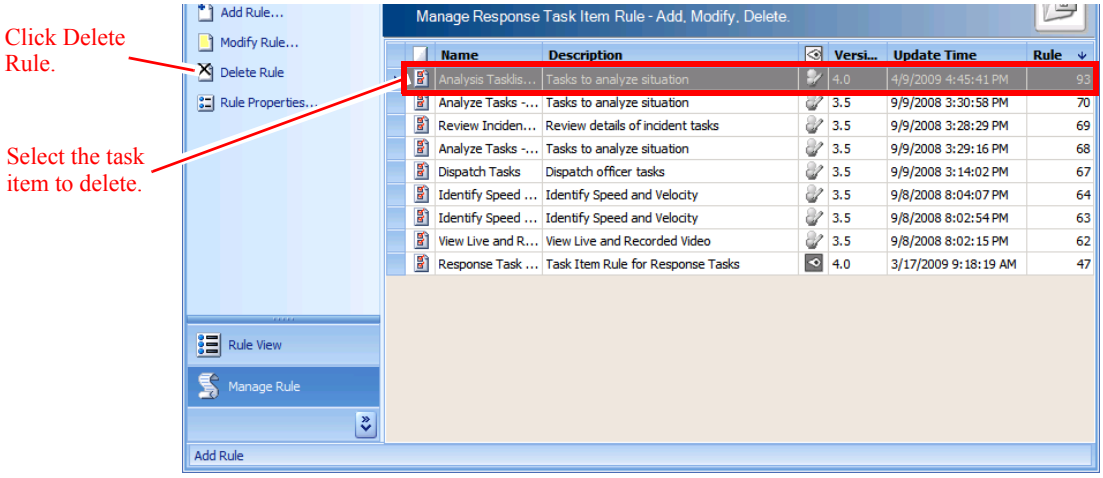
Step 1 Click the **Rules** icon in the Administration Console.

The **Rules** window appears.

Step 2 Click the **Response Task Item** icon in the Rules window.

The Response Task Item Rule window appears.

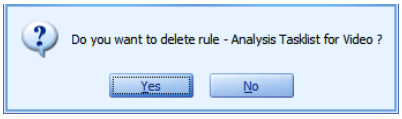
Step 3 Click **Manage Rule** in the left navigation bar.



Step 4 Select the response task item you want to modify from the list.

Step 5 Click **Delete Rule** under **Manage Rule** in the left pane.

A confirmation dialog box appears.



Step 6 Click **Yes** to delete the response task item.

Managing Response Workflow Rules

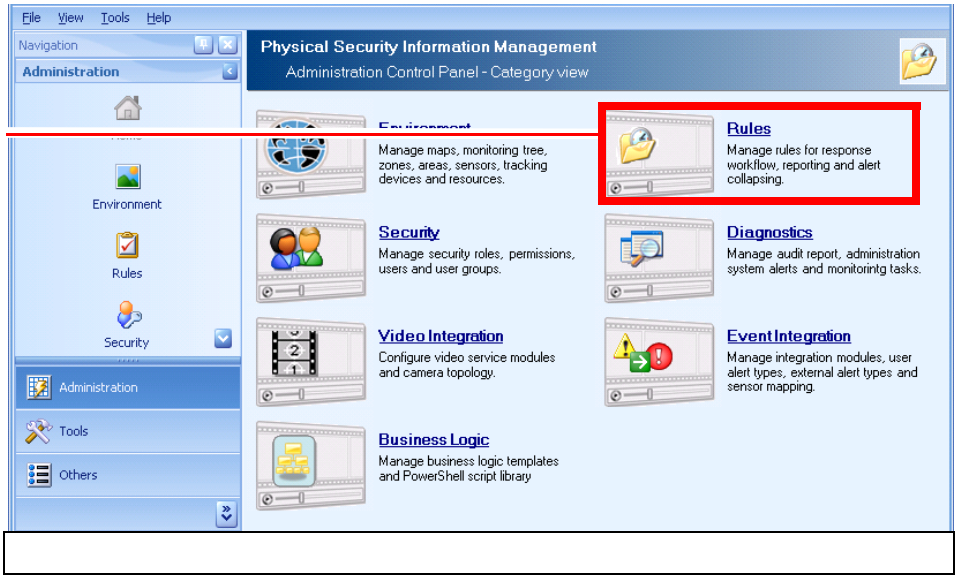
You can build response workflow rules that define the standard operating procedure for responding to different types of alerts. Response workflow rules are built from response task items, and are applied to specific types of alerts.

See the "Managing Response Task Items" section on page 8-2 for information about adding new response task items.

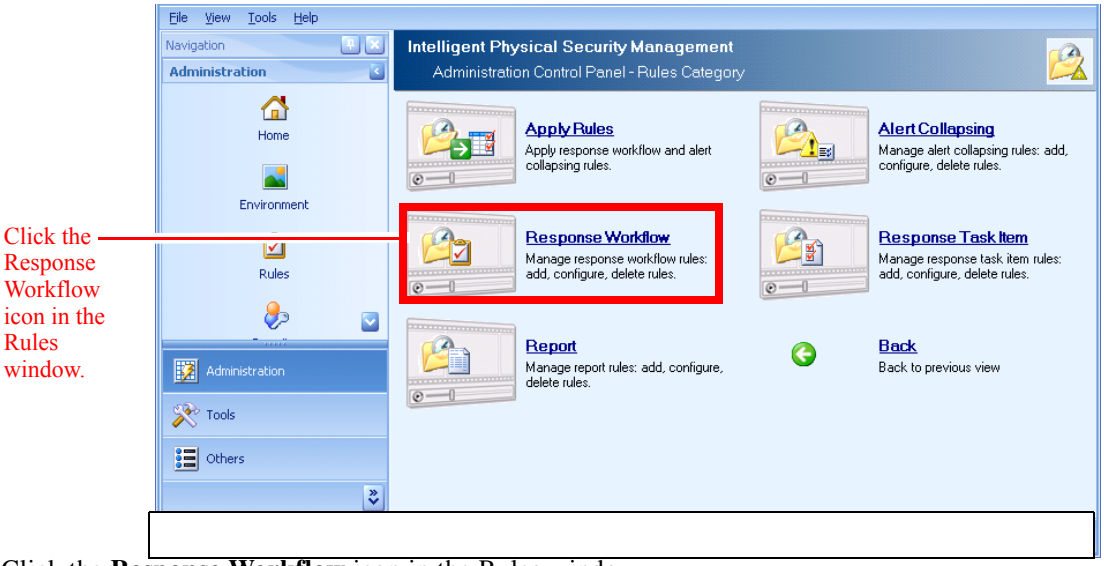
Adding a New Response Workflow Rule

To add a response workflow rule:

Step 1 Click the **Rules** icon in the Administration Console.

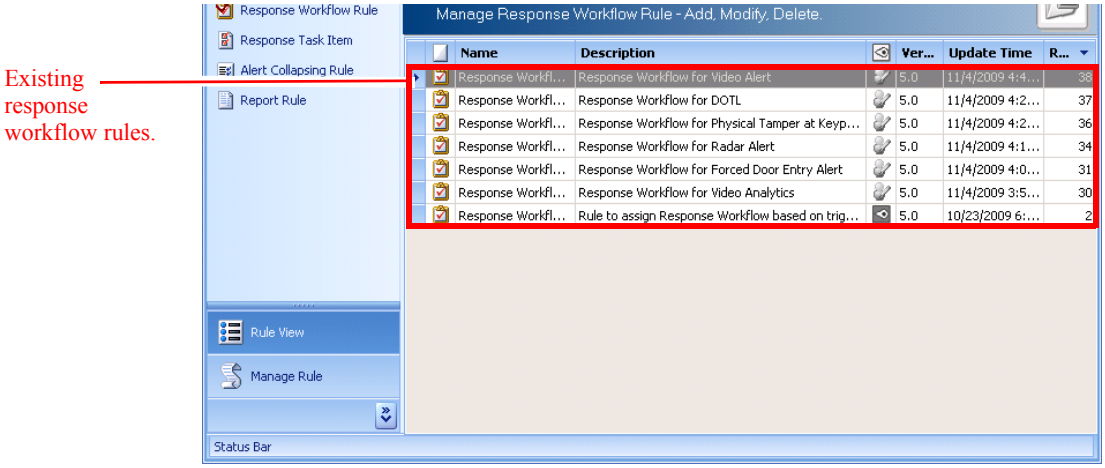


The Rules window appears.

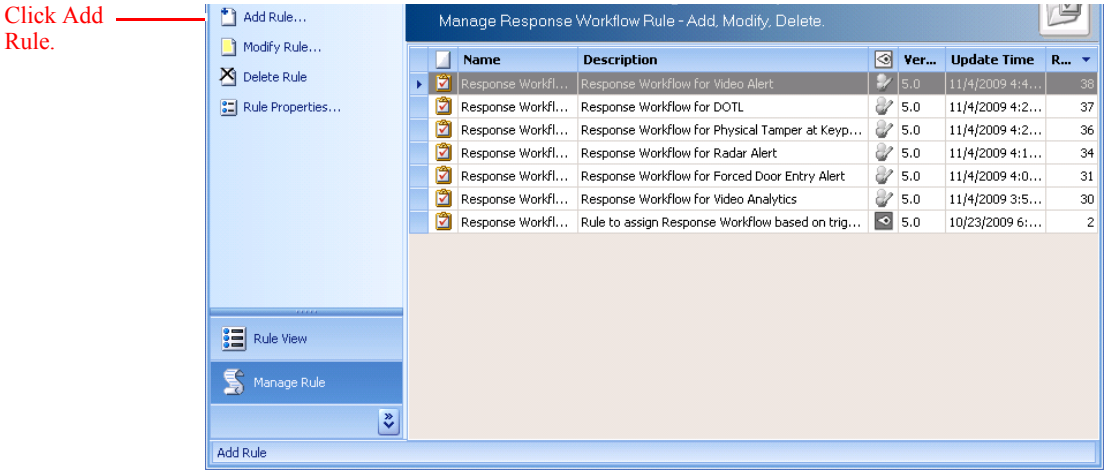


Step 2 Click the **Response Workflow** icon in the Rules window.

The Response Workflow Rule window appears.

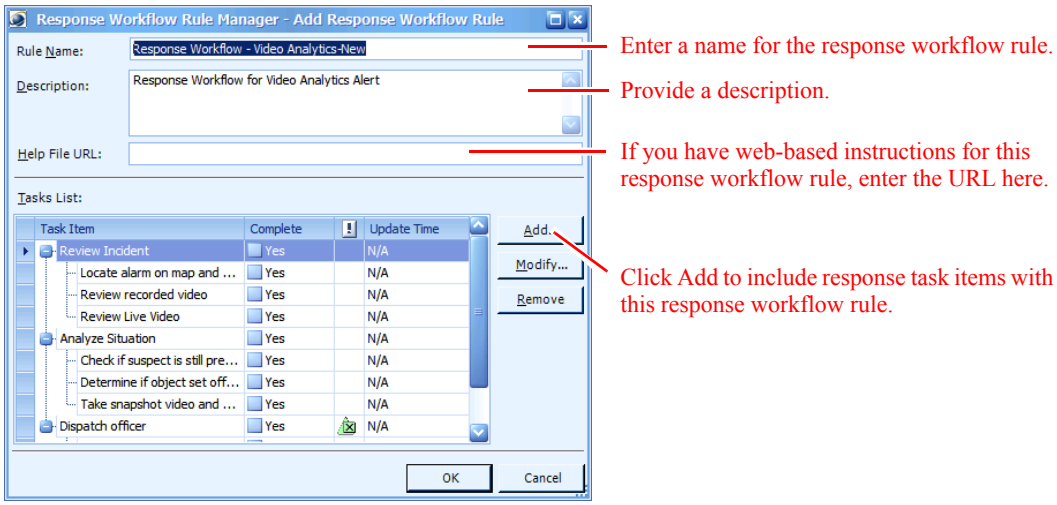


Step 3 Click **Manage Rule** in the left navigation pane.



Step 4 Click **Add Rule** under **Manage Rule** in the left pane.

The Add Response Workflow Rule window appears.



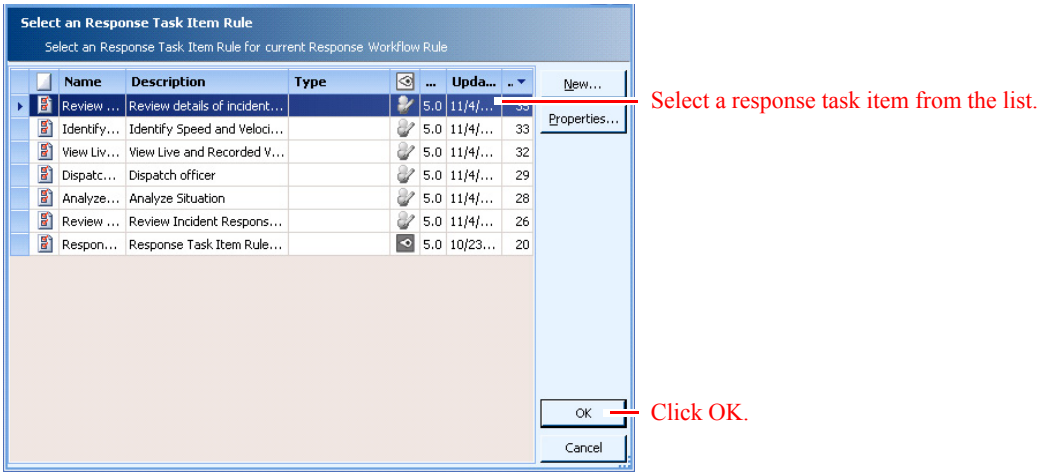
Step 5 In the **Rule Name** field, provide a name for the new response workflow rule.

Step 6 In the **Description** field, enter information about this response workflow rule.

Step 7 If you have web-based instructions for this response workflow rule, enter the URL in the **Help File URL** field. The web address should be entered as a full HTTP address; for example, "http://www.mycompany.com/instructions/sop.html".

Step 8 Click **Add** to include response task items as part of this response workflow rule.

The Select a Response Task Item Rule window appears.



Step 9 Select the response task item you want to add from the list.

Step 10 Click **OK**.

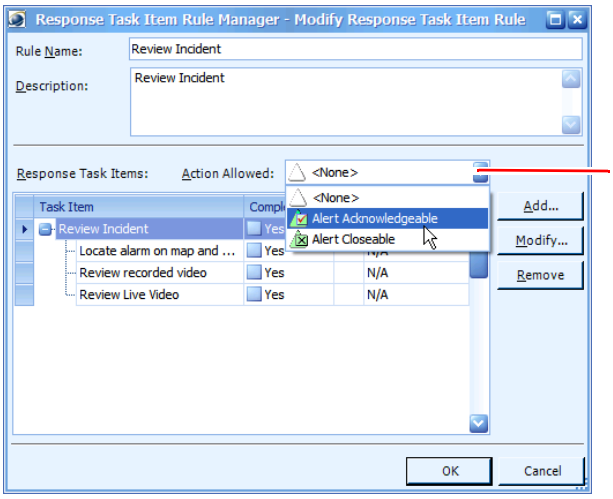
Step 11 Add as many response task items as you need to the response workflow rule.

Step 12 Once you have your response task items selected, you need to determine which response task items must be completed before the alert can be acknowledged, and closed. Then:

a. Select the response task item from the list.

b. Click **Modify**.

The Modify Response Task Item window appears.



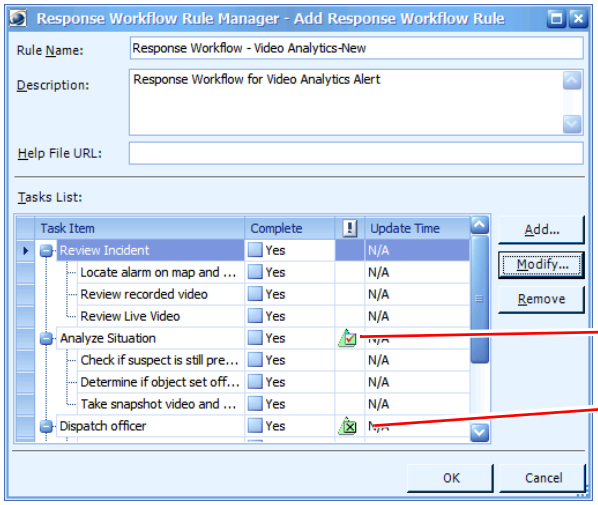
Make a selection from the Action Allowed field.

c. From the **Action Allowed** field, select either **Alert Acknowledgeable** or **Alert Closeable**.

d. Click **OK**.

Note You must have a task item assigned as **Alert Closeable**.

Step 13 Your completed Add Response Workflow Rule window may appear similar to the next screen.



This task item must be completed before the alert can be acknowledged.

This task item must be completed before the alert can be closed.

Step 14 If you want to remove a task item, select it in the list and click **Remove**.

Step 15 If you want to modify a task item, select it in the list and click **Modify**.

Step 16 Click **OK** when you're finished.

The final step is to apply the response tasks rule to an alert type. See the "Applying a Response Workflow Rule to an Alert Type" section on page 8-15 for information.

Modifying a Response Workflow Rule

To change a response workflow rule:

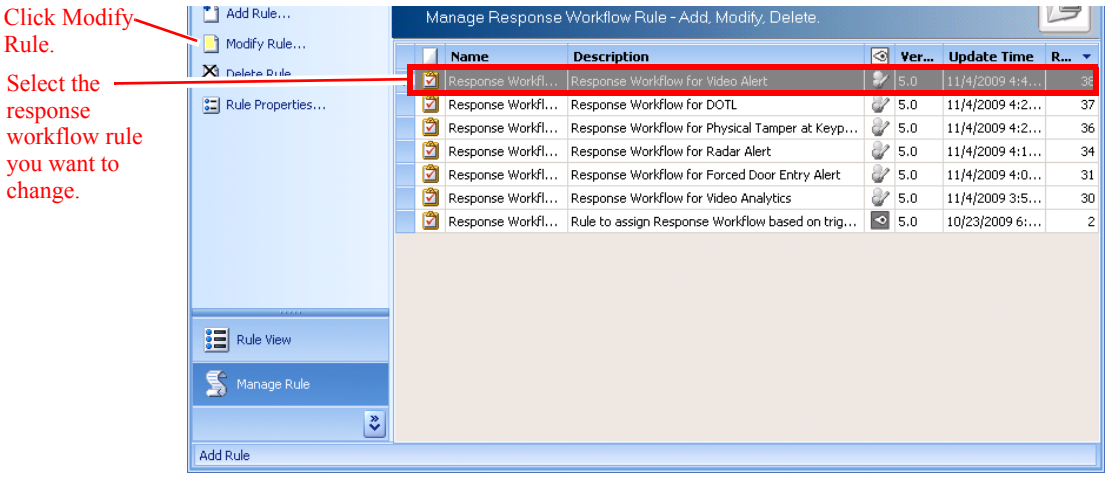
Step 1 Click the **Rules** icon in the Administration Console.

The Rules window appears.

Step 2 Click the **Response Workflow** icon in the Rules window.

The Response Workflow Rule window appears.

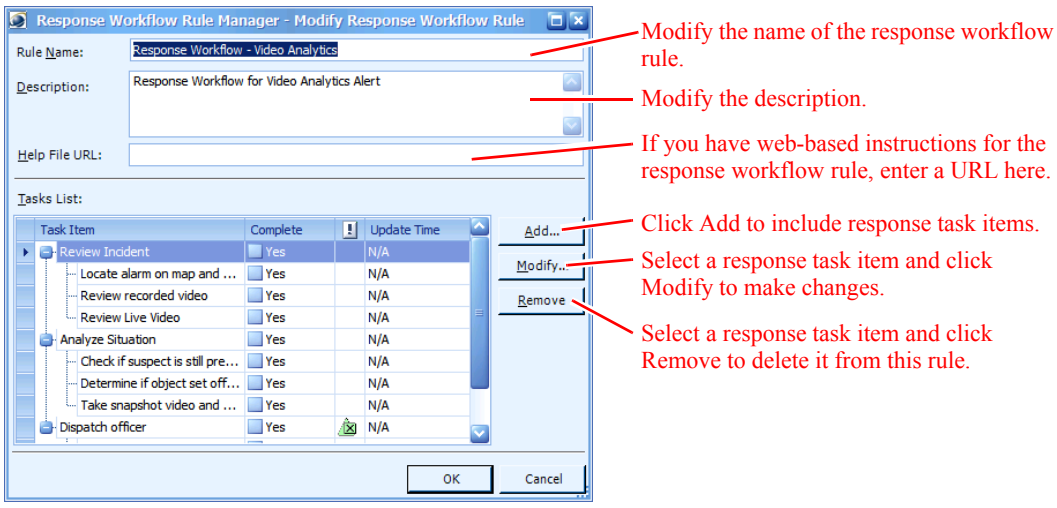
Step 3 Click **Manage Rule** in the left navigation pane.



Step 4 Select the response workflow rule you want to change from the list.

Step 5 Click **Modify Rule** under **Manage Rule** in the left pane.

The Modify Response Workflow Rule window appears.



Step 6 Make changes as necessary and click **OK**.

Deleting a Response Workflow Rule

To remove a response workflow rule:

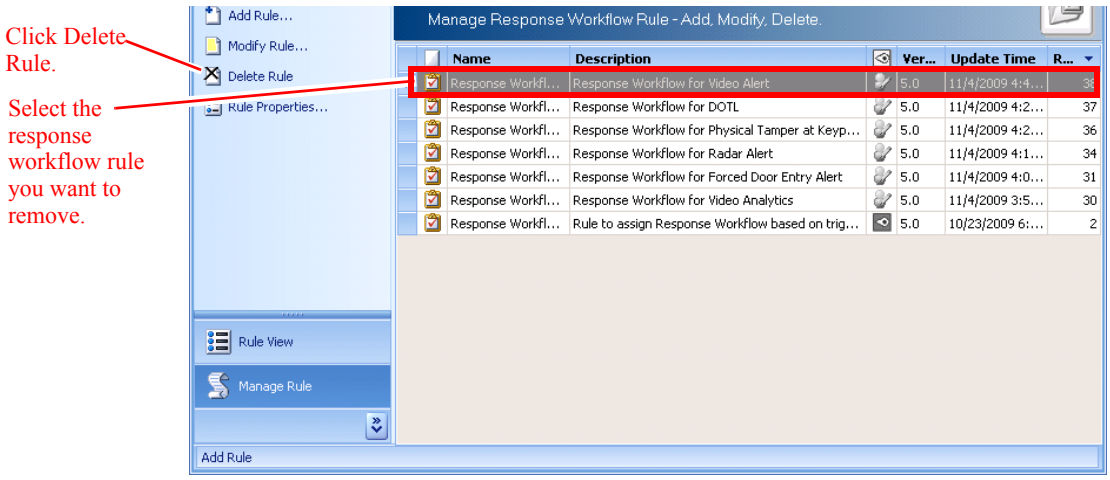
Step 1 Click the **Rules** icon in the Administration Console.

The Rules window appears.

Step 2 Click the **Response Workflow** icon in the Rules window.

The Response Workflow Rule window appears.

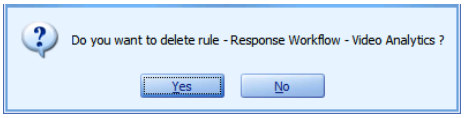
Step 3 Click **Manage Rule** in the left navigation pane.



Step 4 Select the response workflow rule you want to remove from the list.

Step 5 Click **Delete Rule** under **Manage Rule** in the left pane.

A confirmation dialog box appears.



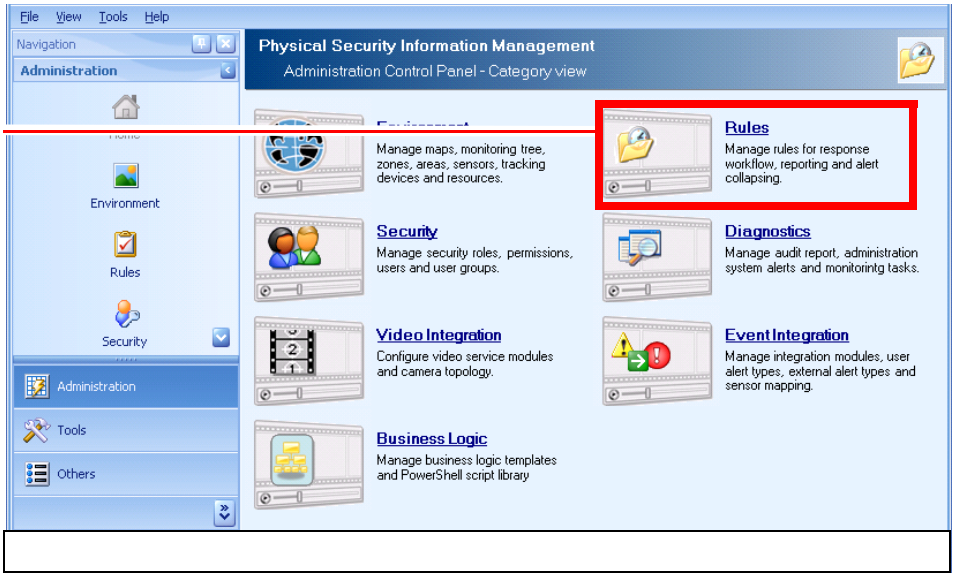
Step 6 Click **Yes** to remove the response workflow rule.

Applying a Response Workflow Rule to an Alert Type

You can apply a response workflow rule to an alert type to specify standard operating procedures for responding to that alert type across PSOM. Only one response workflow rule can be applied for each alert type.

To apply a response workflow rule to an alert type:

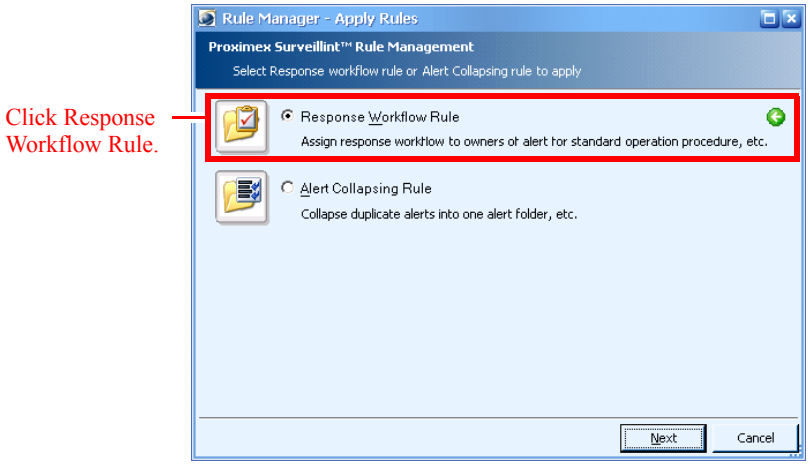
Step 1 Click the **Rules** icon in the Administration Console.



The Rules window appears.

Step 2 Click the **Apply Rules** icon in the Rules window.

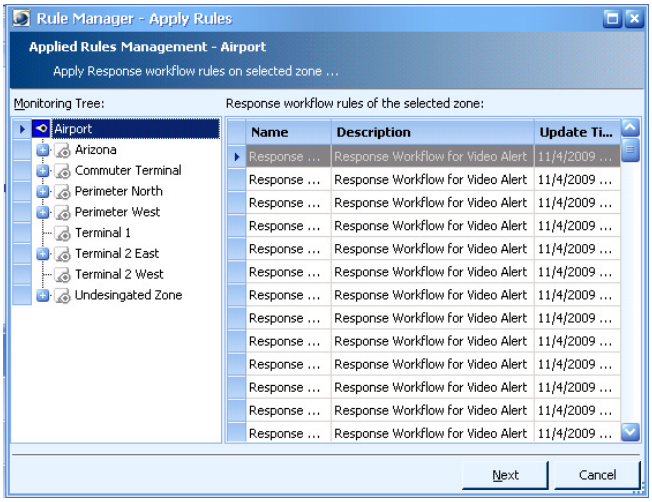
The Apply Rules window appears.



Step 3 Click **Response Workflow Rule**.

Step 4 Click **Next**.

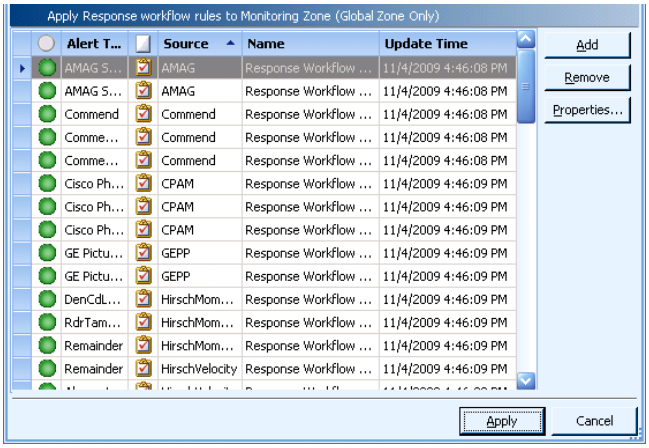
The Applied Rules Management window appears.



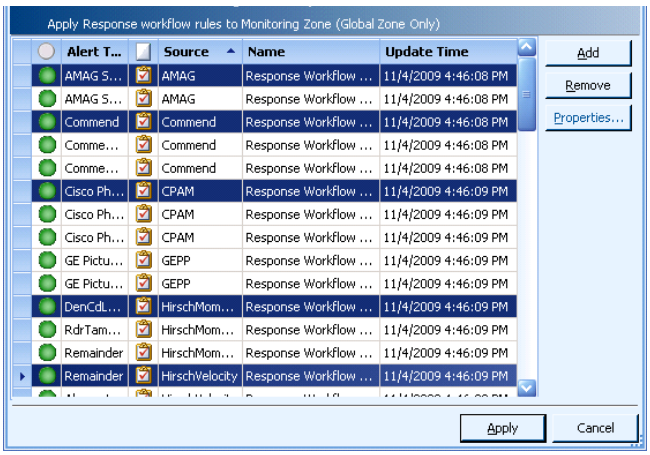
Step 5 Click **Next**.

Note For this release, response workflow rules can only be applied to the top-level node in the Monitoring Tree. Therefore, no action needs to be taken on this screen.

The Apply Response Workflow Rules to Monitoring Zone window appears.

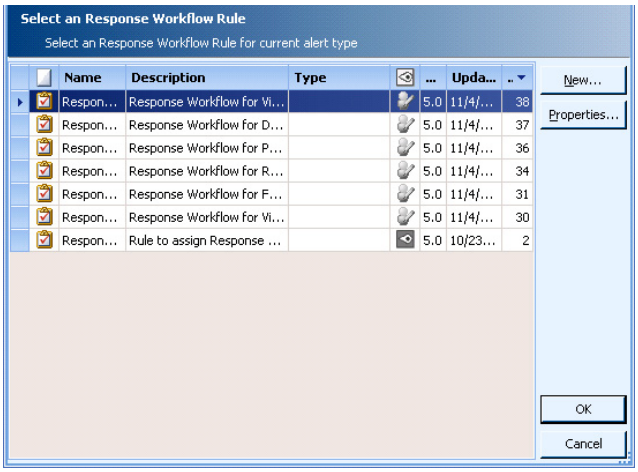


Step 6 Select the alert type(s) to which you want to apply a response workflow rule. You can use Ctrl and Shift keys to select multiple alert types, as shown next.



Step 7 Click **Add**.

The Select a Response Workflow Rule window appears.



Step 8 Select the response workflow rule you want to apply to the selected alert types.

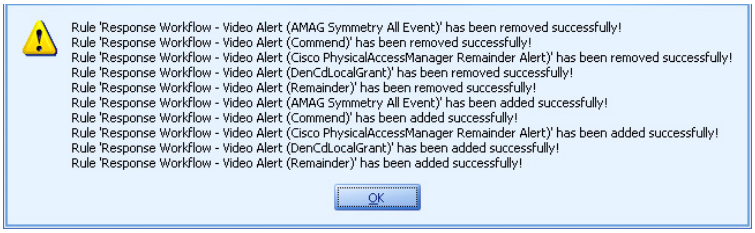
Note If you want to see the details for a response workflow rule, select it and click **Properties**. If you want to add a new response workflow rule, select the rule upon which you want to base your new rule and click **New**. The Add Response Workflow Rule window appears where you can set the properties of the new rule.

Step 9 Click **OK**.

The Apply Response Workflow Rules to Monitoring Zone window re-appears.

Step 10 Click **Apply**.

A confirmation dialog box appears.



Step 11 Click **OK**.

Enforcing Task Completion in the Operation Console

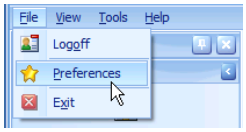
By default, operators must complete tasks designated as Alert Acknowledgeable or Alert Closeable before being able to acknowledge or close an alert. For example, if an operator tries to close an alert for which there are open tasks, an error message will appear.

If you want to disable this behavior, and allow operators to close alerts even though critical tasks have not been completed, you can set a preference in the Administration Console.

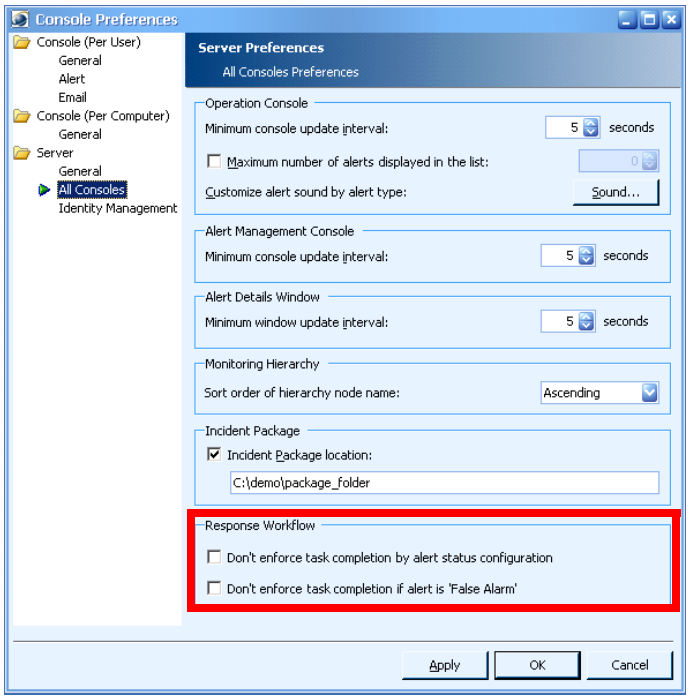
You can also choose not to enforce task completion for false alarms by setting a server preference.

To change behavior for response task completion:

Step 1 Select **File > Preferences**.



Step 2 Click **All Consoles** under **Server**.



Step 3 Check the **Don't enforce task completion by alert status configuration** option if you do not want to require users to complete Alert Acknowledgeable and Alert Closeable response tasks for open alerts.

Step 4 Check the **Don't enforce task completion if alert is 'False Alarm'** option if you do not want to require users to complete response tasks for false alarms.

Step 5 Click **OK**.

When the **Don't enforce task completion by alert status configuration** option is checked, the operator will receive an alert message when attempting to close an alert with outstanding response tasks. The operator will not, however, be prevented from closing the alert anyway.

CHAPTER 9

Managing Alert Collapsing Rules

You can set up an alert collapsing rule to determine when similar alerts should be grouped together.

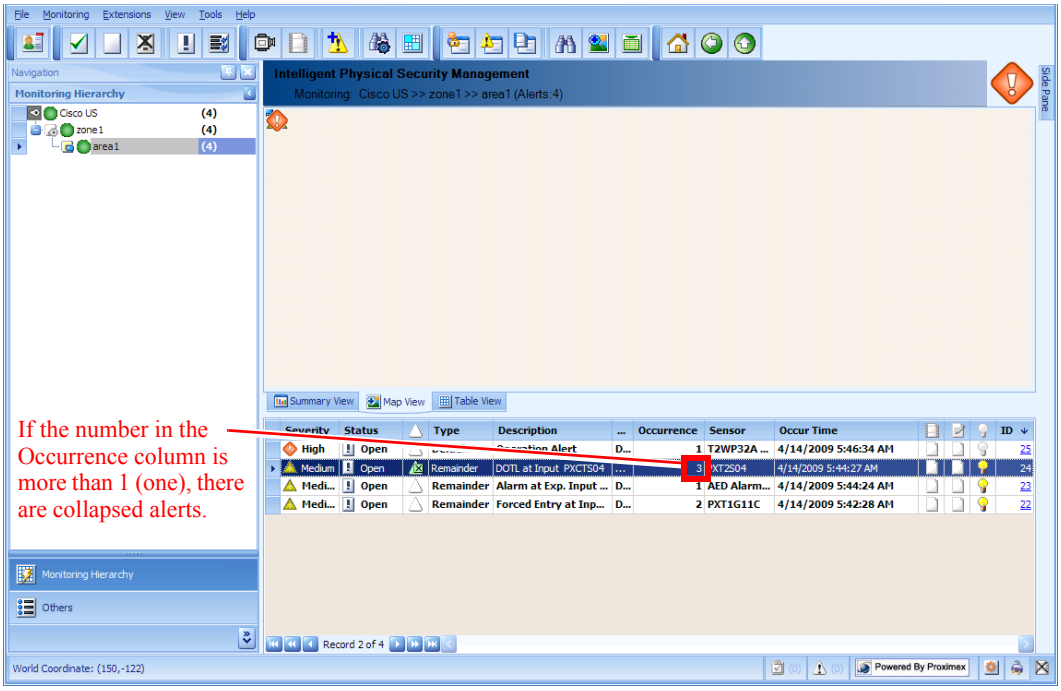
This chapter describes how to collapse similar alerts under a single listing in the Operation Console. It includes these topics:

- Collapsing Similar Alerts Under a Single Listing, page 9-1
- Adding an Alert Collapsing Rule, page 9-2
- Applying an Alert Collapsing Rule, page 9-5

Collapsing Similar Alerts Under a Single Listing

You can configure and apply an alert collapsing rule to reduce duplicate alerts and fold similar alerts under a single listing in the Operation Console.

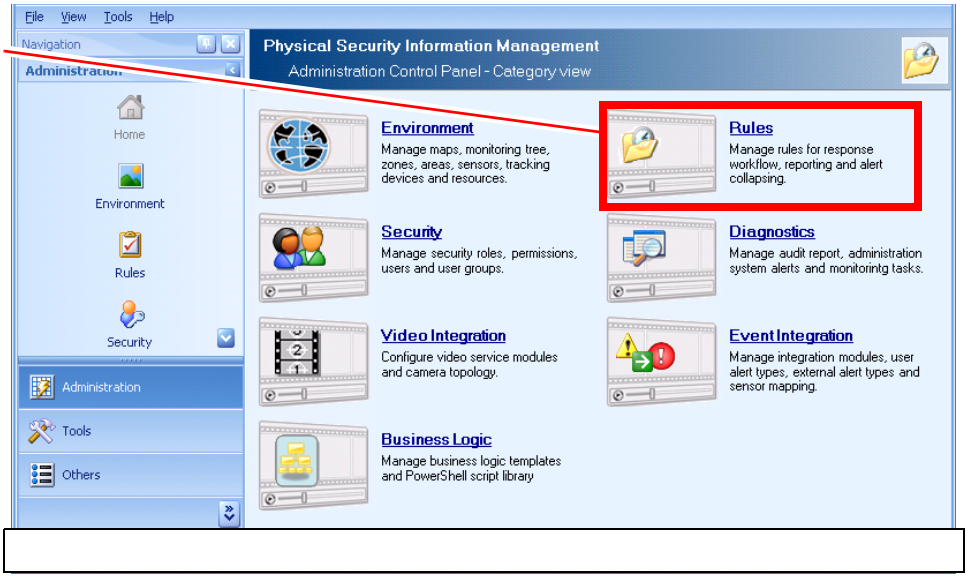
Collapsed alerts are consolidated under a single listing in the Alert List Pane of the Operation Console. The Occurrence column will show a number greater than 1 (one) in this case. To expand these listings, operators right-click the top-level listing and select **View Collapsed Alerts** from the menu.



Adding an Alert Collapsing Rule

To add an alert collapsing rule:

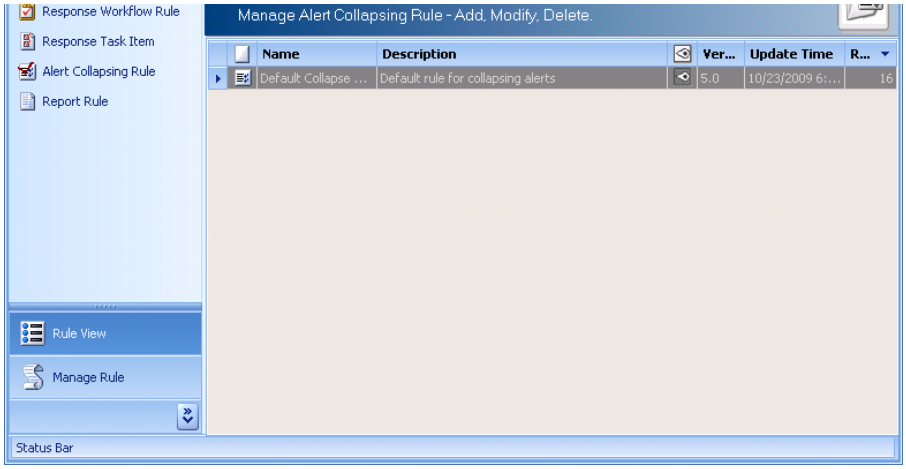
Step 1 Click the **Rules** icon in the Administration Console.



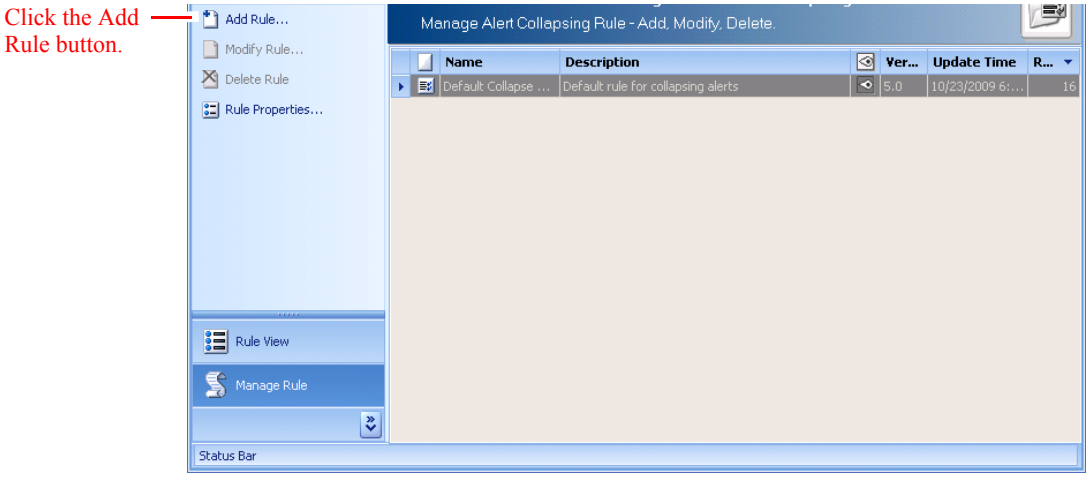
The Rules window appears.

Step 2 Click the **Alert Collapsing** icon in the Rules window.

The Alert Collapsing Rule window appears.



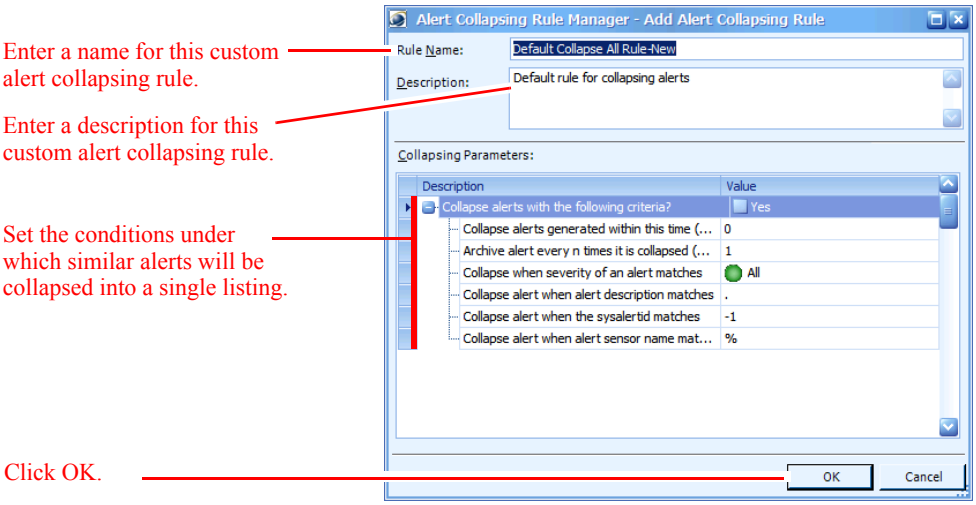
Step 3 Click **Manage Rule** (in the left navigation pane).



Step 4 Select the default alert collapsing rule you want to customize.

Step 5 Click **Add Rule** under **Manage Rule** (in the left navigation pane).

The Add Alert Collapsing Rule window appears.



Step 6 Enter a name for the custom alert collapsing rule in the **Rule Name** field.

Step 7 Enter a description for the custom rule in the **Description** field.

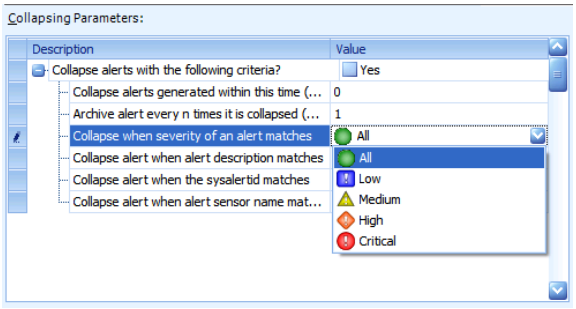
Step 8 Set conditions under which similar alerts will be collapsed into a single listing in the Collapsing Parameters area:

a. Click the **Yes** option next to **Collapse alerts with the following criteria?** to enable alert collapsing. If you deselect this option, alerts will not be collapsed.

b. Set the number of minutes after which similar alerts will be collapsed next to the **Collapse alerts generated within this time** field.

c. Determine when to archive alerts by setting the number of times the alert can be collapsed before it is archived next to the **Archive alert every n times it is collapsed** field.

d. Indicate the severity level that an alert must have to be collapsed by making a selection from the pulldown menu next to the **Collapse when severity of an alert matches** field.



e. Collapse alerts that have a certain alert description by entering the description keywords next to the **Collapse alert when alert description matches** field.

f. Collapse alerts that have a certain system alert ID by entering the sysalertid value next to the **Collapse alert when the sysalertid matches** field.

g. Collapse alerts that were generated by a certain alert sensor by entering the sensor name next to the **Collapse alert when alert sensor name matches** field.

All conditions must be true for alerts to be collapsed.

Step 9 Click **OK**.

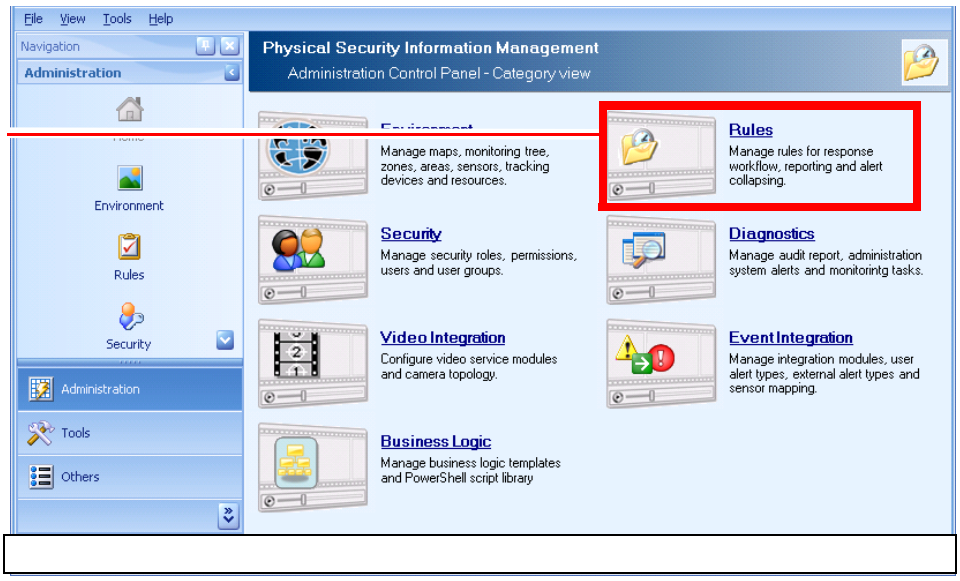
Your new alert collapsing rule appears in the PSOM Rule Manager.

Now you need to apply the alert collapsing rule to activate it for your environment.

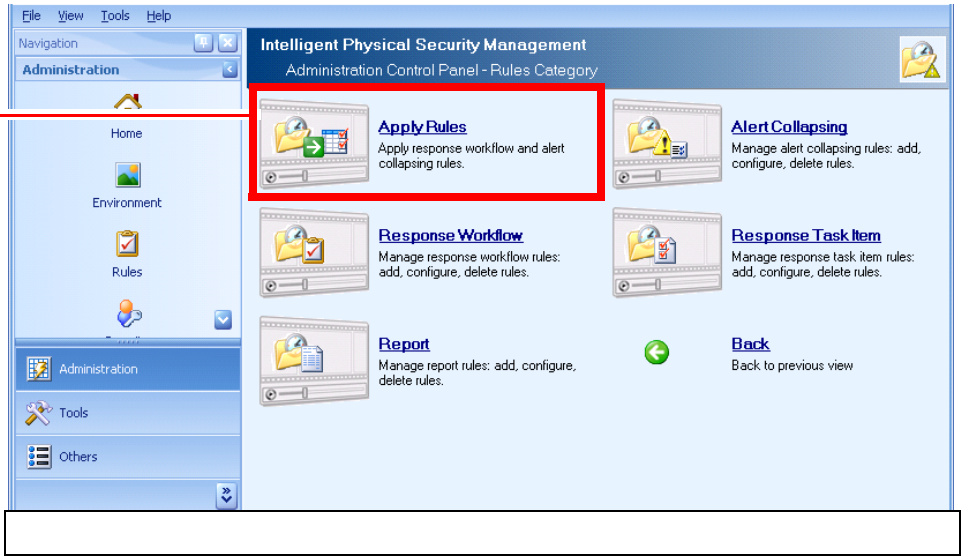
Applying an Alert Collapsing Rule

To apply an alert collapsing rule:

Step 1 Click the **Rules** icon in the Administration Console.



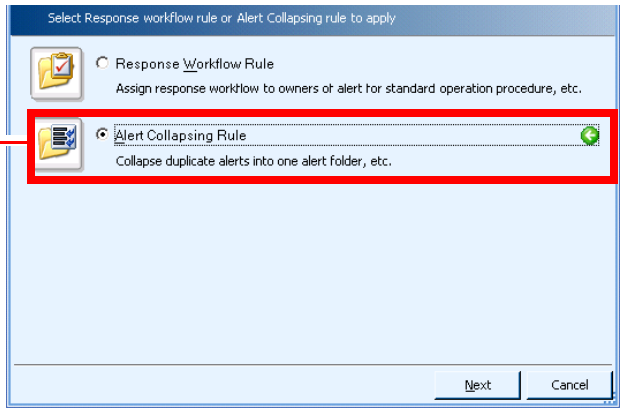
The Rules window appears.



Click the Apply Rules icon in the Rules window.

Step 2 Click the **Apply Rules** icon in the Rules window.

The Apply Rules window appears.

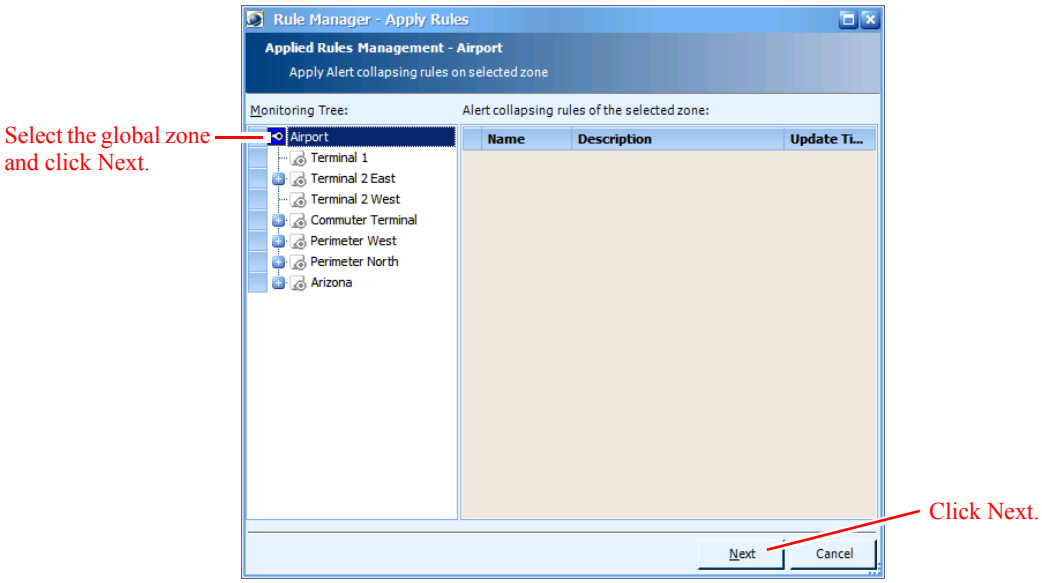


Click the Alert Collapsing icon in the Apply Rules window.

Step 3 Click the **Alert Collapsing Rule** icon in the Apply Rules window.

Step 4 Click **Next**.

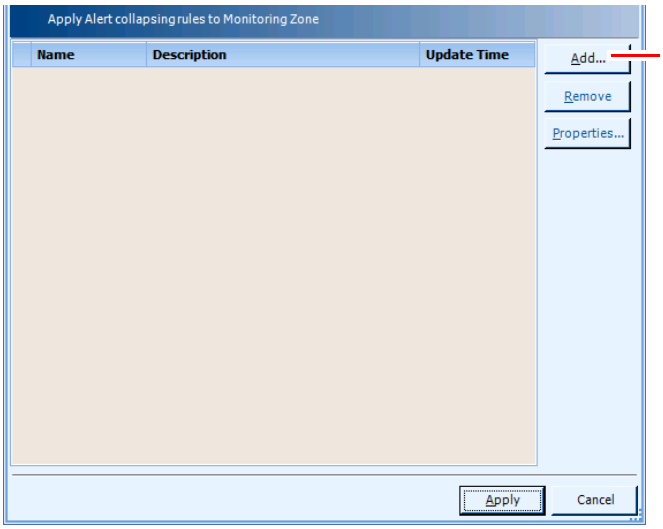
The Apply Rules window appears.



Step 5 Select the global zone and click **Next**.

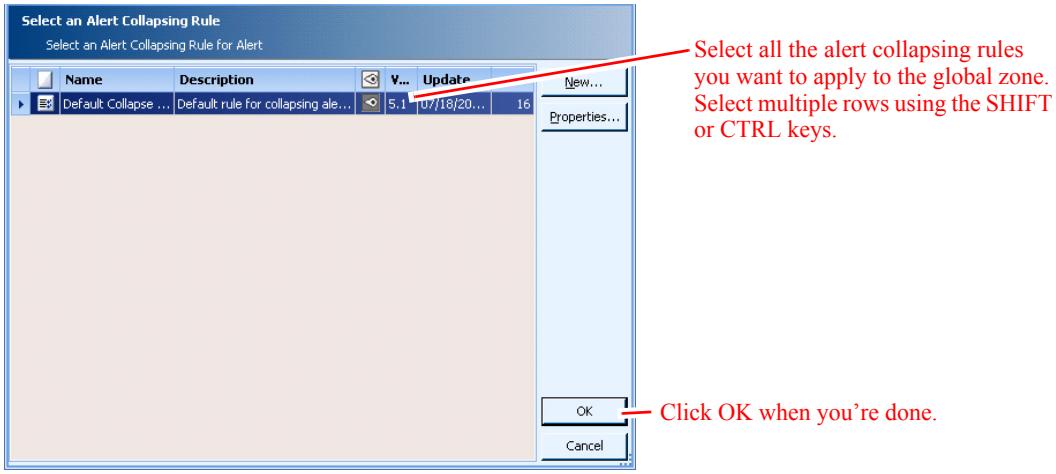
Note Alert collapsing rules can only be applied to the global zone (top node).

The Alert Collapsing Rule Manager window appears.



Step 6 Click the **Add** button.

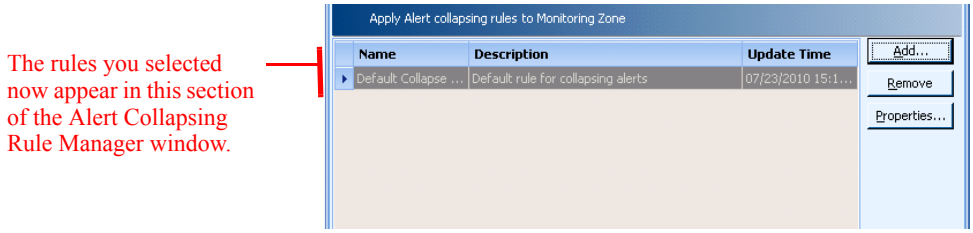
The Select an Alert Collapsing Rule window appears.



Step 7 Select the alert collapsing rules you want to apply.

Step 8 Click **OK**.

The rules you selected appear in the Alert Collapsing Rule Manager window.



Step 9 Click **Apply** to save your changes. The chosen alert collapsing rules will be applied to the global zone.

CHAPTER 10

Customizing Reports

Within the Operation Console, operators have a number of reports they can execute to monitor response times and other administrative functions. From the Administration Console, all of these reports can be customized.

This chapter covers:

- Types of default reports provided by PSOM
- How to customize a default report

This chapter includes these topics:

- Types of Default Reports, page 10-1
- Customizing a Report, page 10-2
- Modifying a Custom Report, page 10-8
- Deleting a Custom Report, page 10-9
- Setting a Default Directory for Incident Packages, page 10-10

Types of Default Reports

From the Operation Console, operators can run the default reports that Table 10-1 describes.

Table 10-1 Reports that Operators can Generate with the Report Wizard

Report	What it Tells You
Alert Count Daily Report	How many alerts occurred each day of the week for the specified time period. It includes information about the types and severity of alerts, as well as the locations of sensors that generated them.
Alert Count Hourly Report	How many alerts occurred each hour of the day for the specified time period. It includes information about the types and severity of alerts, as well as the locations of sensors that generated them.
Alert Detail Report	What alerts occurred during the specified time period. It includes details about the alerts including: severity, status, alert type, sensor, location, and occur time.
Alert Response Time By Alert Type Report	How long it took, on average, to respond to alerts. It shows the average response time for different alert types, alert severities, and zones/areas/sensors.

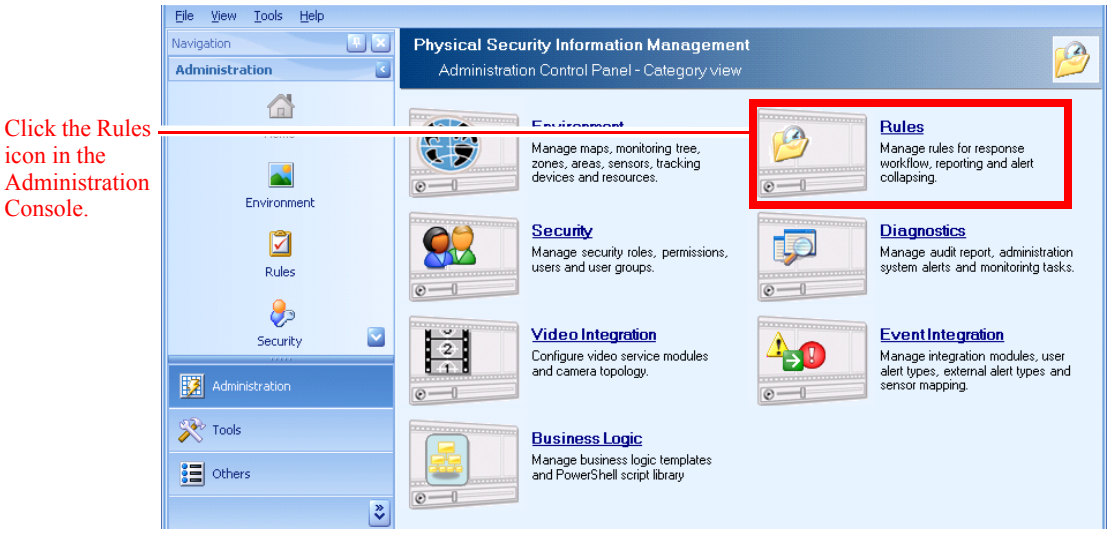
Table 10-1 Reports that Operators can Generate with the Report Wizard (continued)

Report	What it Tells You
Dispatch Incident Report	How long it took, on average, for alerts to be dispatched once they occur.
Operator Alert Count Report	How many alerts each operator closed.
Operator Alert Response Time Report	How long it took for different operators to respond to alerts.
Operator End of Shift Report	How many alerts were handled by a specific operator during a shift.
Top X Alert Response Time Report	How long, on average, it took to respond to different alert types. Data is sorted by alert counts, in ascending order.
Top X Alerts By Alert Type Report	How many alerts occurred, by alert type, including a list of all sensors that raised each alert type.
Top X Alerts By Area Report	How many alerts occurred in each monitoring area.
Top X Alerts By Sensor Report	How many alerts were raised by each sensor.
Top X False Alerts By Sensor Report	How many false alerts were raised by each sensor.
Top X Simulated Alerts By Sensor Report	How many simulated alerts were raised by each sensor.

Customizing a Report

To customize a report:

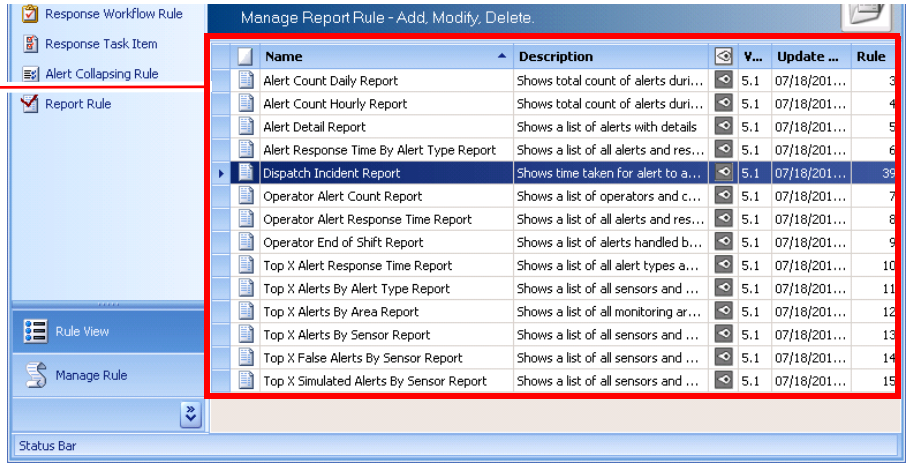
Step 1 Click the **Rules** icon in the Administration Console.



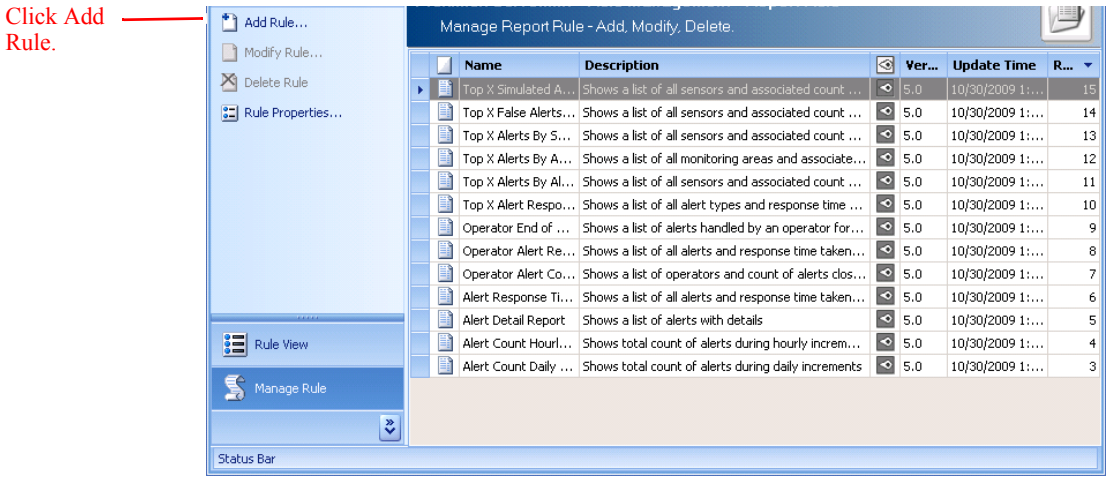
The **Rules** window appears.

Step 2 Click the **Report** icon in the Rules window.

The Report Rule window appears.



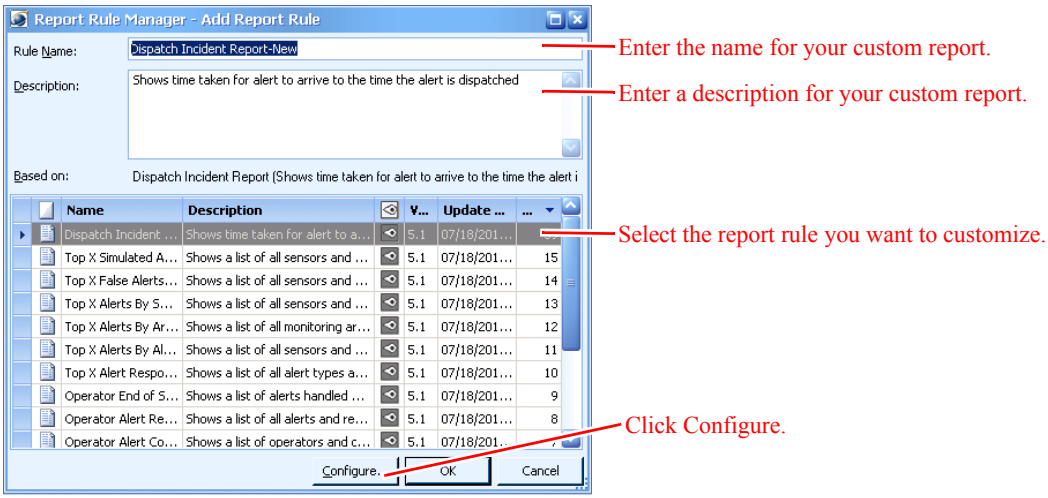
Step 3 Click **Manage Rule** in the left navigation bar.



Step 4 Select the default report that you want to customize.

Click **Add Rule** under Manage Rule in the left pane.

The Add Report Rule window appears.



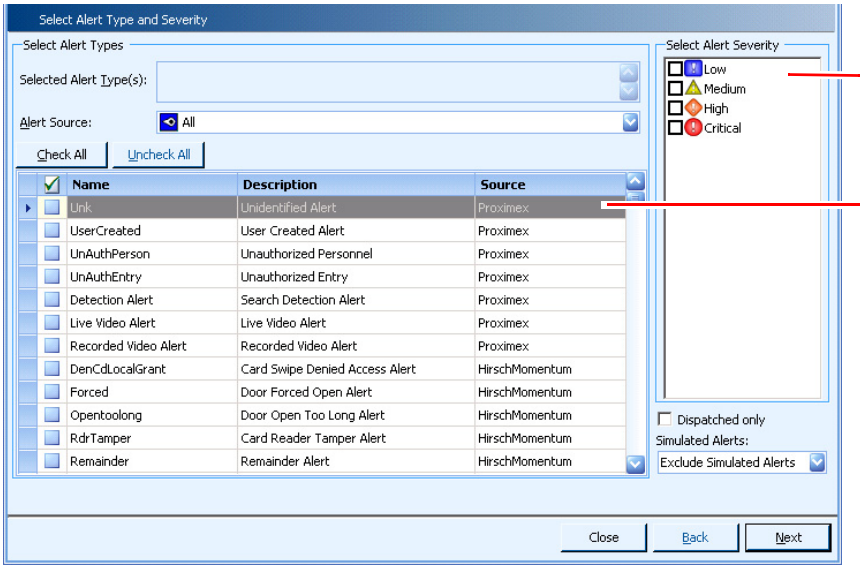
Step 5 In the **Rule Name** field, enter a name for the custom report.

Step 6 In the **Description** field, enter information about the custom report.

Step 7 Select the report rule on which you want to base this custom report.

Step 8 Click **Configure**.

The Alert Type and Severity window appears.



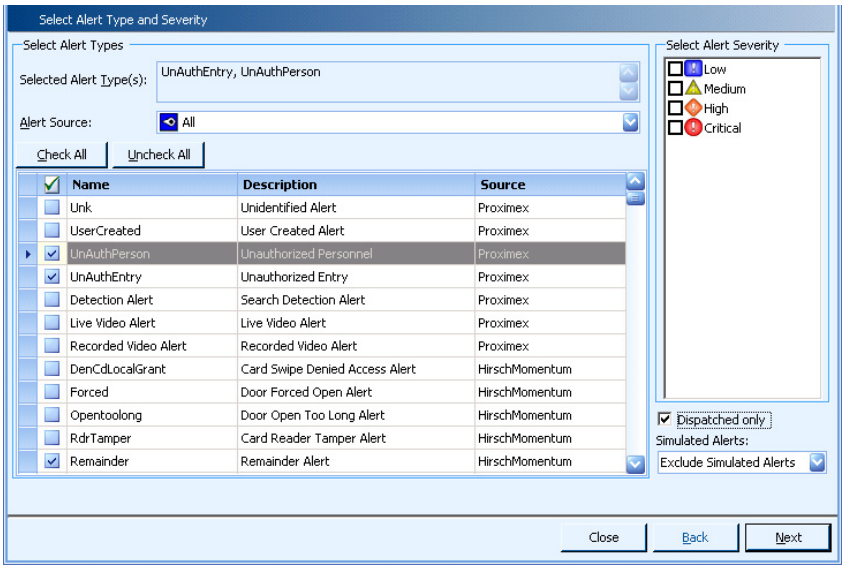
Step 9 Check the boxes for all alert types you want included in this custom report.

Step 10 If you want this report to show data for alerts that have been dispatched, check the **Dispatched only** option.

Step 11 If you do not want this report to show data for simulated alerts, select **Exclude Simulated Alerts** from the **Simulated Alerts** field.

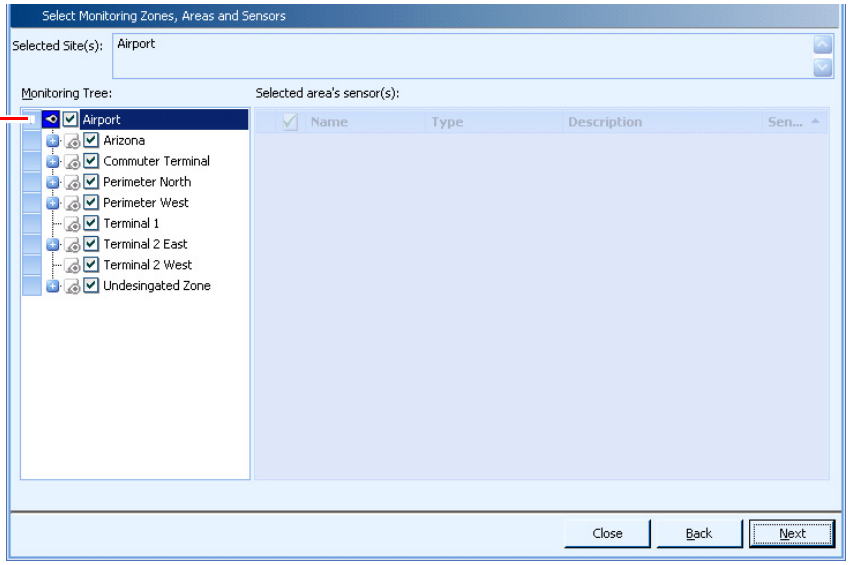
Step 12 Check the boxes for all severity levels you want included in this custom report.

The Alert Type and Severity window might appear similar to the following.



Step 13 Click **Next**.

The Zone, Area and Sensors window appears.

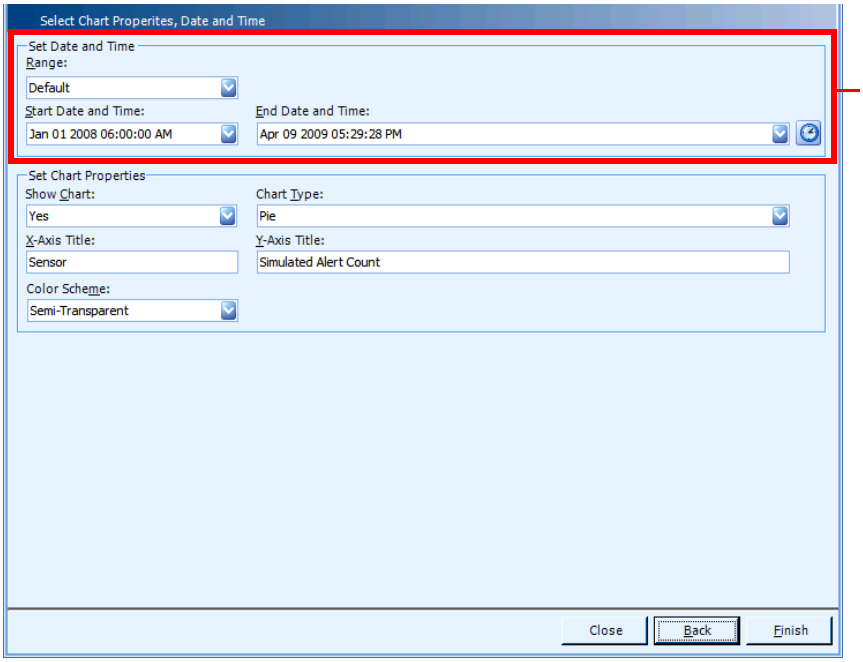


Check all monitoring zones, areas and sensors that should be included in the custom report.

Step 14 Select all monitoring zones, monitoring areas, and sensors that should be included in this custom report.

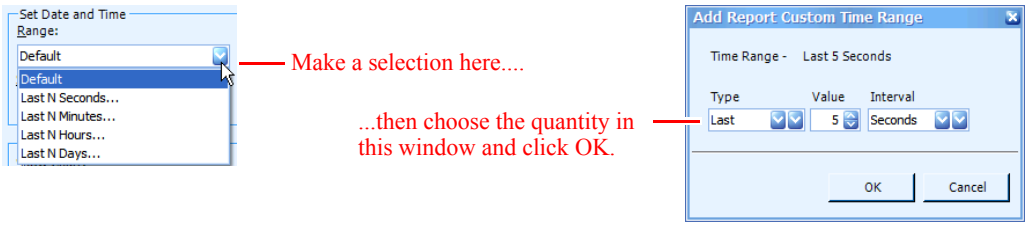
Step 15 Click **Next**.

The Chart Properties, Date and Time window appears.



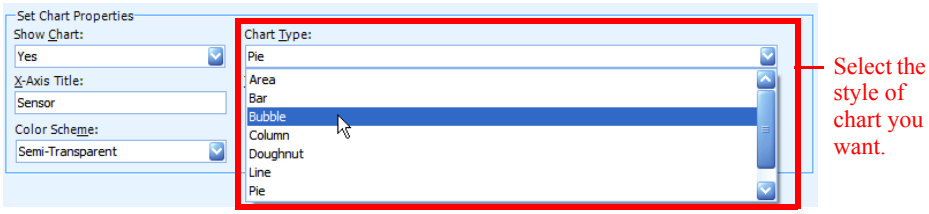
Select the date/time range for reporting.

Step 16 Select the period for which you want to do reporting in the Set Date and Time area. You can specify a starting and ending point for reporting using the **Start Date and Time** and **End Date and Time** fields. Or you can make a different selection from the **Range** field, as shown next.



As shown, you can generate a report for the last *N* days, hours, minutes or seconds. When you make a selection from the **Range** field, a new window appears where you can specify the number of days, hours, minutes or seconds for reporting.

Step 17 Next specify the types of charts you want displayed in the report using fields in the **Set Chart Properties** field.



Choose whether to display a chart in the **Show Chart** field.

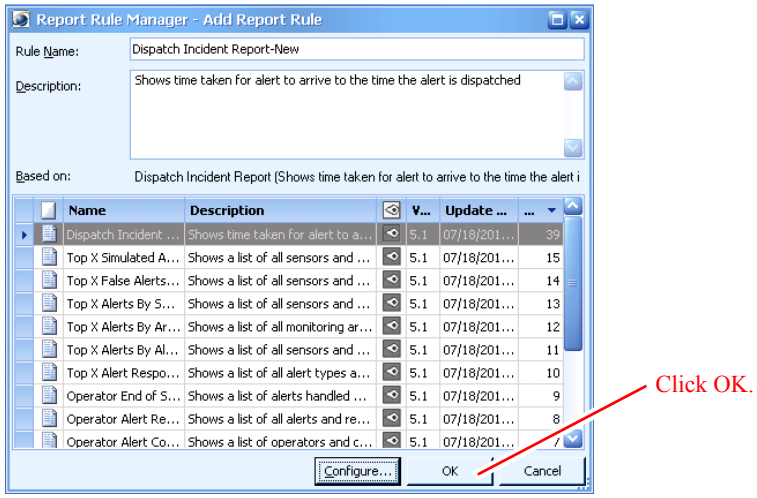
a. If you choose to display a chart, select what kind of chart you want from the **Chart Type** field.

b. Enter titles for the x-axis and y-axis in the **X-Axis Title** and **Y-Axis Title** fields.

c. Choose a color scheme for the chart from the **Color Scheme** field.

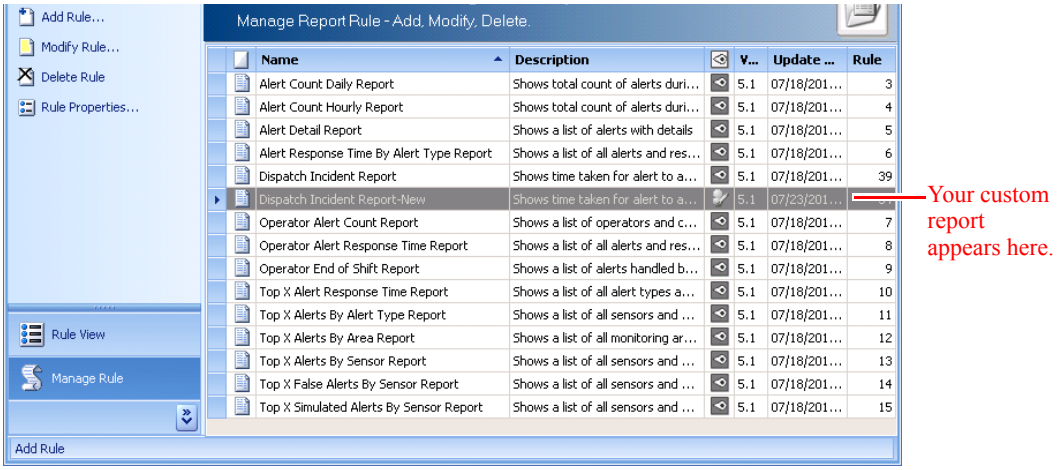
Step 18 Click **Finish**.

The Add Report Rule window reappears.



Step 19 Click **OK** to save the custom report.

Your new report appears in the Report Rule window.



Operators will now be able to select and run this report from Report Manager in the Operation Console.

Modifying a Custom Report

You cannot modify a default report, but you can modify any customized report using the Administration Console.

To modify a custom report:

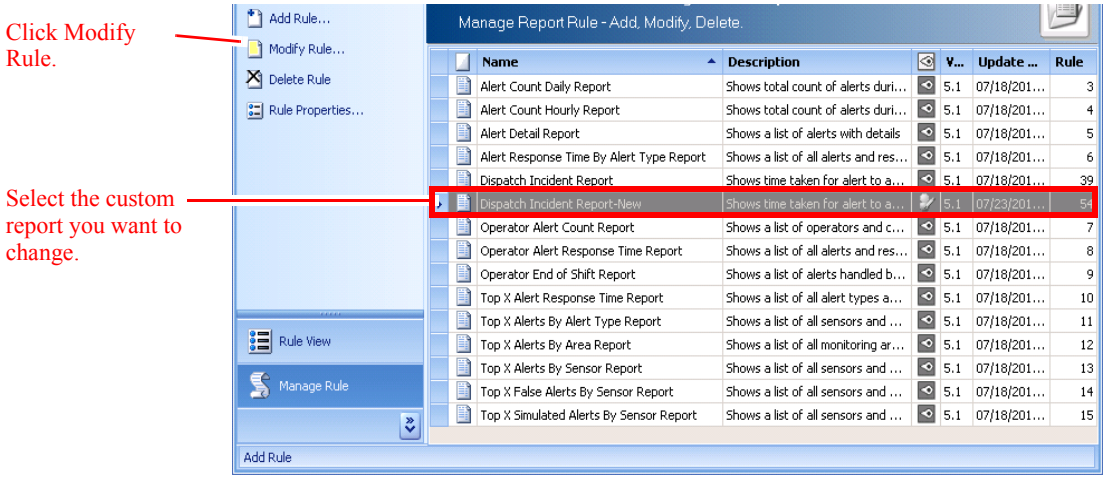
Step 1 Click the **Rules** icon in the Administration Console.

The Rules window appears.

Step 2 Click the **Report** icon in the Rules window.

The Report Rule window appears.

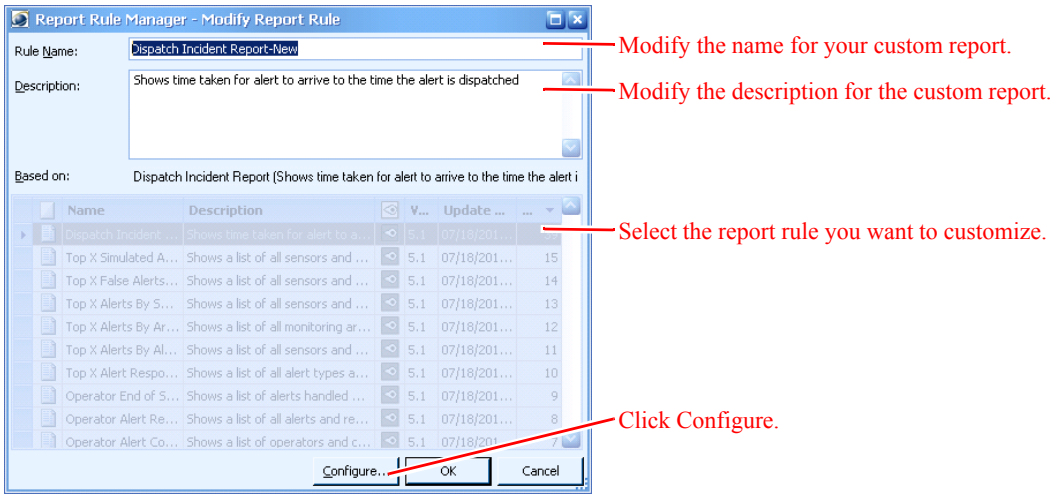
Step 3 Click **Manage Rule** in the left navigation bar.



Step 4 Select the custom report that you want to modify.

Step 5 Click **Modify Rule** under Manage Rule in the left pane.

The Modify Report Rule window appears.



Step 6 Follow the instructions in the "Customizing a Report" section on page 10-2 to reconfigure the report rule for the custom report.

Step 7 Click **OK** to save the modified custom report.

Deleting a Custom Report

You cannot remove default report rules, but you can delete a custom report rule.

To delete a custom report:

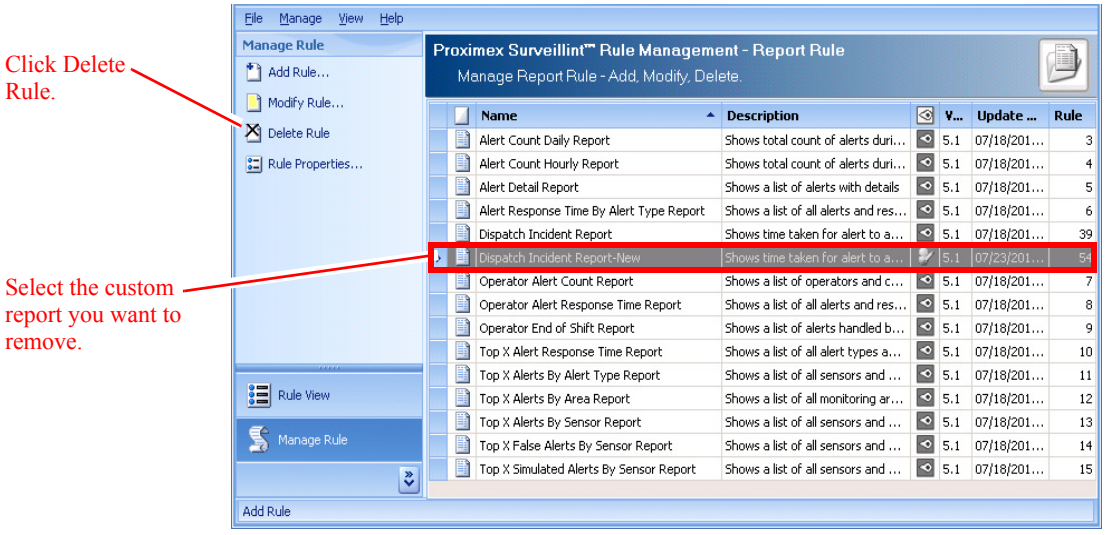
Step 1 Click the **Rules** icon in the Administration Console.

The Rules window appears.

Step 2 Click the **Report** icon in the Rules window.

The Report Rule window appears.

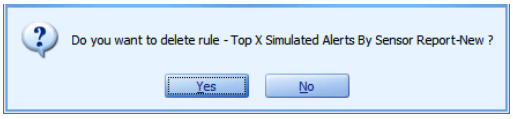
Step 3 Click **Manage Rule** in the left navigation bar.



Step 4 Select the custom report that you want to remove.

Step 5 Click **Delete Rule** under Manage Rule in the left pane.

A confirmation dialog box appears.



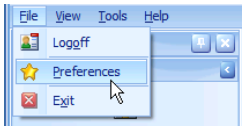
Step 6 Click **Yes** to remove the selected custom report.

Setting a Default Directory for Incident Packages

You can set a default directory where Incident Packages are stored for all users when they export alert incident packages. Users won't be able to browse to their own folder under export incident package dialog box if this option is enabled.

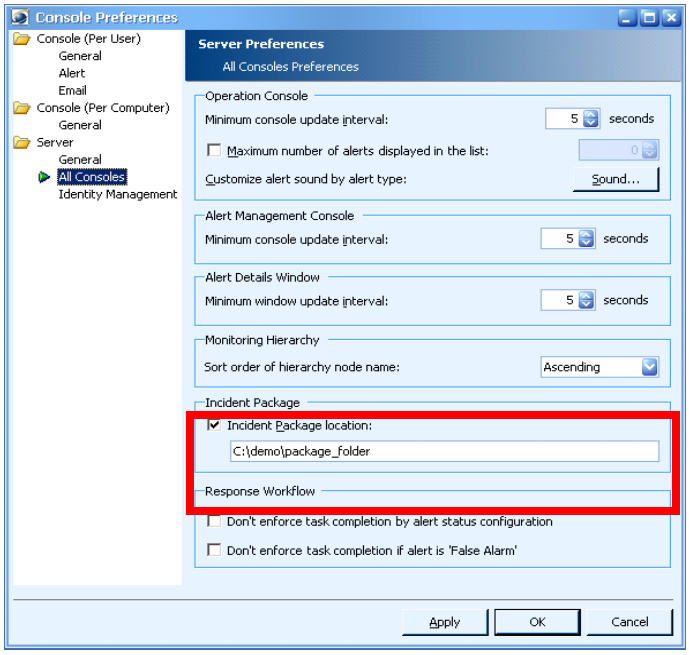
To set a default directory for Incident Packages:

Select **File > Preferences**.



Step 7 Click **All Consoles** under **Server**.

Step 8 Check the **Incident Package location** option and provide a path to a shared directory where incident packages will be stored for all users.



Step 9 Click **OK**.

CHAPTER 11

Integrating Sensors with External Systems, Registering Third-Party Alarm Types, and Configuring Integration Modules

To synchronize information between external intrusion detection systems and PSOM, you must define sensor mappings that correlate sensor names between the systems. PSOM also allows you to register alarm types from third-party systems, define your own alarm types, and configure access to external systems with Integration Modules.

This chapter explains:

- How information is synchronized between PSOM and external intrusion detection systems using sensor mappings.
- How to create a new sensor mapping.
- How to edit or delete a sensor mapping.
- How to register a third-party alarm type.
- How to create a custom alert type.
- How to begin configuration of Integration Modules.

This chapter includes these topics:

- Overview of Sensor Mappings, page 11-1
- Mapping a Sensor, page 11-2
- Editing or Deleting a Sensor Mapping, page 11-5
- Registering Third-Party Alarms, page 11-6
- Editing or Deleting a Registered Alert Type, page 11-10
- Creating a Custom Alert Type, page 11-12
- Creating a System Alert Type, page 11-15
- Configuring Integration Modules for External Systems Integration, page 11-16

Overview of Sensor Mappings

A *sensor mapping* within PSOM is a two-way event connector that synchronizes information in PSOM with information in external intrusion detection systems. The sensor mapping works by correlating the sensor names in PSOM with the names for the same devices within the external system.

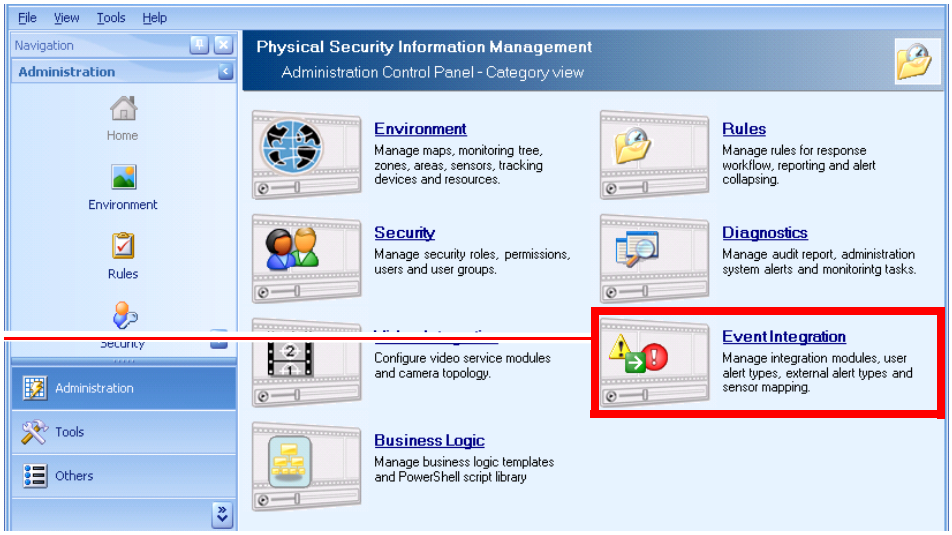
Using sensor mapping enables PSOM to raise alerts in the appropriate sensor when an event occurs with the actual sensor device. Without this mapping, PSOM raises alerts in a miscellaneous zone called “Zone Unassigned...”, and in a miscellaneous area called “Area Unassigned...”, in the alert list view. However, if PSOM can locate the sensor in a sensor mapping, it raises the alert from the matched sensor. To obtain video for an event, PSOM uses the camera sensor that is a member of the group to which this sensor belongs.

Sensor mapping also has benefits for the external intrusion detection system. Using sensor mappings enables the alerts of external systems to contain URL links to video clips and snapshot images, which are generated by PSOM. Also, PSOM is able to enrich Vident alerts with information about the last access attempts for an access control device (if this information is available).

Mapping a Sensor

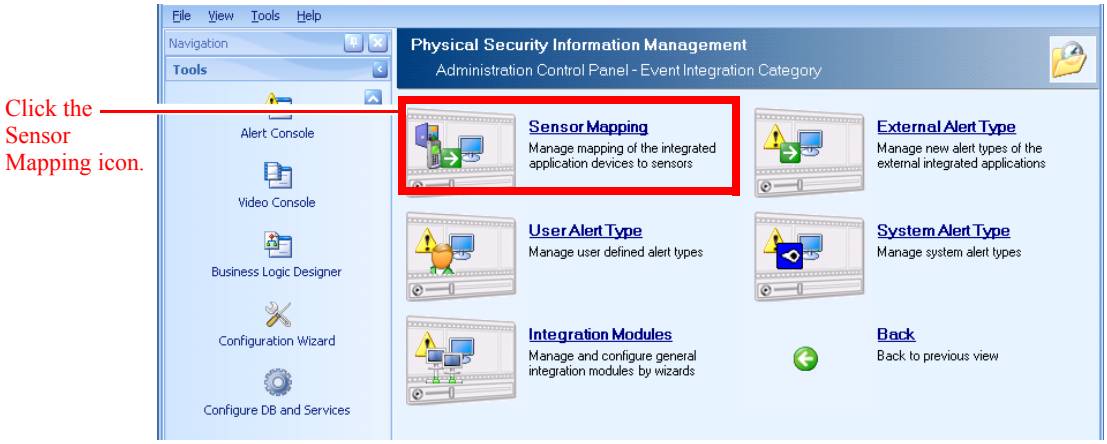
To create a new sensor mapping:

Step 1 Click the **Event Integration** icon in the Administration Console.

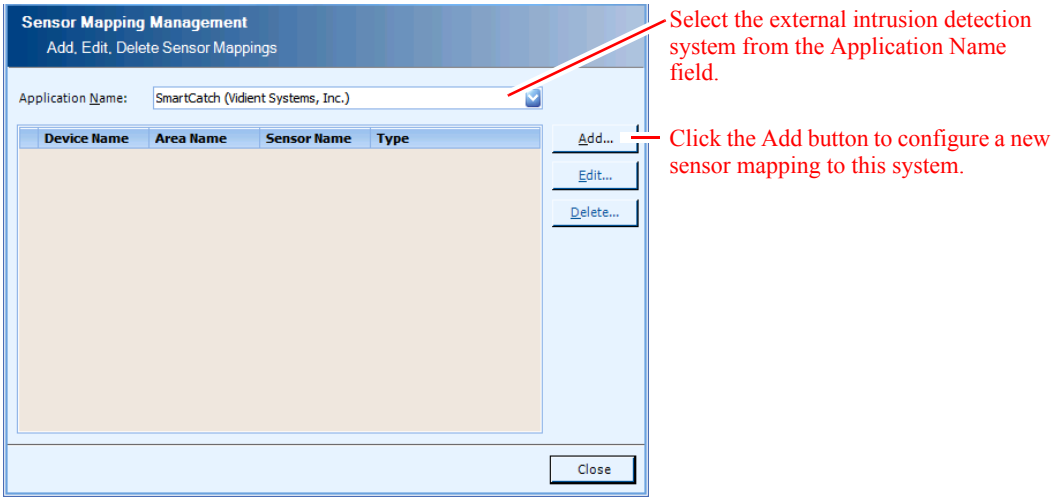


Click the Event Integration icon.

Step 2 Click the **Sensor Mapping** icon in the Administration Console.



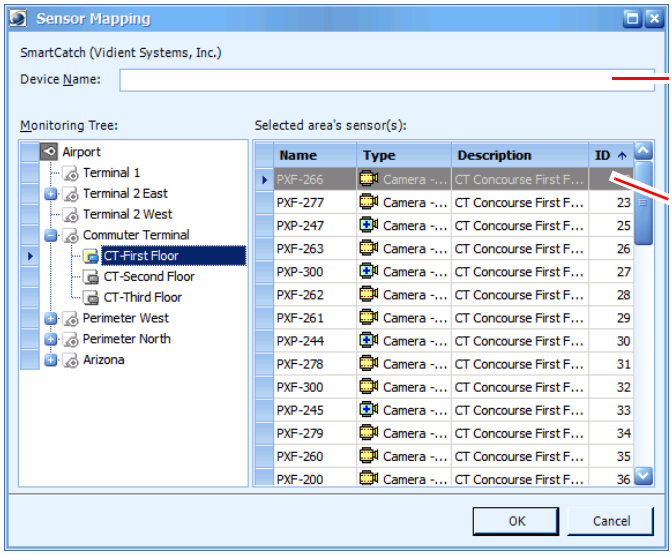
The PSOM Sensor Mapping Manager window appears.



Step 3 From the **Application Name** field, select the external intrusion detection system for which you want to configure sensor mapping.

Step 4 Click the **Add** button to configure a new sensor mapping.

The Sensor Mapping window appears.



Enter the name of the sensor device as it is listed in the external intrusion detection system.

Select the sensor in PSOM that should be mapped to the sensor device in the external system.

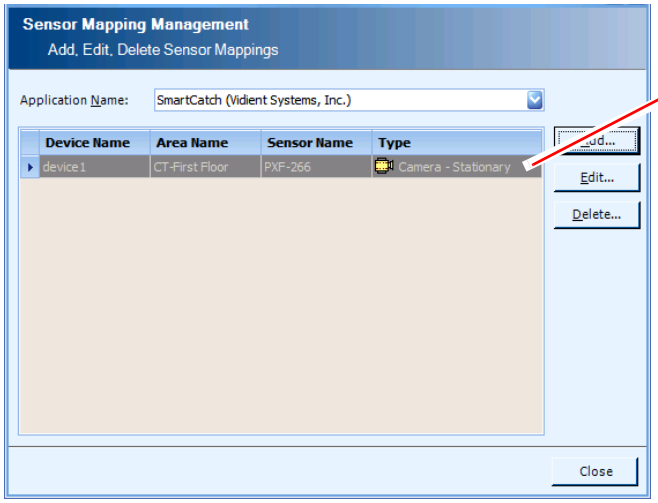
Step 5 In the **Device Name** field, enter the name assigned to a sensor device in the external intrusion detection system. This name must *exactly match* the name for the sensor device in the external system.

Step 6 In the Monitoring Tree area, select the monitoring area within PSOM where the corresponding sensor is located.

Step 7 In the sensors list, select the sensor name with which the external sensor device should be correlated.

Step 8 Click **OK** to save the mapping.

The new mapping appears in the Sensor Mapping Manager window.



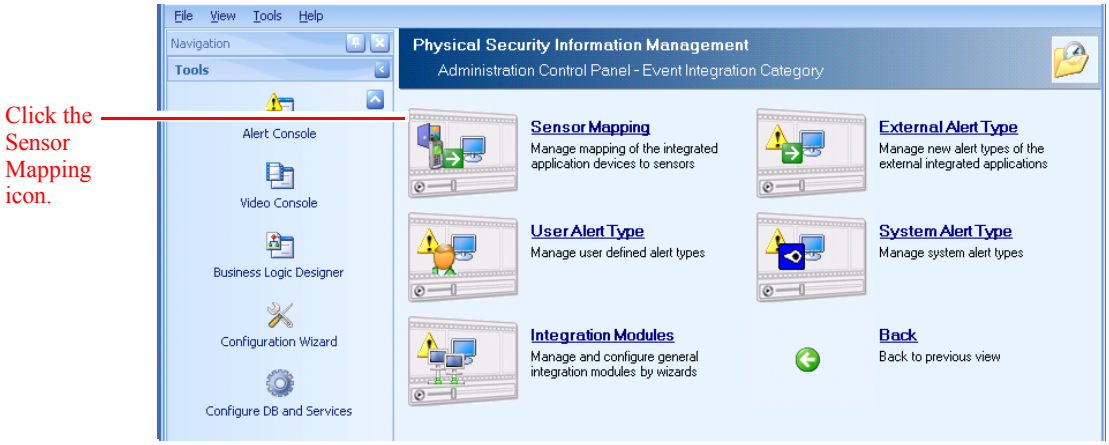
The new mapping appears in the list of sensor mappings.

Editing or Deleting a Sensor Mapping

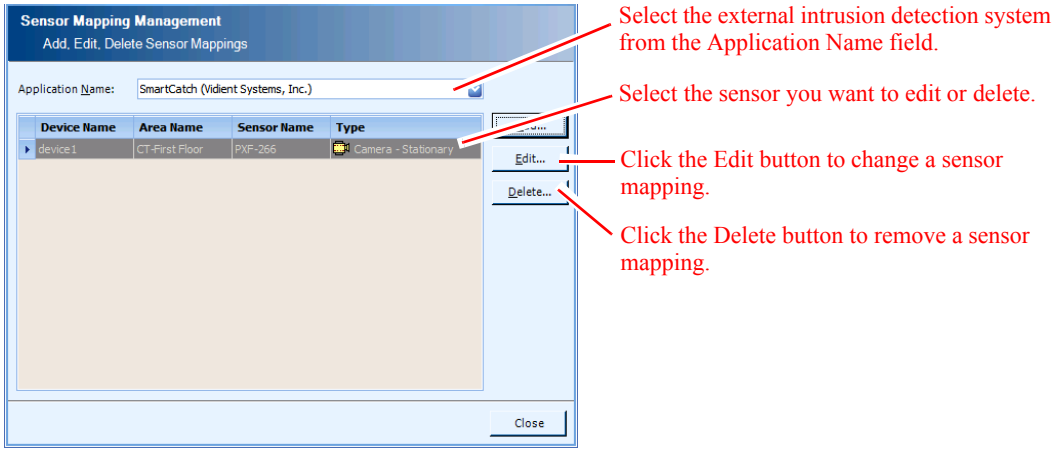
To edit or delete a sensor mapping:

Step 1 Click the **Event Integration** icon in the Administration Console.

Step 2 Click the **Sensor Mapping** icon in the Administration Console.



The PSOM Sensor Mapping Manager window appears.



Step 3 From the **Application Name** field, select the external intrusion detection system for which you want to edit or remove a sensor mapping.

Step 4 Select the sensor mapping you want to edit or delete from the list of mappings.

To edit a sensor mapping:

Step 1 Click the **Edit** button.

The Sensor Mapping window appears.

a. Change the name in the **Device Name** field if necessary.

b. Select a new sensor from the list if necessary

c. Click **OK**.

Step 2 To remove a sensor mapping:

a. Click the **Delete** button.

A confirmation dialog box appears.

b. Click **Yes** to proceed with the deletion.

Step 3 Click **Close** to close the Sensor Mapping window.

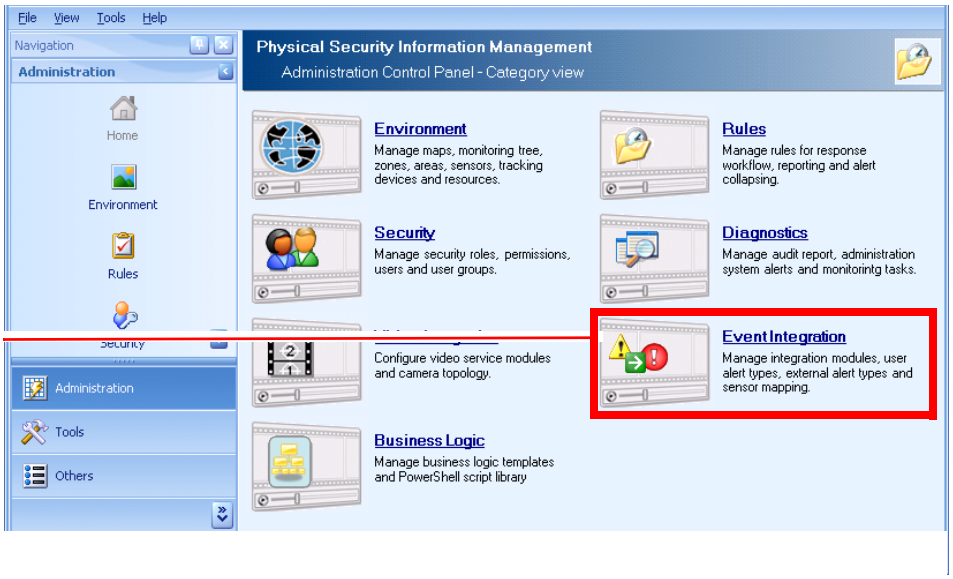
Registering Third-Party Alarms

To allow better integration with third-party alarm sources (for example for tracking, assigning alert tasks or default severity levels), you can register these external alarm types with PSOM.

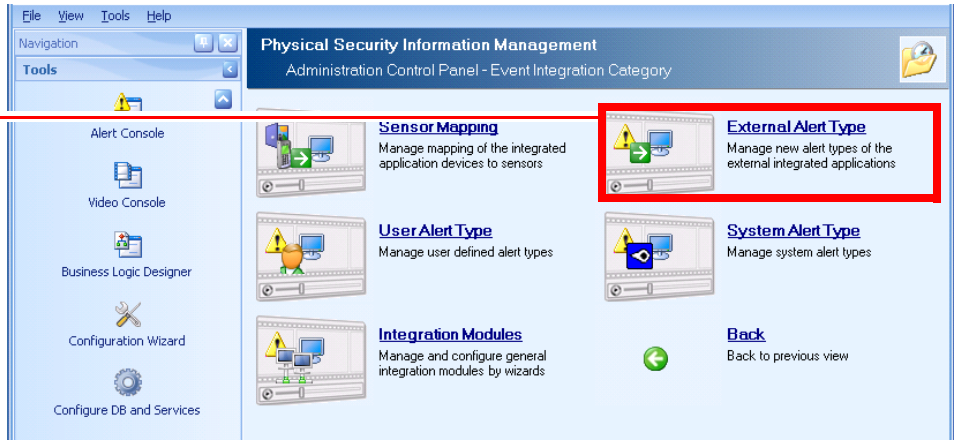
Note If you do not register specific third-party alarms, PSOM will create one alarm type per external alert source. For example, PSOM will create a single default alarm type for both a Tailgating and Duress alarm if you do not register each of these third-party alarms separately; in this situation, the same alert task and escalation must be applied to these different third-party alarms because PSOM views them as a single type of alarm.

To register a third-party alarm type:

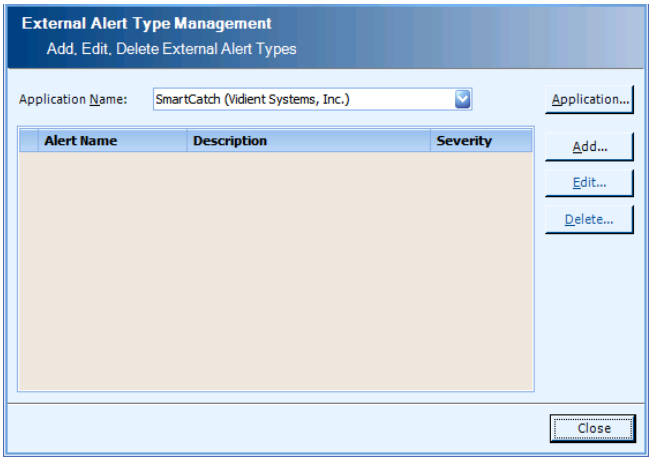
Step 1 Click the **Event Integration** icon in the Administration Console.



Step 2 Click the **External Alert Type** icon in the Administration Console.



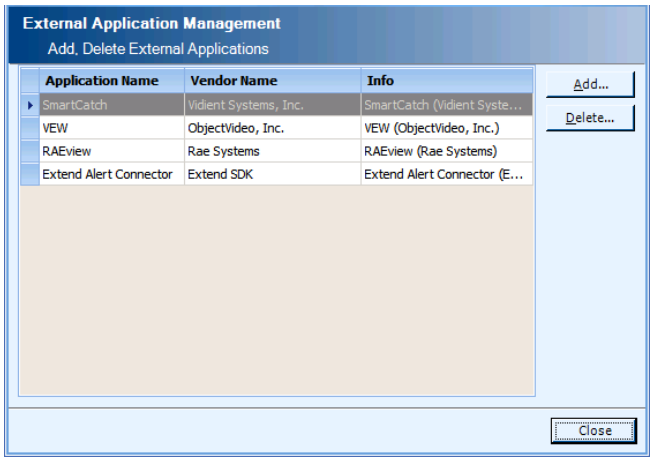
The PSOM External Alert Type Manager window appears.



Step 3 From the **Application Name** field, select the external intrusion detection system for which you want to register external alert types.

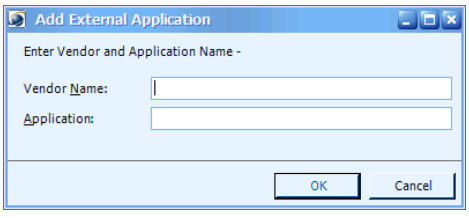
a. If you do not see the application you want, click the **Application** button.

The External Application Management window appears.



b. Click the **Add** button.

The Add External Application window appears.



c. In the **Vendor Name** field, enter the name of the company that develops the application.

d. In the **Application** field, enter the name of the external application.

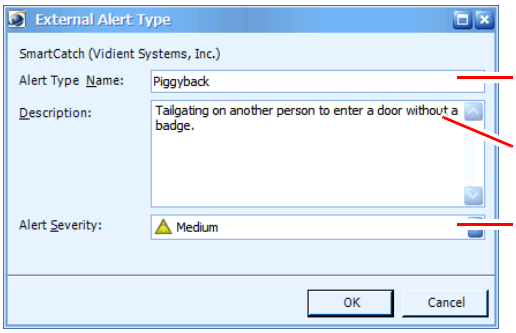
Note The values in the **Vendor Name** and **Application** fields must match what is defined in the XML used to send the command from the Event Integration SDK.

Step 4 Click **OK**.

Step 5 Click **Close**.

Step 6 Click the **Add** button to register a new external alert type.

The External Alert Type window appears.



Step 7 Enter information about this alert type you want to register:

a. In the **Alert Type Name** field, enter the name of the external alert type you want to register with PSOM.

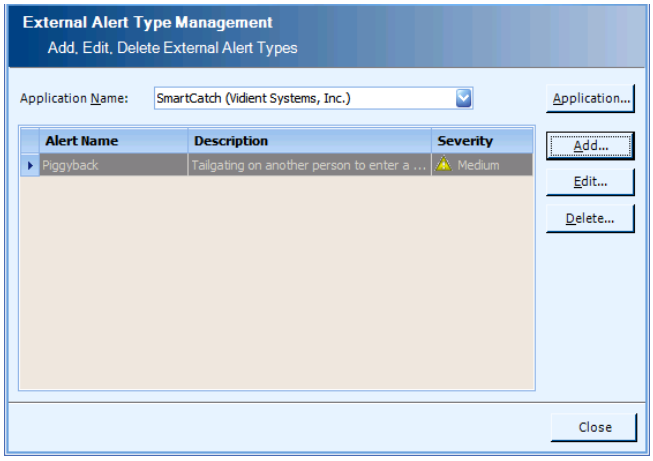
Note You need to enter the alert type that is specified in the EventInfo.Type node in the EventInfo document that is sent to PSOM at event creation. In other words, locate the value contained in the EventInfo parameter of the CreateGeneralEvent() call. If the value entered in the Alert Type Name field does not exactly match the EventInfo.Type value, PSOM will generate a default alarm type for the 3rd party system.

b. In the **Description** field, provide a description of this alert type.

c. From the **Alert Severity** field, select the level of importance to assign to this alert type.

d. Click **OK**.

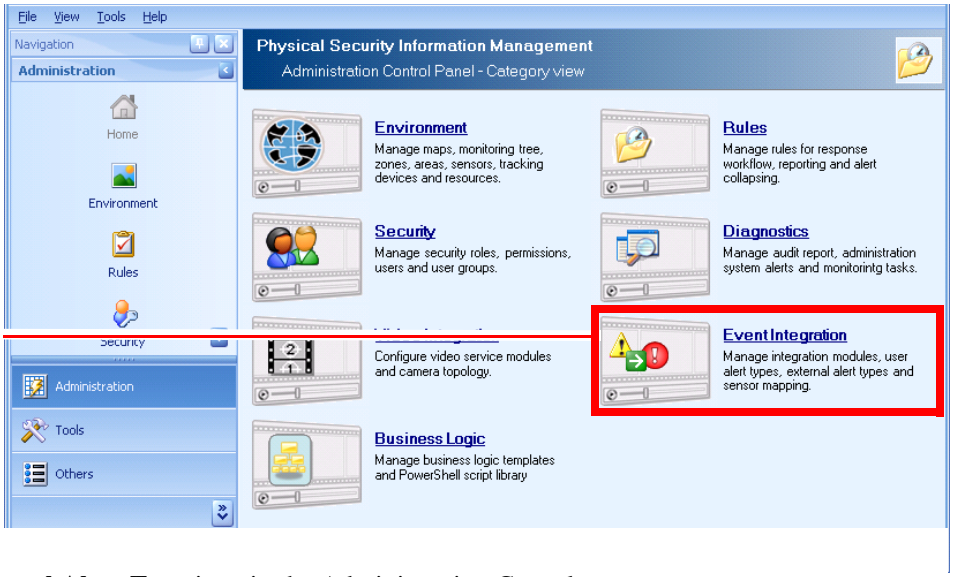
The PSOM External Alert Type Manager window shows the new registered alert type.



Editing or Deleting a Registered Alert Type

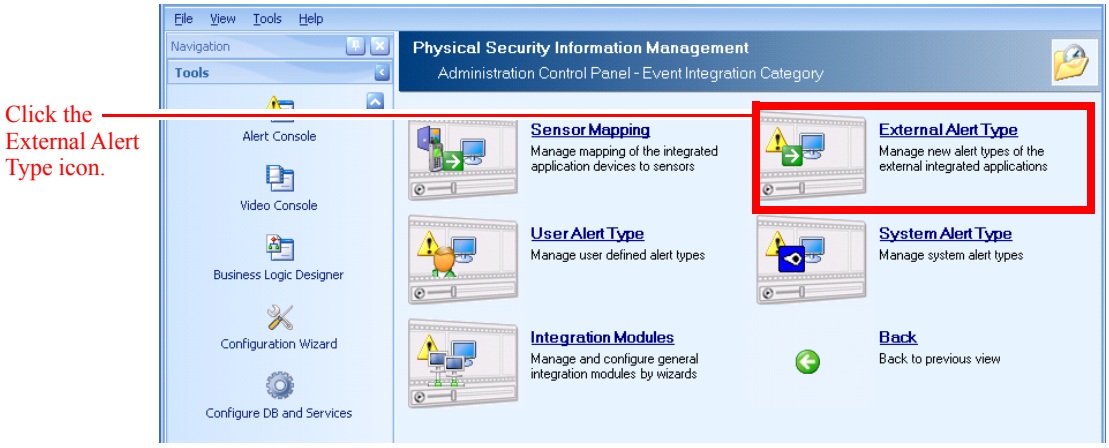
To edit or delete a registered alert type:

Step 1 Click the **Event Integration** icon in the Administration Console.

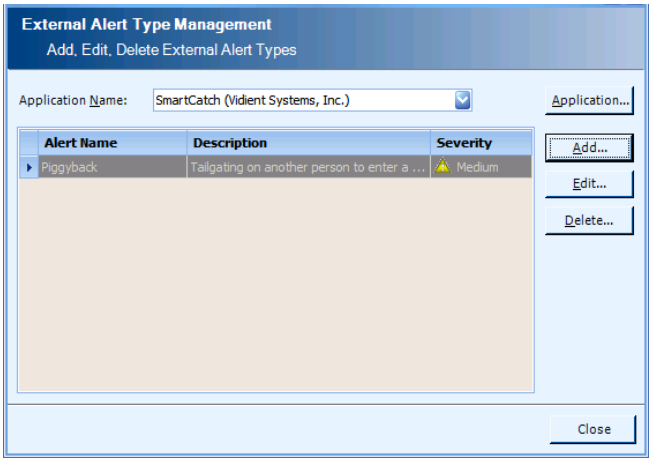


Click the Event Integration icon.

Step 2 Click the **External Alert Type** icon in the Administration Console.



The PSOM External Alert Type Manager window appears.



Step 3 From the **Application Name** field, select the external intrusion detection system for which you want to edit or remove a registered alert type.

Step 4 Select the registered alert type you want to edit or delete from the list.

Step 5 To edit a registered alert type:

a. Click the **Edit** button. The External Alert Type window appears.

b. Change the name in the **Alert Type Name** field if necessary.

c. Select a new severity from the **Alert Severity** field if necessary

d. Click **OK**.

Step 6 To remove a registered alert type:

a. Click the **Delete** button. A confirmation dialog box appears.

b. Click **Yes** to proceed with the deletion.

Step 7 Click **Close** to close the External Alert Type Manager window.

Creating a Custom Alert Type

You can create a custom alert type to handle task-oriented types of alerts such as reminding operators to check video cameras periodically.

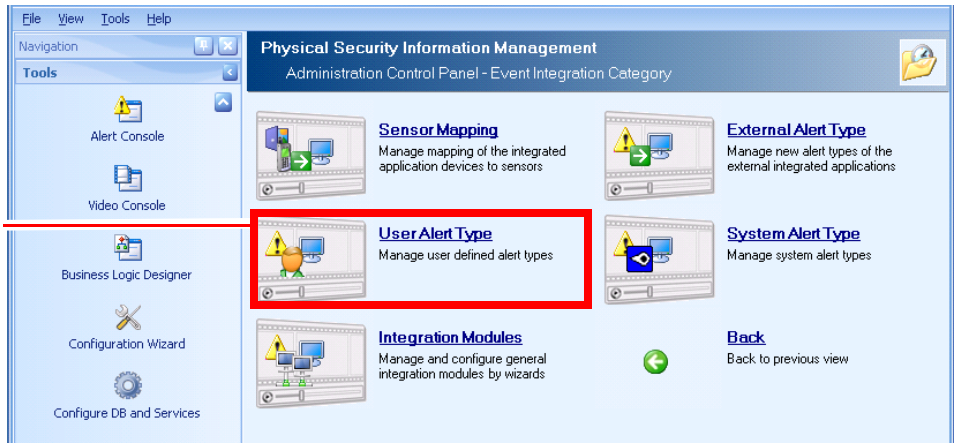
To create a custom alert type:

Step 1 Click the **Event Integration** icon in the Administration Console.

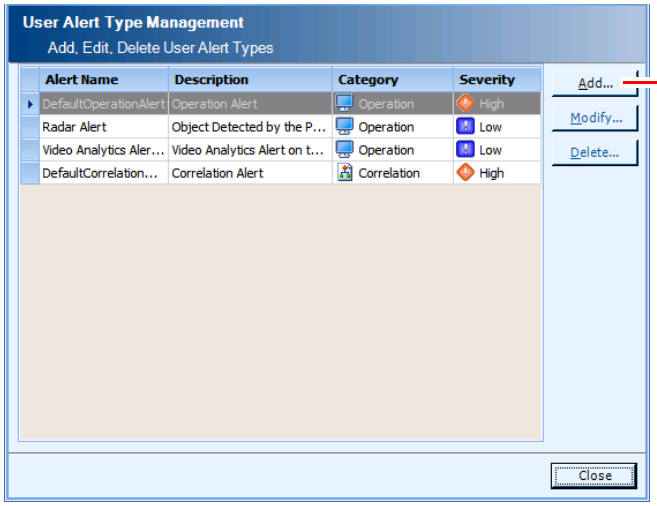
Click the Event Integration icon.

Step 2 Click the **User Alert Type** icon in the Administration Console.

Click the User Alert Type icon.

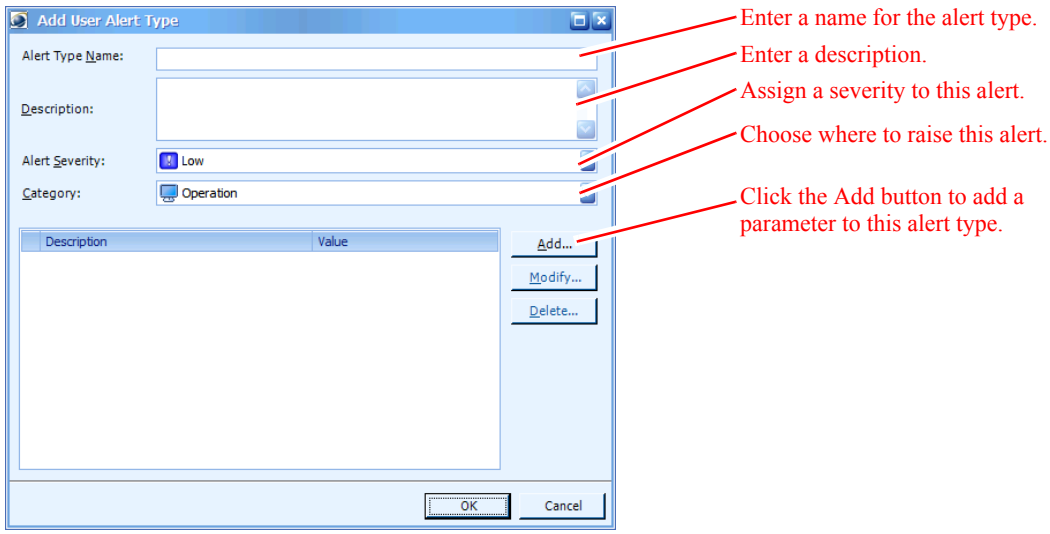


The PSOM User Alert Type Manager window appears.



Step 3 Click **Add** to configure a new alert type.

The Add User Alert Type window appears.



Step 4 Enter a name for this new alert type in the **Alert Type Name** field.

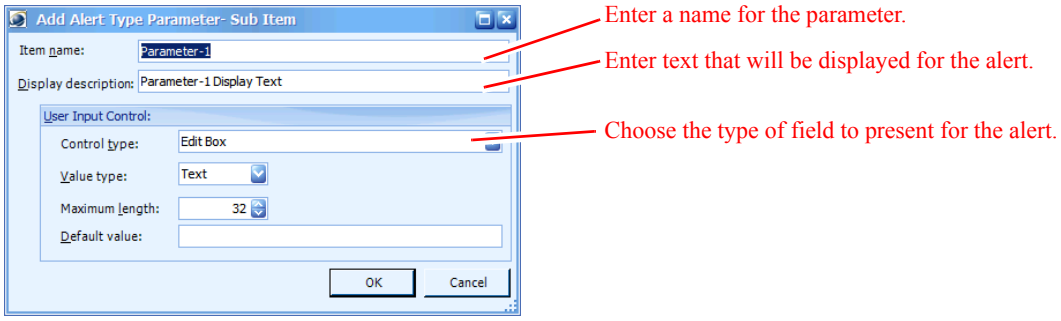
Step 5 Provide an explanation of the alert type's functionality in the **Description** field.

Step 6 Select the severity to assign to this alert type from the **Alert Severity** field.

Step 7 Choose where you want this alert to be raised from the **Category** field. Choose **Operation** to have the alert raised in the Operation Console, and **Correlation** to create an alert based on the occurrence of certain sensor alerts.

Step 8 Click **Add** to enter a parameter for this alert type.

The Add Alert Type Parameter window appears.



Step 9 Enter a name for the parameter in the **Item name** field.

Step 10 Enter the text that will be displayed for this parameter when the alert is raised in the **Display description** field.

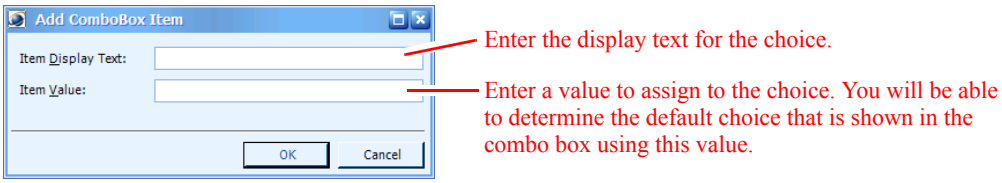
Step 11 Choose whether to make this parameter a checkbox (**CheckBox**), drop-down menu (**ComboBox**), or text area (**Edit Box**).

As shown, you can control the type of content for an Edit field (integer or text), enter the maximum number of characters, and provide a default value.

If you choose to make the parameter a ComboBox, more fields appear.

a. Click **Add** to add a choice to the ComboBox.

The **Add ComboBox Item** dialog appears.



b. Enter display text for the choice in the **Item Display Text** field.

c. Enter a value to assign to the choice in the **Item Value** field. You will be able to determine the default choice that is shown in the combo box using this value.

d. Click **OK**.

e. Repeat to add all choices to the ComboBox.

Step 12 Click **OK** in the Add Rule Parameter window to add this parameter.

Step 13 Click **OK** in the Add User Alert Type window to add this new user alert.

Creating a System Alert Type

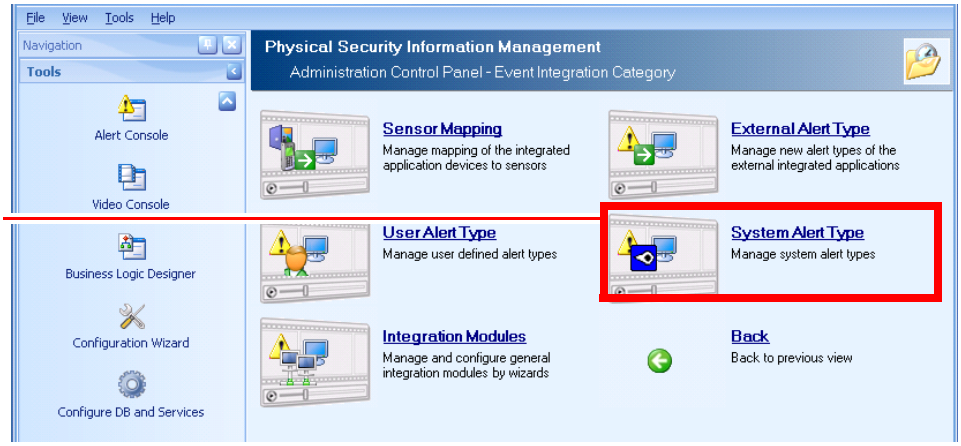
You can create a system alert type for use with business logic; these are mapped with the Event Map field. See Chapter 15, "Business Logic Component Reference," for details.

To create a system alert type:

Step 1 Click the **Event Integration** icon in the Administration Console.

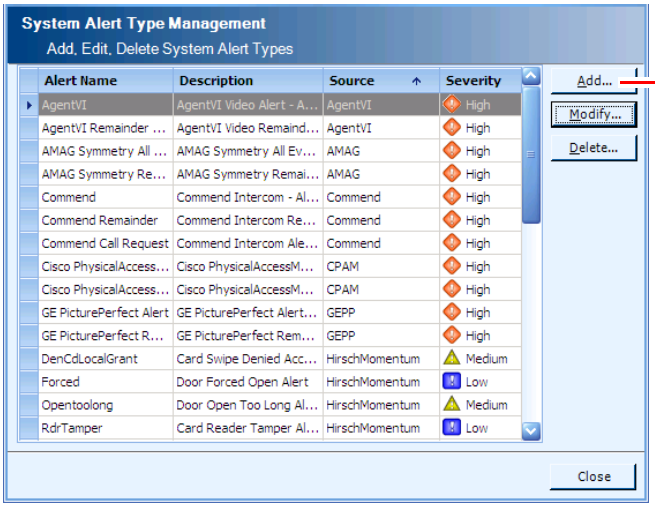
Click the Event Integration icon.

Step 2 Click the **System Alert Type** icon in the Administration Console.



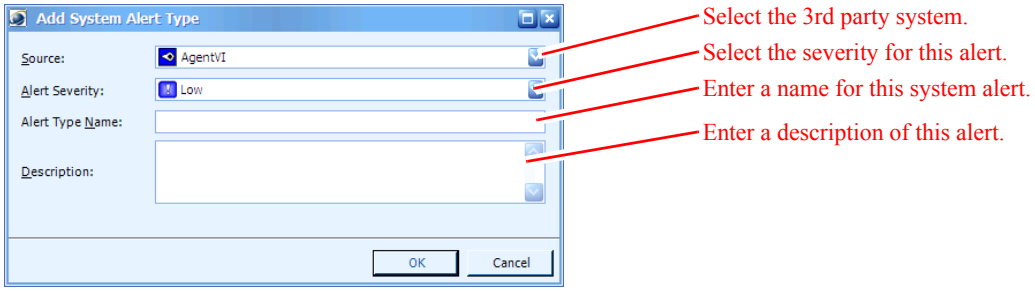
Click the System Alert Type icon.

The PSOM System Alert Type Manager window appears.



Step 3 Click **Add** to configure a new alert type.

The Add System Alert Type window appears.



Step 4 Select the 3rd party system that will generate this system alert from the **Source** field.

Step 5 Select the severity to assign to this system alert in PSOM from the **Alert Severity** field.

Step 6 Enter a name for this system alert to display in PSOM in the **Alert Type Name** field.

Step 7 Enter a description of this system alert in the **Description** field.

Step 8 Click **OK** to add this new system alert.

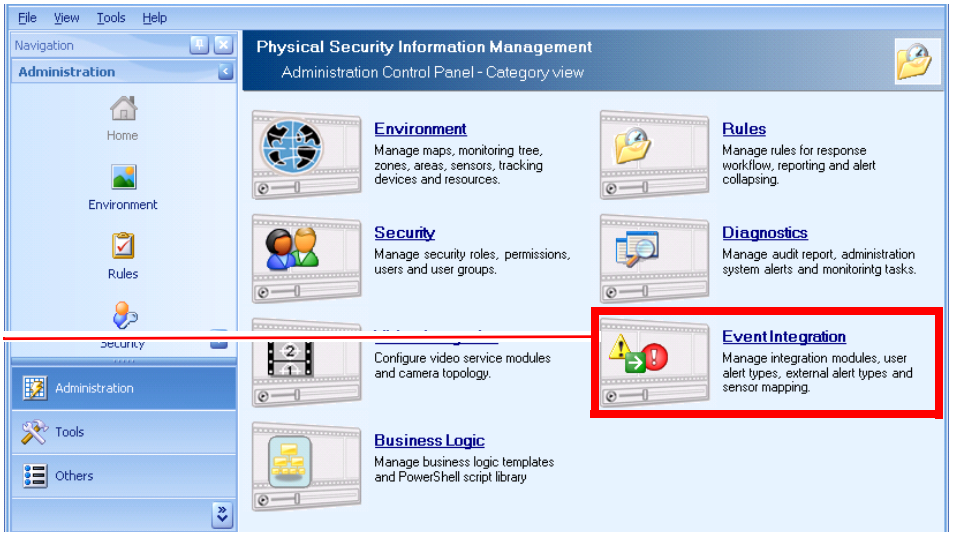
Configuring Integration Modules for External Systems Integration

You can configure PSOM to integrate with external systems by defining instances of the appropriate Integration Modules.

To configure an Integration Module:

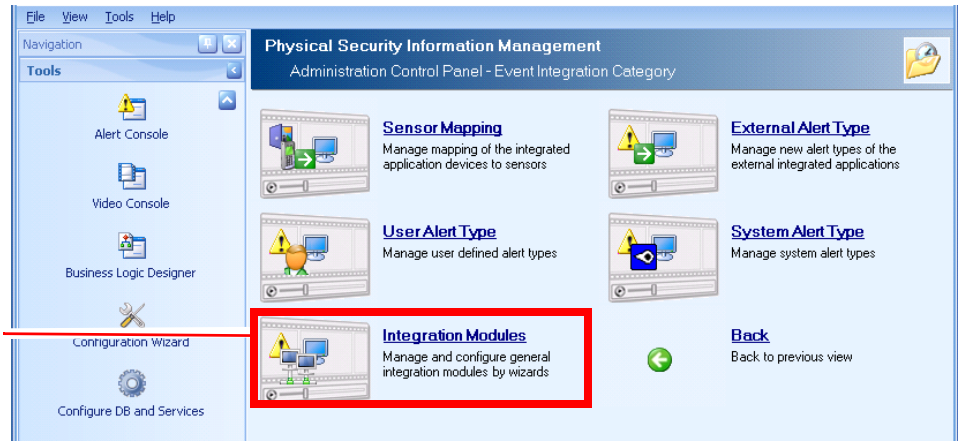
Step 1 Click the **Event Integration** icon in the Administration Console.

Click the Event Integration icon.

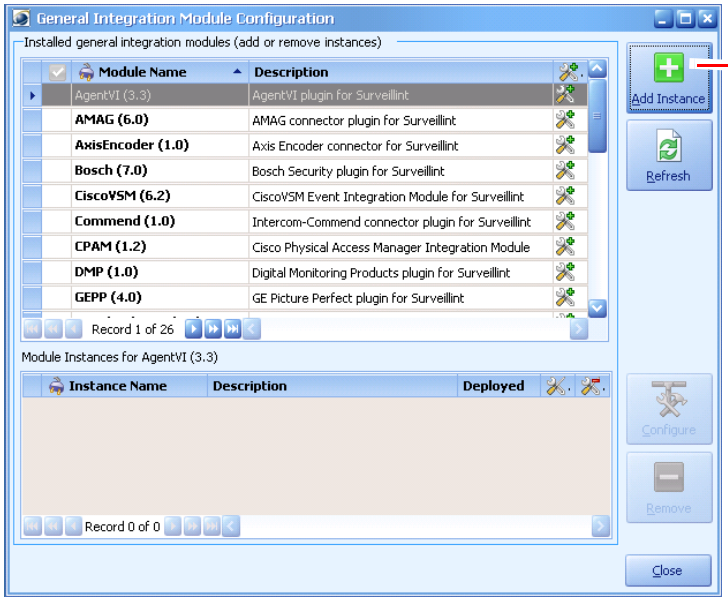


Step 2 Click the **Integration Modules** icon in the Administration Console.

Click the Integration Modules icon.



The General Integration Module Configuration window appears.



Step 3 Select the Integration Module for which you want to configure an external system, and click **Add Instance**.

Refer to the Integration Module documentation for the external system you are trying to configure for the remaining configuration steps.

CHAPTER 12

Setting Up EZ-Track

EZ-Track enables security teams to track suspects across video cameras with simple point-and-click operations. There are several configurations in the Administration tool to set up EZ-Track.

This chapter explains how to:

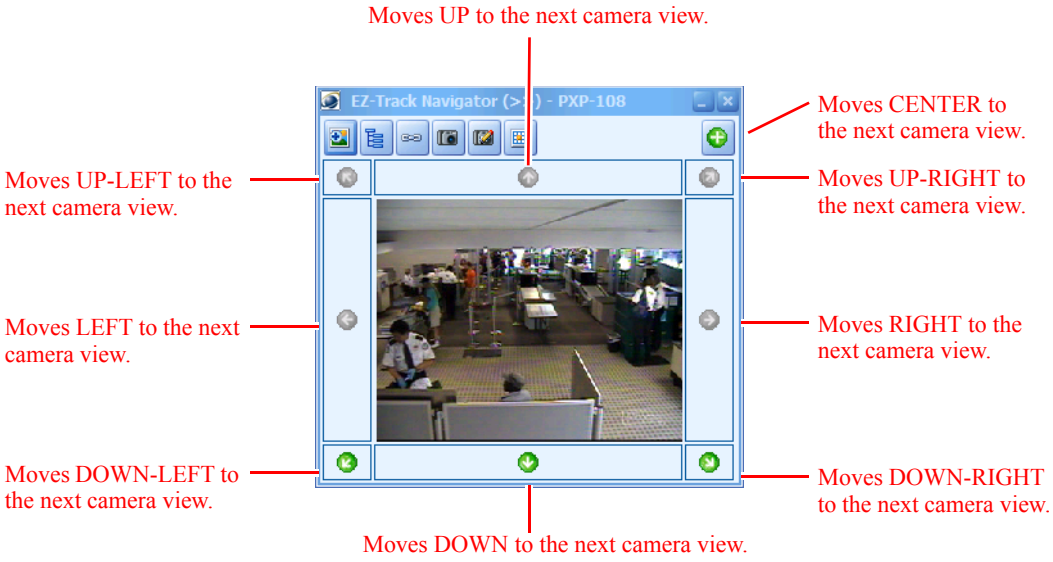
- Prepare video camera sensors for EZ-Track.
- Configure EZ-Track navigation for camera sensors in your PSOM environment.
- Import an EZ-Track configuration from an XML file.
- Enable backward tracking with EZ-Track (Backward).

This chapter includes these topics:

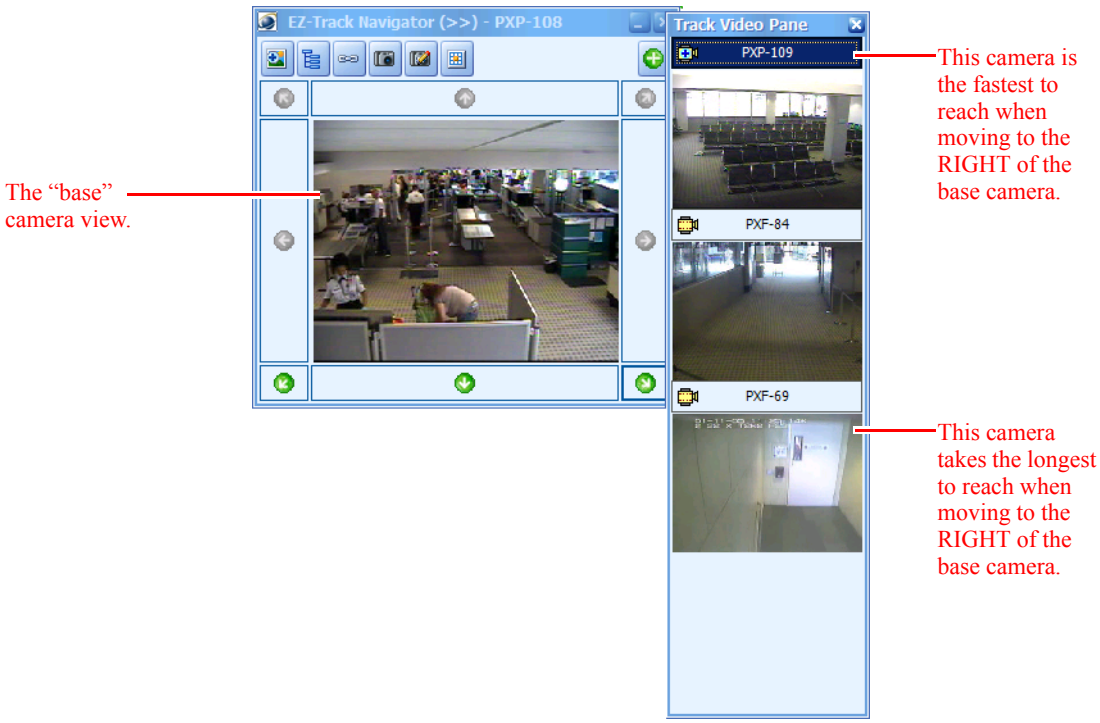
- How Operators use EZ-Track, page 12-1
- Configuring PSOM for EZ-Track, page 12-3
- Enabling EZ-Track (Backward), page 12-19
- Configuring EZ-Track in Batch with XML Configuration File, page 12-20
- Exporting Your EZ-Track Configuration, page 12-22

How Operators use EZ-Track

From the Operation Console, operators use EZ-Track to follow suspects across adjacent camera views with simple point-and-click. They do not need to know any sensor names, or where camera sensors are geographically located—EZ-Track takes all the guesswork out of it.

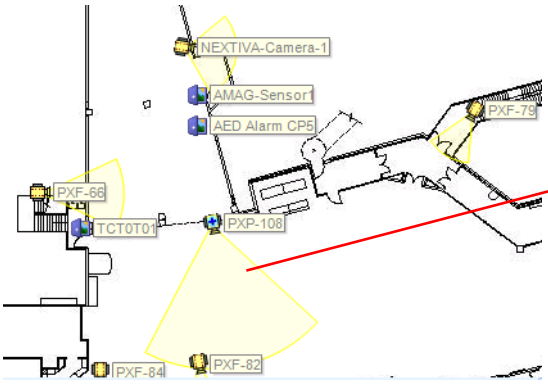


When operators click on a green arrow in the direction grid, the Track Video Pane appears showing potential camera views for that adjacent direction. The camera that is the fastest to reach from the base camera is displayed at the top, and the camera that take the longest to reach from the base camera is displayed at the bottom. The screen below shows what happened when the Right arrow button was clicked: three different camera views show the view to the right of the "base" camera view.



Configuring PSOM for EZ-Track

Each camera in your physical security environment has a field of view based on the camera angle, how far it can capture images clearly, and its peripheral view. For example, the yellow highlights in the map view shown below indicate the field of view of the various cameras in the environment.



When PSOM is configured with this information, EZ-Track can automatically present the operator with a directional grid that enables point-and-click traversing across various camera views.

EZ-Track performs best when used with stationary cameras. This is because the field of view for a stationary camera is always the same, enabling EZ-Track to predictably present the correct camera view from its directional grid. However, PTZ cameras can also be used with EZ-Track; if the field of view is moved from the default view, it will be automatically restored to the default view within a certain timeframe.

Configuring PSOM for EZ-Track involves a few steps:

1. Take 'field of view' snapshot images for each camera sensor.
2. Configure the view range, view distance and view direction settings for each camera sensor.
3. Display the range and name of the sensor in the Map View.
4. Configure the camera topology to enable EZ-Track navigation.
5. Test your EZ-Track configuration.

Taking 'Field of View' Snapshot Images for Camera Sensors

The 'field of view' snapshot image is useful for determining the camera sensor's visual monitoring area.

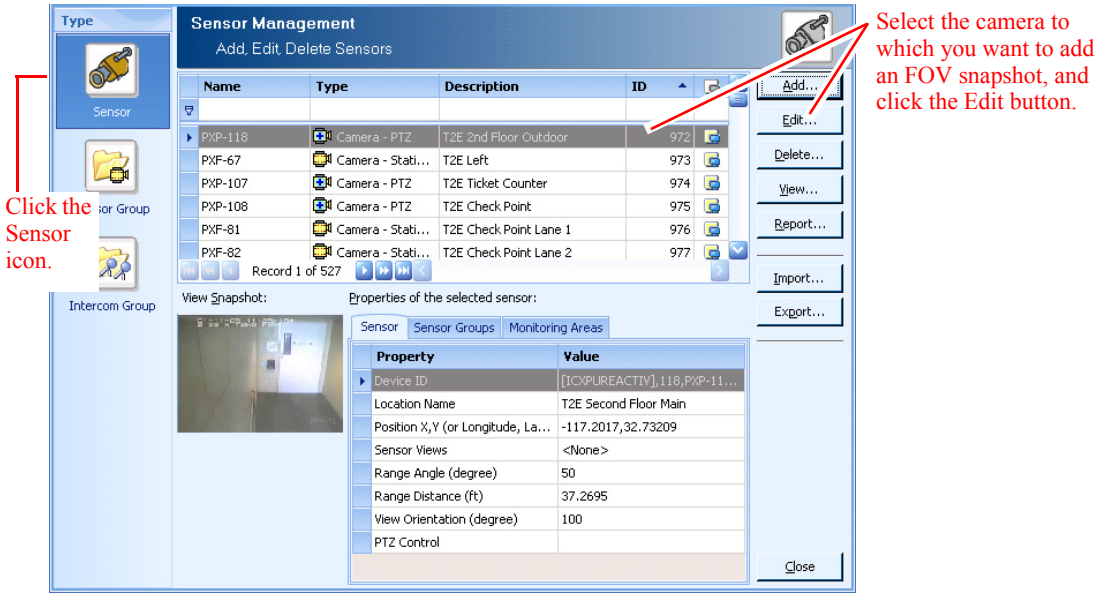
To take a field of view snapshot:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

The Sensor Management window appears.

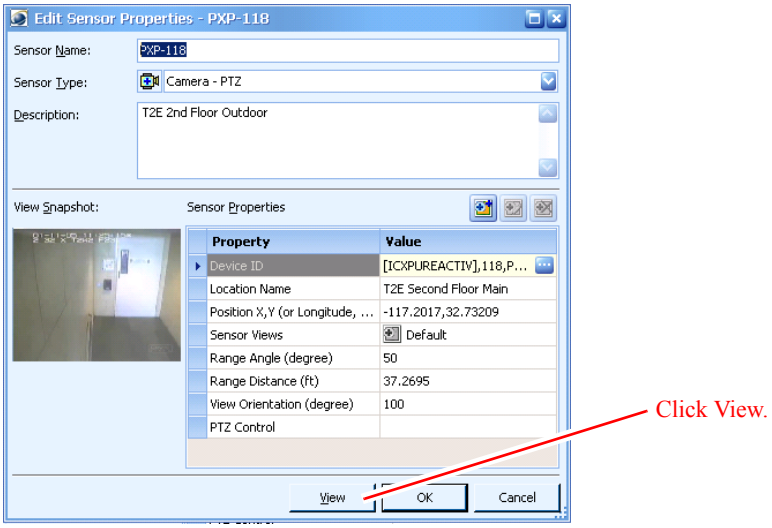


Step 3 Click the **Sensor** icon to display a list of all sensors currently defined for PSOM.

Step 4 Select the camera sensor for which you want to add a field of view snapshot.

Step 5 Click the **Edit** button.

The Edit Sensor Properties window appears.



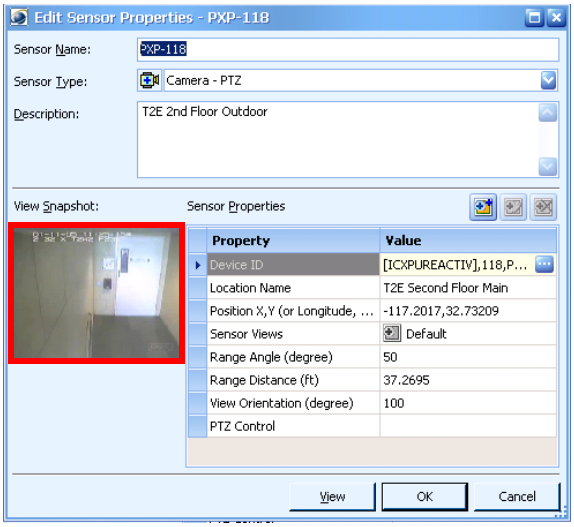
Step 6 Click **View**.

The Live Video Viewer window appears.

Step 7 Click the **FOV Snapshot** button to take a still image of the video feed from this camera that will be added to the sensor's definition in PSOM.

A confirmation dialog box appears. Click **Yes**.

The snapshot is shown as a preview in the Edit Sensor Properties window.



Configuring the View Settings for Camera Sensors

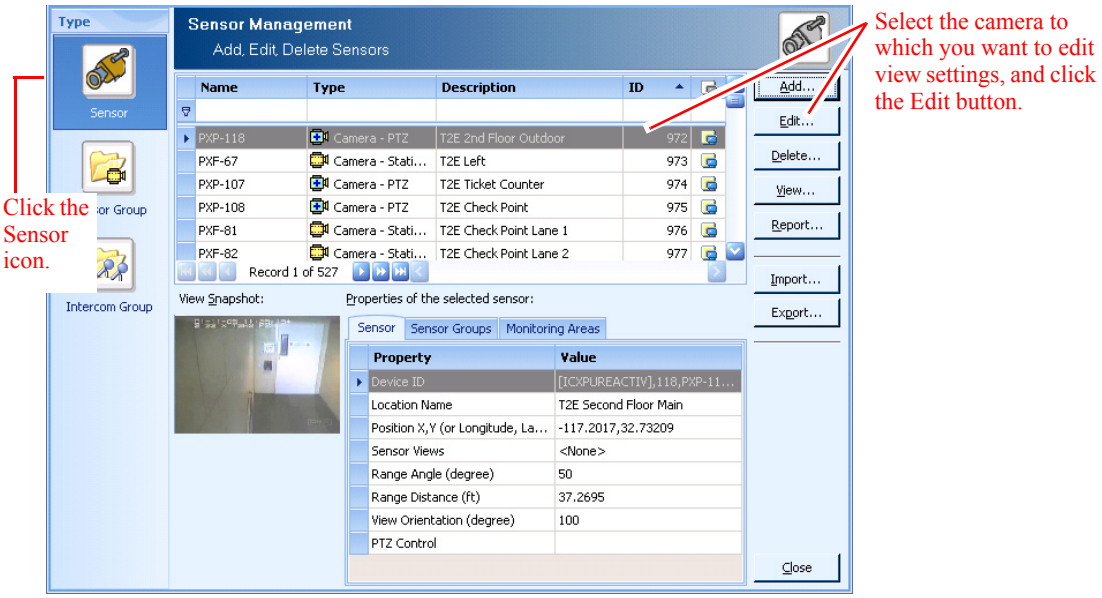
To configure the view range, view distance and view direction settings:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Sensors** icon.

The Sensor Management window appears.

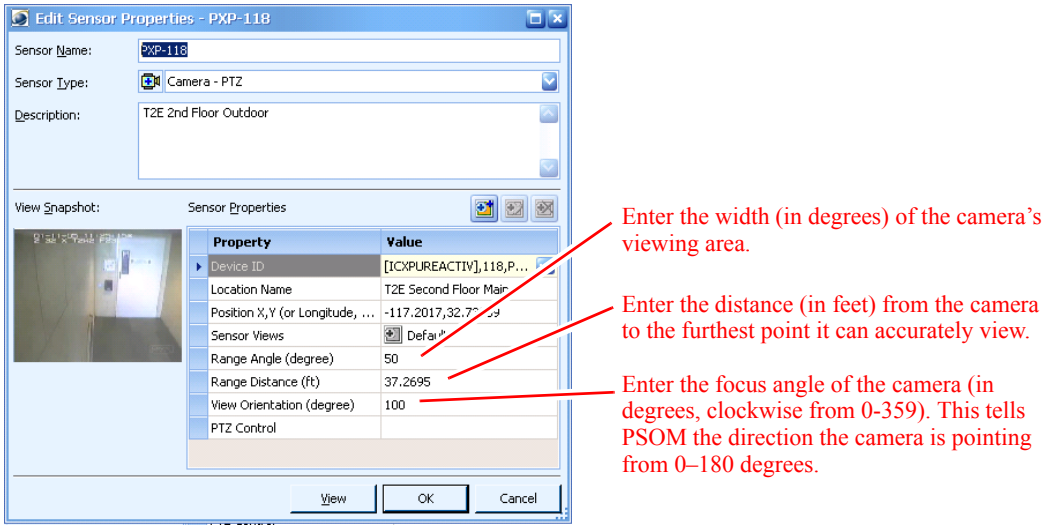


Step 3 Click the **Sensor** icon to display a list of all sensors currently defined for PSOM.

Step 4 Select the camera sensor for which you want to configure view settings.

Step 5 Click the **Edit** button.

The Edit Sensor Properties window appears.



Step 6 In the **View Range (degree)** field, enter the width of the camera's viewing area in degrees.

Step 7 In the **View Distance (ft)** field, enter the distance from the camera to the furthest point it can accurately view.

Step 8 In the **View Direction (degree)** field, enter the angle of the camera view in degrees (clockwise from 0–359 degrees). 0 degrees indicates the camera is pointing to the left, 180 degrees indicates the camera is pointing to the right.

Step 9 For PTZ cameras, you can define different *sensor views* that correspond to preset positions configured in the DVR. See the "Setting Up PTZ Preset Positions" section on page 6-12.

Step 10 Click **OK**.

Displaying the Sensor Name and Range in the Map View

You can display the sensor's name and view range along with the camera icon in the Map View pane. To do so, you must modify the design properties of the map.

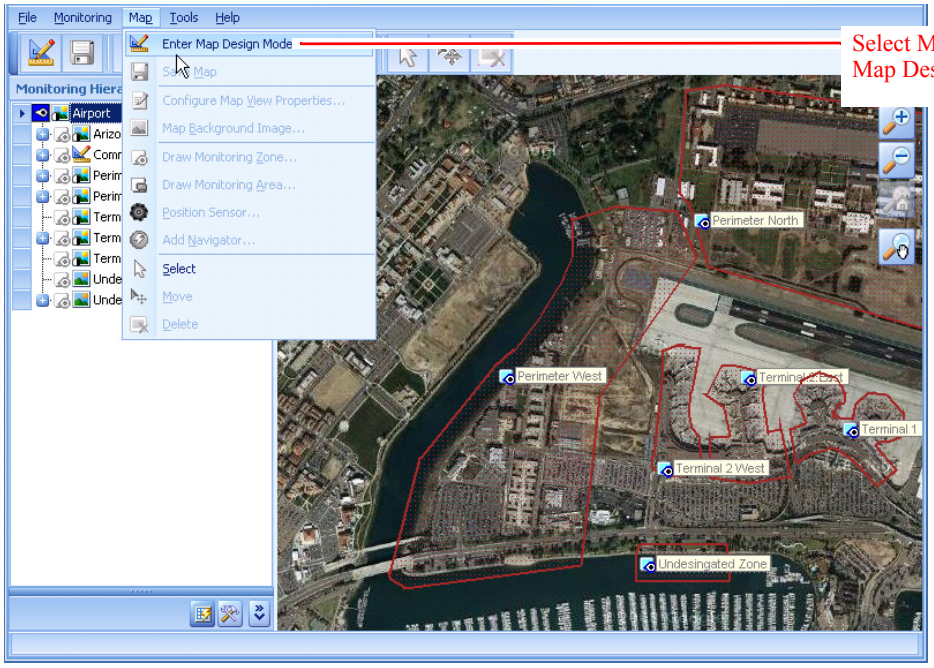
To display the sensor name and range in the Map View pane:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Monitoring Environment** icon.

The PSOM Environment Management window appears.

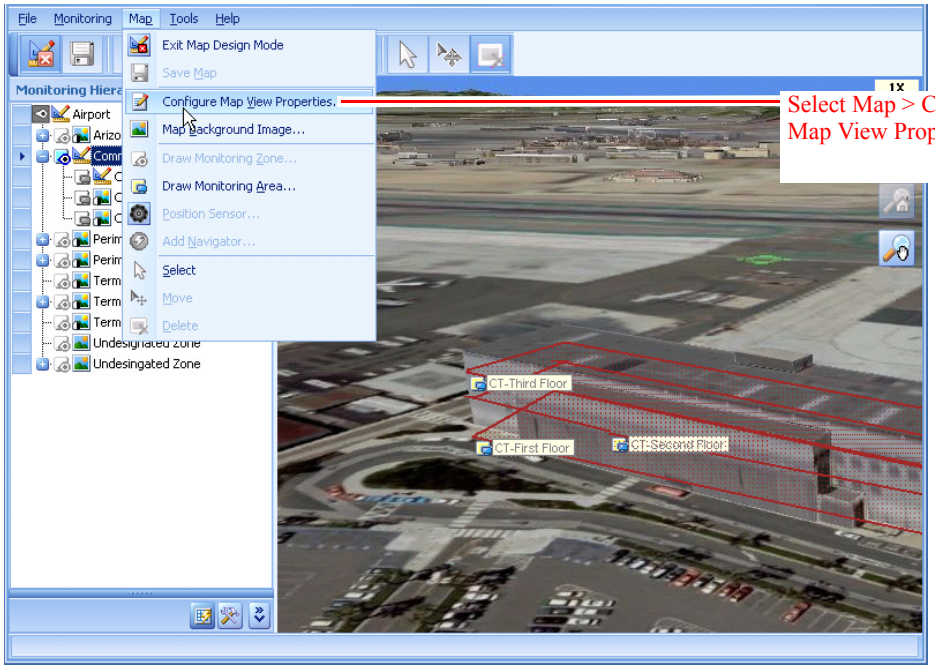


Step 3 Select the global zone node, the top-most node, in the Monitoring Tree.

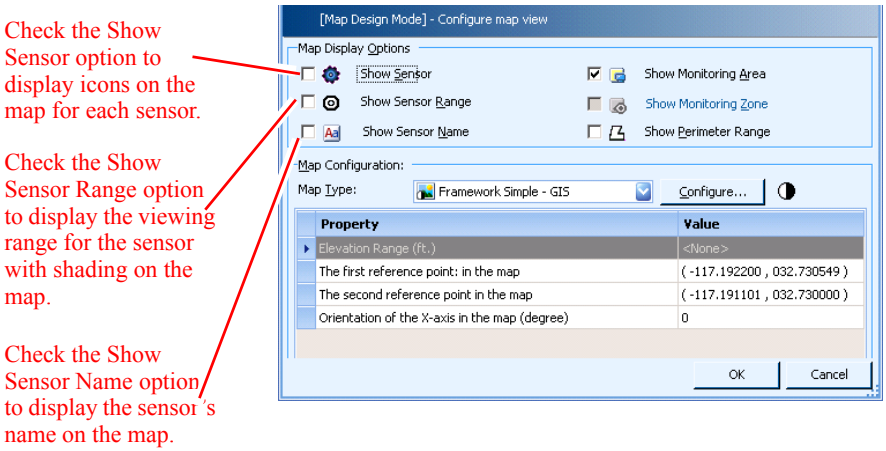
Step 4 From the menu bar select **Map > Enter Map Design Mode**.

Step 5 Select the top-level monitoring zone in the Monitoring Tree for which you want to change display settings.

Step 6 Select **Map > Configure Map View Properties** from the menu bar.



The Map View Properties Configuration window appears.



Step 7 To display icons on the map for each sensor in the environment, check the **Show Sensor** option.

Step 8 To display the viewing range for a camera sensor (a shaded area that represents the area it can capture with video), check the **Show Sensor Range** option.

Step 9 To display the name of each sensor next to its location on the map, check the **Show Sensor Name** option.

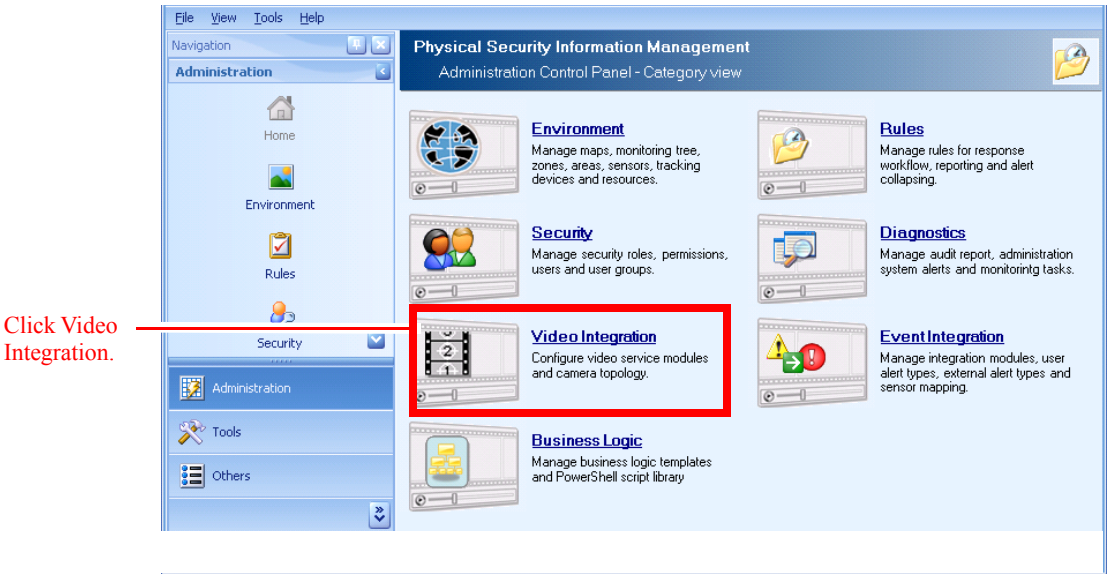
Step 10 Click **OK**.

Step 11 Repeat these steps for each monitoring zone and area for which you want to display the sensor's name and range.

Configuring the EZ-Track Camera Topology

To configure the EZ-Track camera topology:

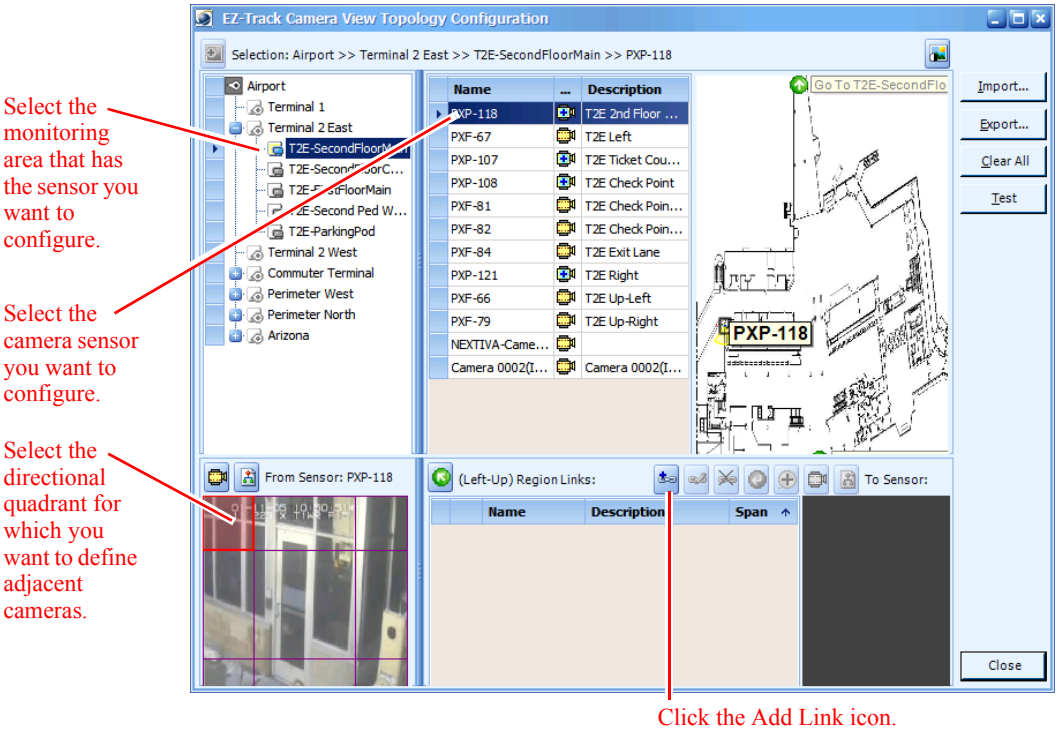
Step 1 Click the **Video Integration** icon in the tools area of the Administration Console.



The Video window appears.

Step 2 Click **Camera Topology** to configure the EZ-Track topology.

The EZ-Track Camera View Topology Configuration window appears.



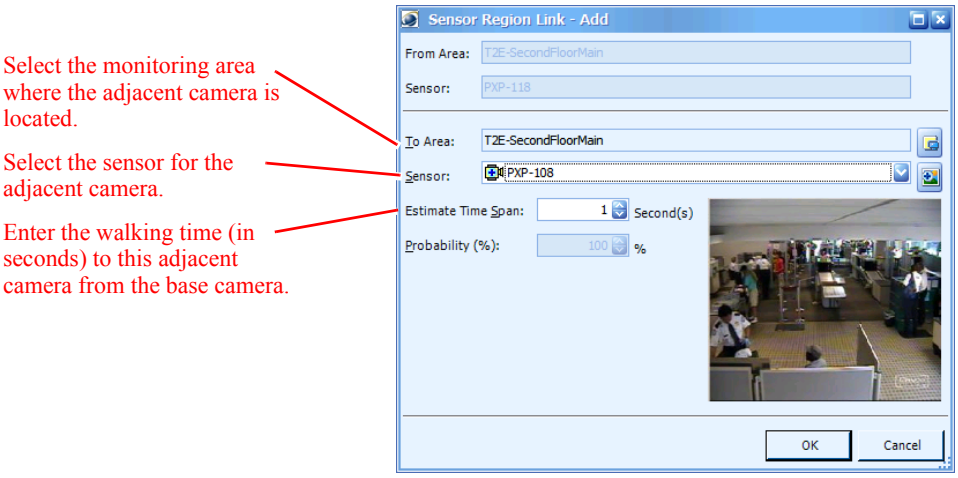
Step 3 Select the monitoring area where the camera sensor is located.

Step 4 Select the camera sensor you want to configure from the list of sensors.

Step 5 In the **From Sensor** area, select the directional quadrant for which you want to designate adjacent cameras.

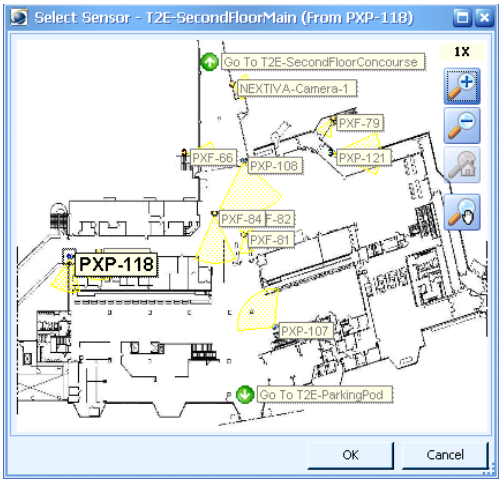
Step 6 Click the **Add Link** icon .

The Sensor Region Link Add window appears.



Step 7 From the **To Area** field, select the monitoring area where the adjacent camera is located.

Step 8 From the **Sensor** field, select the sensor for the adjacent camera. You can either select a sensor from the pull-down menu, or click the **Map** icon to select the sensor from a map view. The Select Sensor window appears.



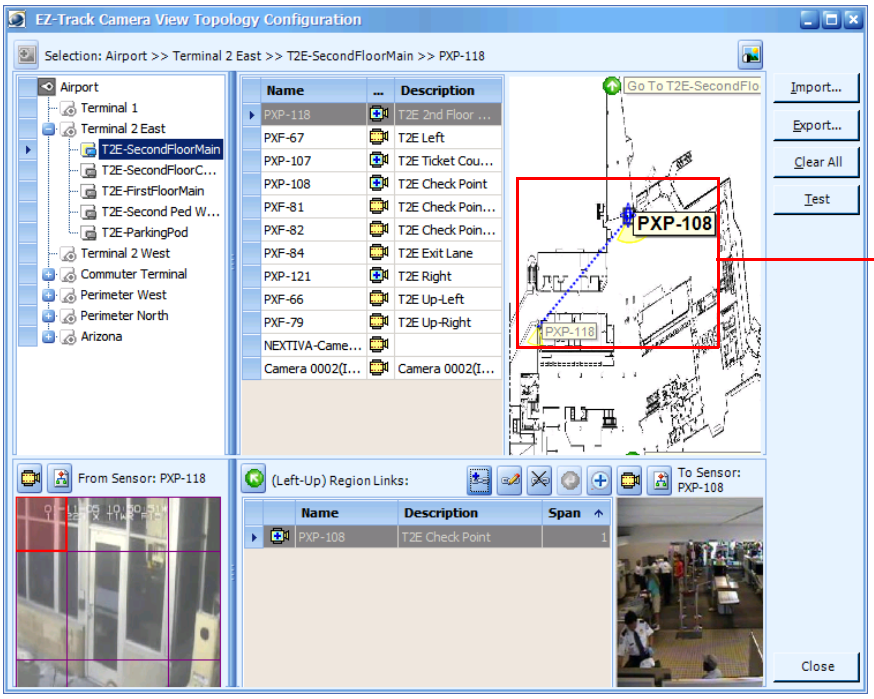
Step 9 Select the sensor from the map to highlight it, and then click **OK**.

Step 10 In the **Estimated Time Span** field, enter the walking time (in seconds) to this adjacent camera from the base camera.

Step 11 Click **OK**.

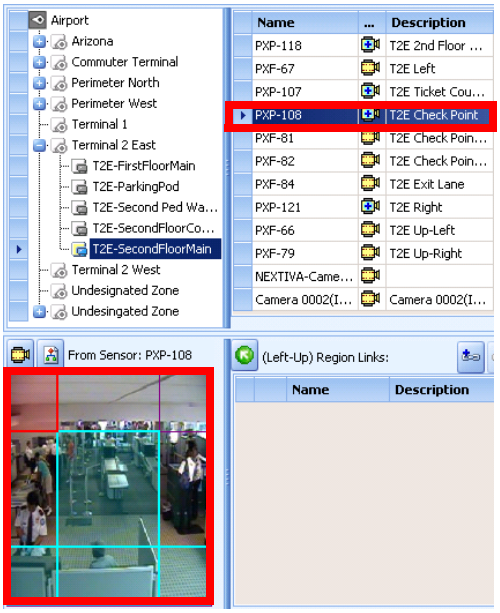
The bottom of the EZ-Track Camera View Topology Configuration window now lists the adjacent camera as a **(Left-Up) Region Link**.

Note You can have up to 4 sensor links per region.

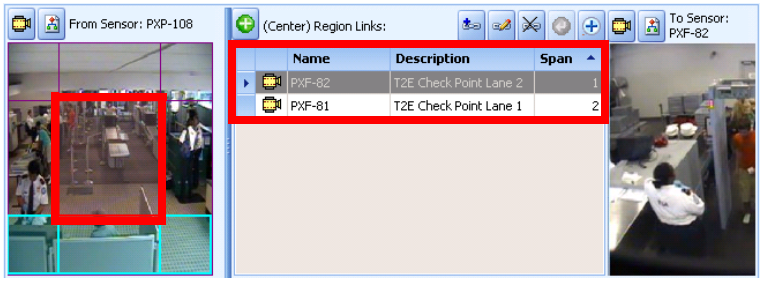


Step 12 Repeat the steps in this section to define adjacent cameras for each quadrant of each camera sensor in your PSOM configuration.

To see the regions with camera links for a sensor, click the sensor in the list. The regions that have defined camera links appear with cyan highlight.



Select one of the regions to see the defined camera links for that region.



To see all the camera sensors that link to a particular camera, select the camera from the Region Links area and click the button. The Sensor Region Links window appears.

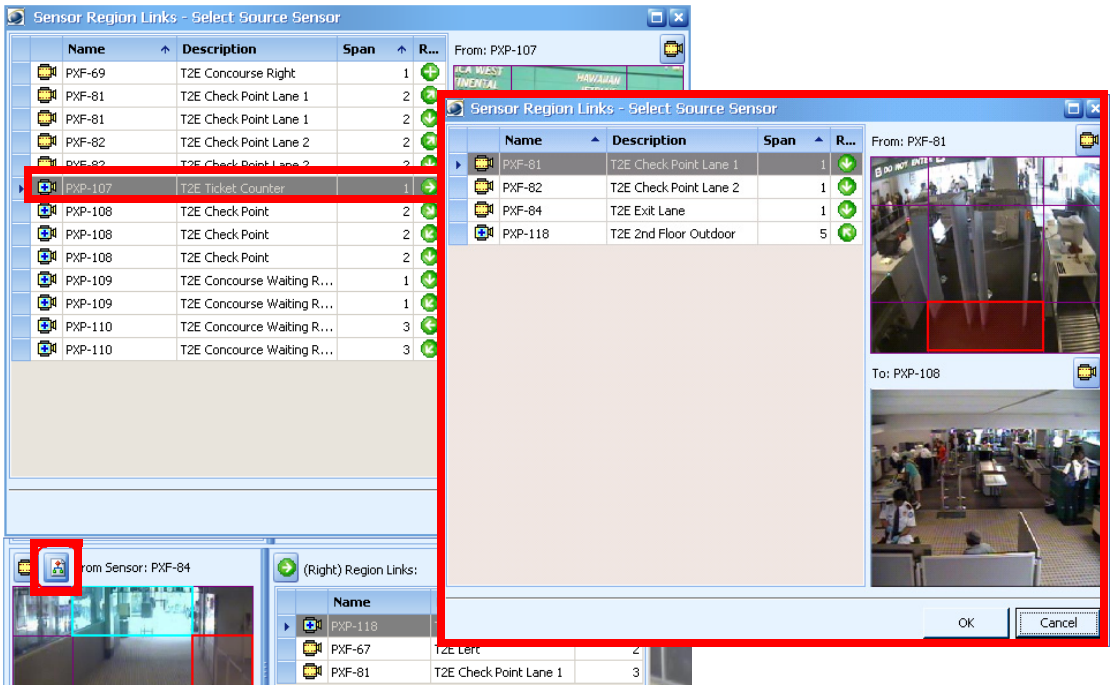


Table 12-1 explains the purpose of the various icons in the **Region Links** area of the EZ-Track Camera View Topology Configuration window.

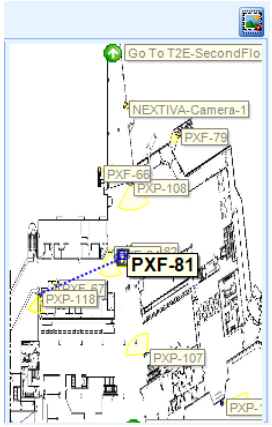
Table 12-1 Icons Displayed in the Region Links Area

Icon	Use this icon to...
	Add a new camera sensor link to the selected region.
	Edit an existing camera sensor link.
	Delete an existing camera sensor link from the selected region.
	Browse back to the previous camera sensor to make it the “base” camera again. This icon is enabled when you’ve browsed away from the original camera sensor to make an adjacent camera the “base” camera.
	Browse to the selected adjacent camera sensor to make it the “base” camera.
	View live video for the selected adjacent camera. You can update the camera’s field of view image from this window.
	Show other region links to the selected adjacent camera.

Displaying Camera Positions and Names on the Map

You can streamline topology configuration by displaying sensor names and positions on the map in the EZ-Track Camera View Topology Configuration window.

To do so, click the Show Sensors icon . The map now appears as shown next.



Viewing Live Video for a Camera Sensor

You can view live video and take a snapshot for a camera sensor from the EZ-Track Camera View Topology Configuration window.

To do so, click the **Live Video** icon . The Live Video Viewer window appears. Click the **FOV Snapshot** link to capture a snapshot for the camera sensor.

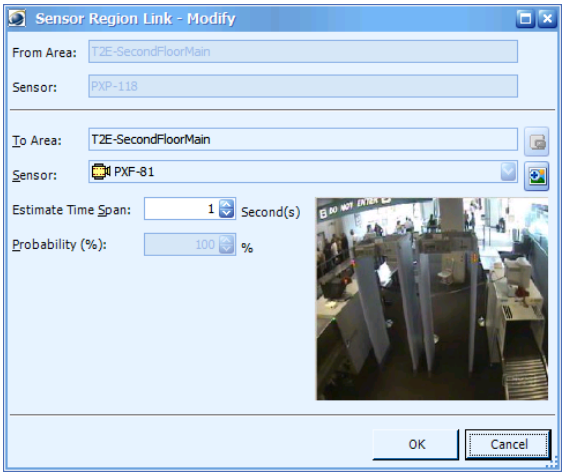
Editing a Link to an Adjacent Camera

To edit the properties of an adjacent camera:

Step 1 Select the adjacent camera in the EZ-Track Camera View Topology Configuration window.

Step 2 Click the **Edit Link** icon .

The Sensor Region Link - Modify window appears.



Step 3 Change the number of seconds in the **Estimate Time Span** field to modify how long it takes to walk to this camera sensor from the base camera.

Step 4 Click **OK**.

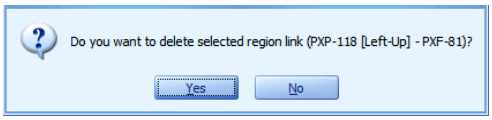
Deleting a Link to an Adjacent Camera

To remove a link to an adjacent camera:

Step 1 Select the adjacent camera in the EZ-Track Camera View Topology Configuration window.

Step 2 Click the **Delete Link** icon .

A confirmation dialog box appears.



Step 3 Click **Yes** to delete the link to this adjacent camera.

Making an Adjacent Camera the New "Base" Camera

You can make an adjacent camera the new "base" camera, and then change back to the original base camera, using the **Browse To** icon and **Browse Back** icon .

Viewing Other Region Links to an Adjacent Camera

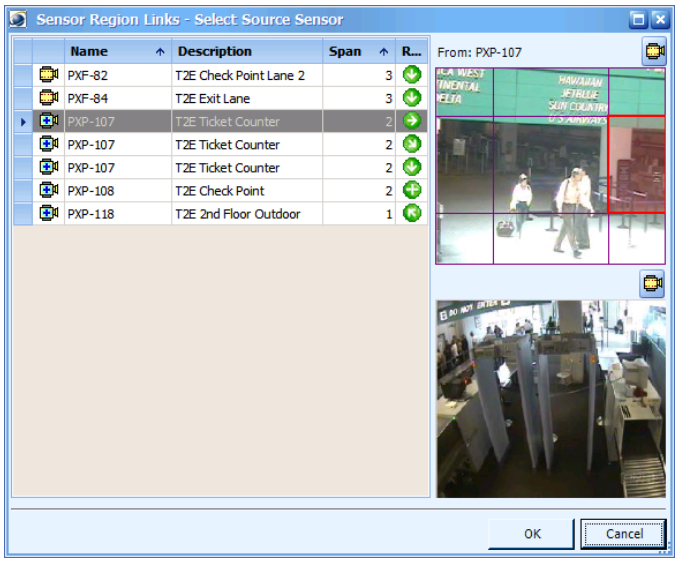
You can view all the region links to an adjacent camera.

To view other region links:

Step 1 Select the adjacent camera from the **Region Links** area.

Step 2 Click the **Other Links** icon .

The Sensor Region Links window appears.



Select different sensors from the list to see the quadrant views they provide for the adjacent camera. You can view live video for a selected camera by clicking the **Live Video** icon .

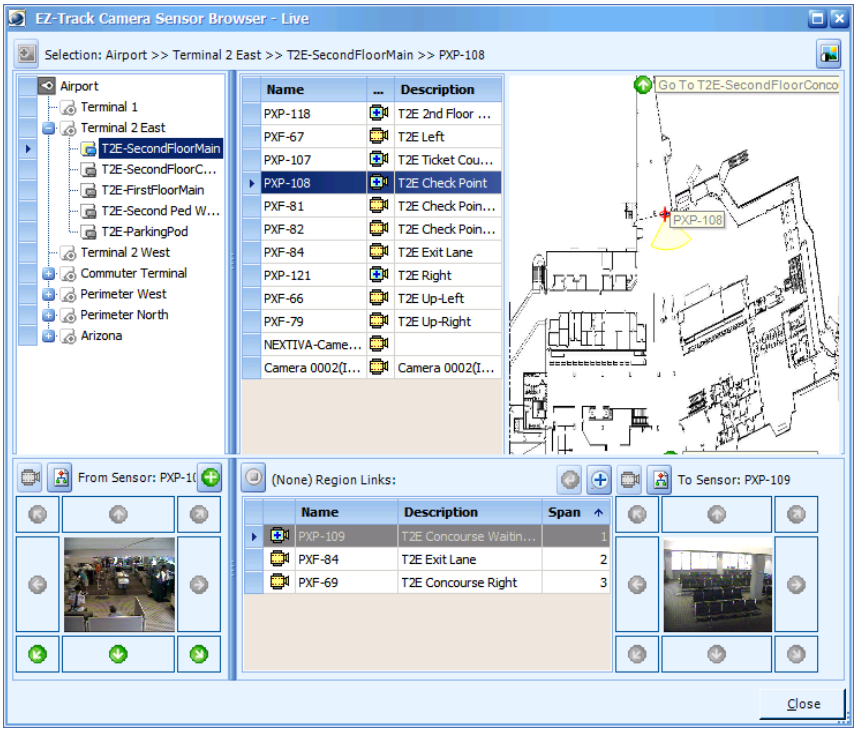
Testing the EZ-Track Configuration

To test an EZ-Track configuration:

Step 1 Make sure your base camera is selected.

Step 2 Click the **Test** button.

The EZ-Track Camera Sensor Browser window appears.



Step 3 Click the different quadrants that have green arrows to test that the adjacent camera views are displayed appropriately.

The bottom of the window shows the **From Sensor** and **To Sensor** live video views so you can ensure the correct video is being displayed. Also, the sensor's location appears on the map so you can verify that the correct sensor has been selected for the adjacent quadrant.

If more than one camera has been defined for a quadrant, there will be multiple cameras shown in the **Region Links** area. Switch between them by selecting the different camera sensors from the list, and the **To Sensor** live video will change as well as the sensor's location in the Map area.

Use the **Browse To** icon and **Browse Back** icon to change the "base" camera to an adjacent camera view, and then back again to the original "base" camera.

Click the **Other Links** icon to see other region links to the adjacent camera that is selected in the Region Links area.

Enabling EZ-Track (Backward)

You can enable operators to track suspects backward through recorded video using EZ-Track (Backward). EZ-Track (Backward) requires the use of Cisco Video Surveillance Manager as well as a license key that unlocks the EZ-Track (Backward) feature.

Configuring EZ-Track in Batch with XML Configuration File

You can configure EZ-Track by setting up configurations in an XML file, and then importing that to the EZ-Track Camera View Topology Configuration window using the **Import** button.

Defining the EZ-Track Configuration in XML

The syntax for the XML-based EZ-Track configuration is as follows:

```
<PxRegionTopology>
==> <PxSensorRegionLinks SourceSensorName="{From Sensor Name}”>
==> <PxRegionLinks SourceRegionCode="{Region Name}">
==> <PxRegionLink>
==> <DestinationSensorName> {To Sensor Name}
==> <SecondSpan> {Estimate Time Span}
```

where:

Parameter	Description	Valid Values
`"{From Sensor Name}”`	The name assigned to the “base” camera sensor. **Note** The sensor name must be enclosed in quotes.	e.g., “P-300”
`"{Region Name}”`	The region of the “base” camera view where the adjacent camera is being assigned. Keywords for the {Region Name} are case-sensitive. **Note** The region name keyword must be enclosed in quotes.	“UpLeft”—Upper left quadrant “Up”—Upper middle quadrant “UpRight”—Upper right quadrant “Right”—Right quadrant “DownRight”—Lower right quadrant “Down”—Lower middle quadrant “DownLeft”—Lower left quadrant “Left”—Left quadrant “Center”—Center quadrant
`{To Sensor Name}`	The name assigned to the “adjacent” camera sensor.	e.g., P-291
`{Estimate Time Span}`	The number of seconds it takes to walk from the base camera to the adjacent camera.	e.g., 30

For example, the following EZ-Track configuration defines the adjacent camera views to the right and lower right quadrants for “base” camera P-107. It configures camera sensors F-84 and F-81 as adjacent cameras for the right quadrant of camera P-107, and camera sensors F82 and F81 as adjacent cameras for the lower right quadrant of camera P-107.

```
<?xml version="1.0" encoding="utf-8"?>
<PxRegionTopology VERSION="1.0">
    <PxSensorRegionLinks SourceSensorName="P-107">
        <PxRegionLinks SourceRegionCode="Right">
            <RegionLink>
```

```
                <DestinationSensorName>F-84</DestinationSensorName>
                <SecondSpan>1</SecondSpan>
            </RegionLink>
            <RegionLink>
                <DestinationSensorName>F-81</DestinationSensorName>
                <SecondSpan>2</SecondSpan>
        </RegionLink>
         </PxRegionLinks>
         <PxRegionLinks SourceRegionCode="DownRight">
            <RegionLink>
                <DestinationSensorName>F-82</DestinationSensorName>
                <SecondSpan>1</SecondSpan>
            </RegionLink>
            <RegionLink>
                <DestinationSensorName>F-81</DestinationSensorName>
                <SecondSpan>2</SecondSpan>
            </RegionLink>
        </PxRegionLinks>
    </PxSensorRegionLinks>
</PxRegionTopology>
```

Uploading the XML Configuration File for EZ-Track

Once you've defined the EZ-Track configuration in an XML file, you can upload the file to PSOM to define all EZ-Track camera configurations all at once.

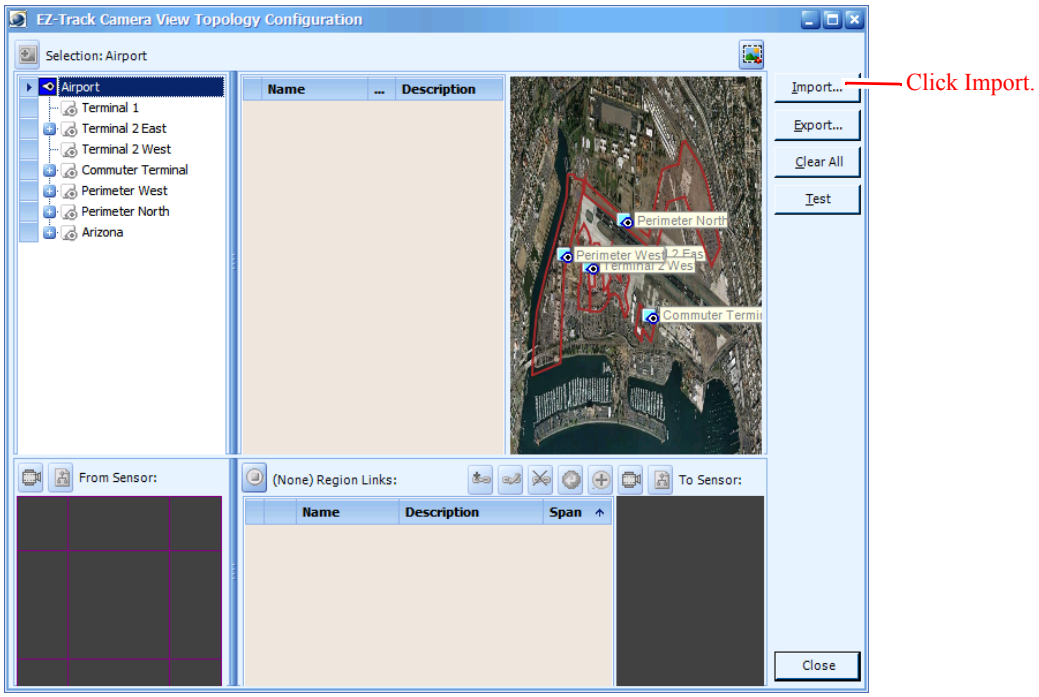
To upload the XML configuration file:

Step 1 Click the **Video Integration** icon in the tools area of the Administration Console.

The **Video** window appears.

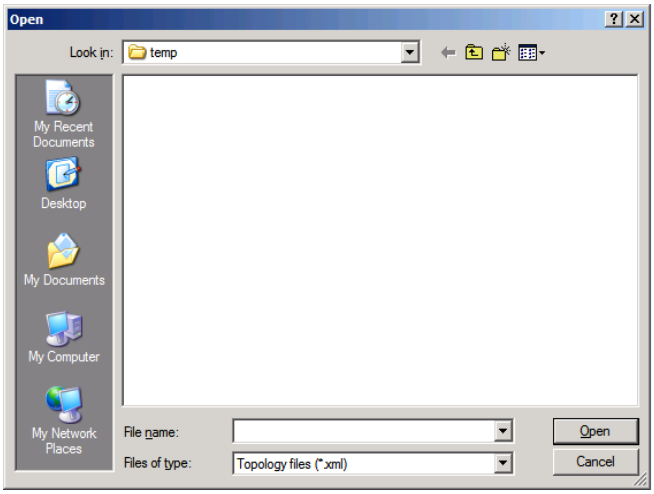
Step 2 Click **Camera Topology** to configure the EZ-Track topology.

The EZ-Track Camera View Topology Configuration window appears.



Step 3 Click **Import**.

The Open window appears.



Step 4 Locate and select the XML configuration file and click **Open**.

Exporting Your EZ-Track Configuration

If you want to backup your EZ-Track configuration—perhaps to re-import it later using the **Import** button—you can click **Export** to save the topology file with all necessary XML to define the EZ-Track navigation as you have configured it.

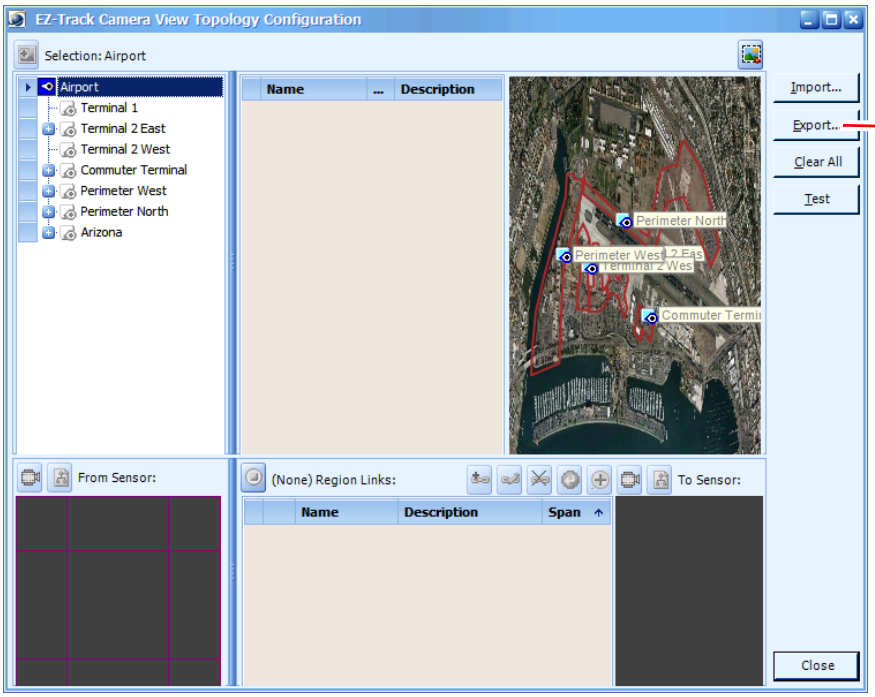
To export the EZ-Track configuration to a file:

Step 1 Click the **Video Integration** icon in the tools area of the Administration Console.

The Video window appears.

Step 2 Click **Camera Topology** to access the EZ-Track topology.

The EZ-Track Camera View Topology Configuration window appears.



Step 3 Click **Export**.

The Save as topology file window appears.

Step 4 Choose a location to save the XML configuration file and click **Save**.

CHAPTER 13

Managing Tracking Devices and Resources

Within the Operation Console, operators can monitor the movements of tracking devices and security resources within the environment. In the Administration Console, you can:

- Configure GPS geographic coordinates for all maps within the PSOM environment. See the "Configuring Coordinates using GPS" section on page 7-8 for instructions.
- View and activate/deactivate resources within PSOM that represent security officers, vehicles, or other assets within your environment.
- View and activate/deactivate tracking devices within PSOM that integrate with external 3rd party tracking services so that the location of these devices is displayed in the Operation Console.

Before proceeding with this chapter, refer to PSOM Integration Module documentation for instructions on integrating your third-party security systems with PSOM so that resources and tracking devices can automatically be defined.

This chapter includes these topics:

- Viewing Security Resources, page 13-1
- Understanding Tracking Devices, page 13-5

Viewing Security Resources

Security resources are assets within your environment including:

- People
- Land vehicles
- Water vehicles
- Air vehicles
- Generic assets
- Security officers
- Law enforcement officers
- Law enforcement vehicles
- Emergency vehicles (fire, ambulance, etc.)

Each security resource can be associated with a tracking device within PSOM; for example, a security officer could carry a tracking device to show his position within the environment. PSOM integrates with 3rd party location service applications to display the current location, or historical trail of locations for a security resource, within the Operation Console.

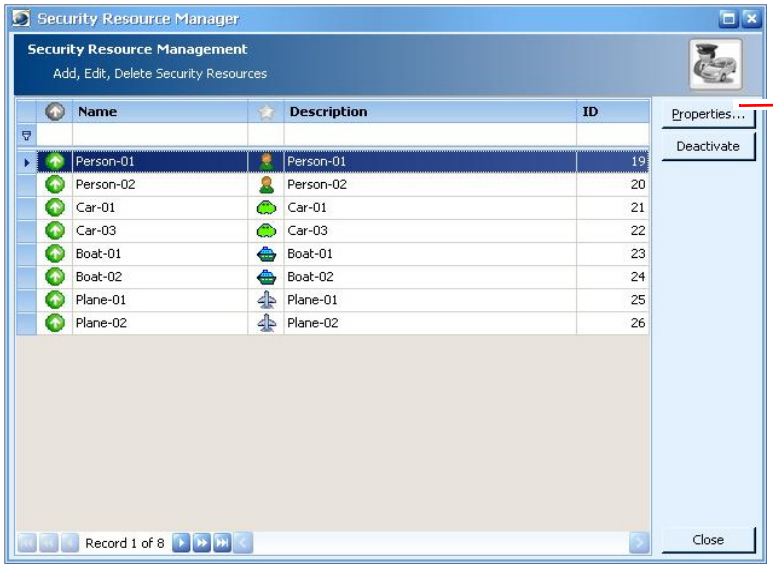
To view security resources defined in PSOM:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

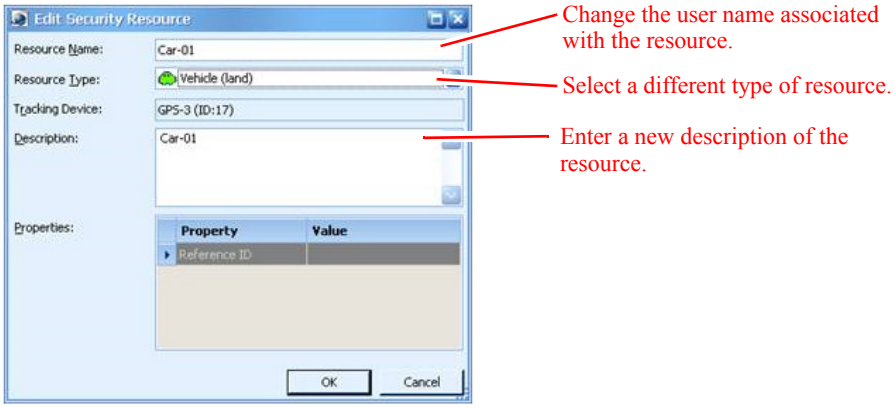
Step 2 Click the **Resources** icon.

The Security Resource Manager window appears.



Step 3 Click **Properties**.

The Edit Security Resource window appears.



Step 4 To change the name associated with the resource, enter a new name in the **Resource Name** field.

Step 5 To change the type assigned to the resource, make a selection from the **Resource Type** field.

Step 6 To change the description, enter modifications in the **Description** field.

Step 7 Click **OK**.

Activating or Deactivating a Resource

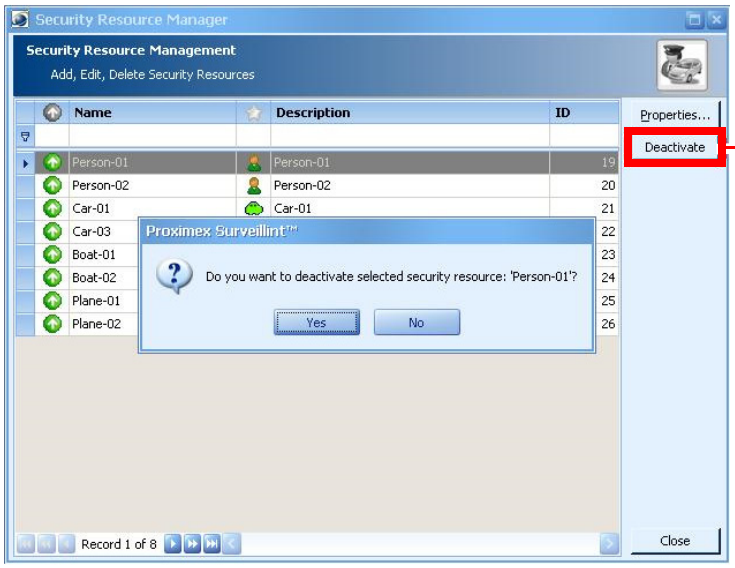
To activate or deactivate a resource:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Resources** icon.

The Security Resource Manager window appears.

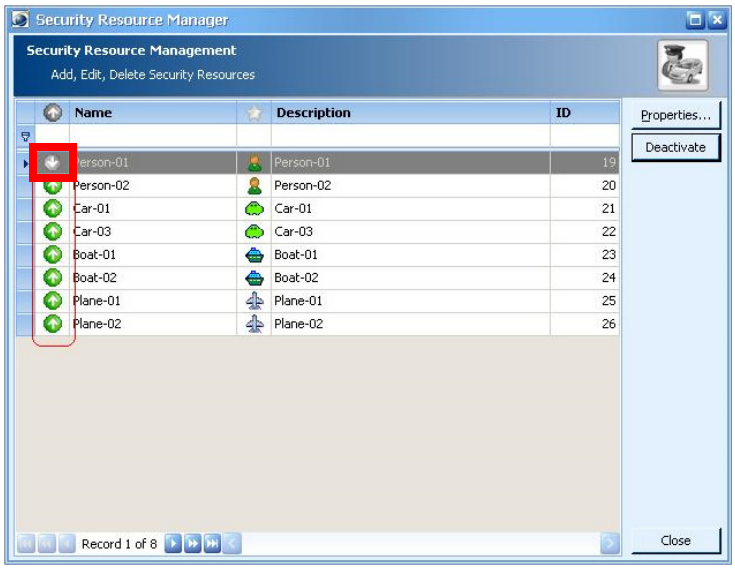


Select the resource you want to disable and click the Deactivate button to disable the resource or the Activate button to enable the resource.

Step 3 Select the resource and click the **Deactivate** button to disable it, or the **Activate** button to enable it.

Step 4 Click **Yes** in the confirmation dialog box to verify the operation.

Resources that have been deactivated appear with a greyed-out icon in the resource list in the **Security Resource Manager**. Active resources appear with green icons.



Understanding Tracking Devices

Tracking devices are wireless electronic devices whose GPS (global positioning system) coordinates can be viewed on an electronic map using specialized software. PSOM synchronizes with integrated subsystems to create tracking devices that appear on maps including:

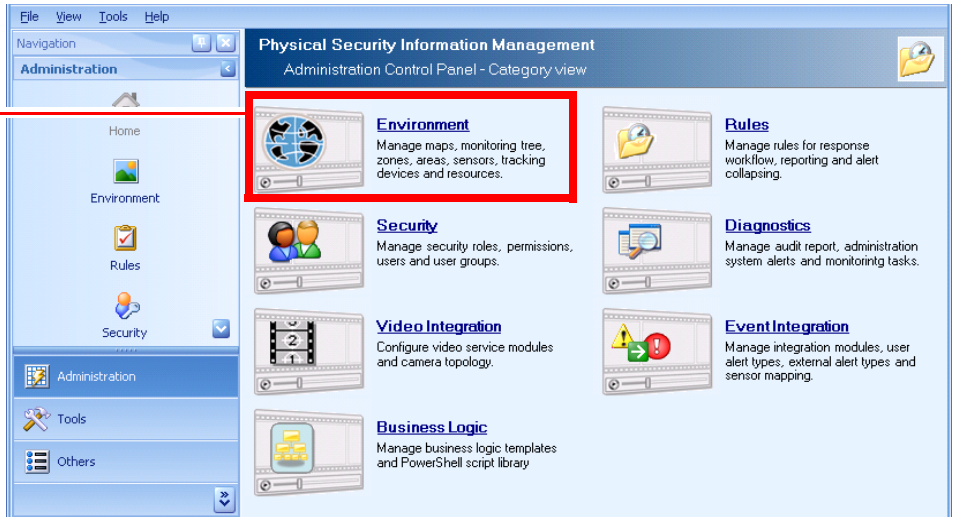
- GPS devices—These devices use GPS transmitters to communicate their coordinates.
- RFID devices—These devices use radio-frequency identification (RFID) tags or transponders to communicate coordinates.
- Radar devices—These devices use electromagnetic waves to identify the range, altitude, direction, or speed of both moving and fixed objects such as aircraft, ships, motor vehicles, and terrain.
- Mobile devices—These pocket-sized computing devices include cell phones, smart phones, personal digital assistants (PDAs), and personal navigation devices (PNDs). These devices use cellular signals to transmit location to PSOM.
- Radio devices—These devices use short-range radio frequency to communicate coordinates.
- Virtual devices—These devices show the location of tracking objects; for example, radar-generated tracking objects.

Security resources can carry tracking devices, or tracking devices can be placed in vehicles or other assets, to allow security operators to track movements within the environment.

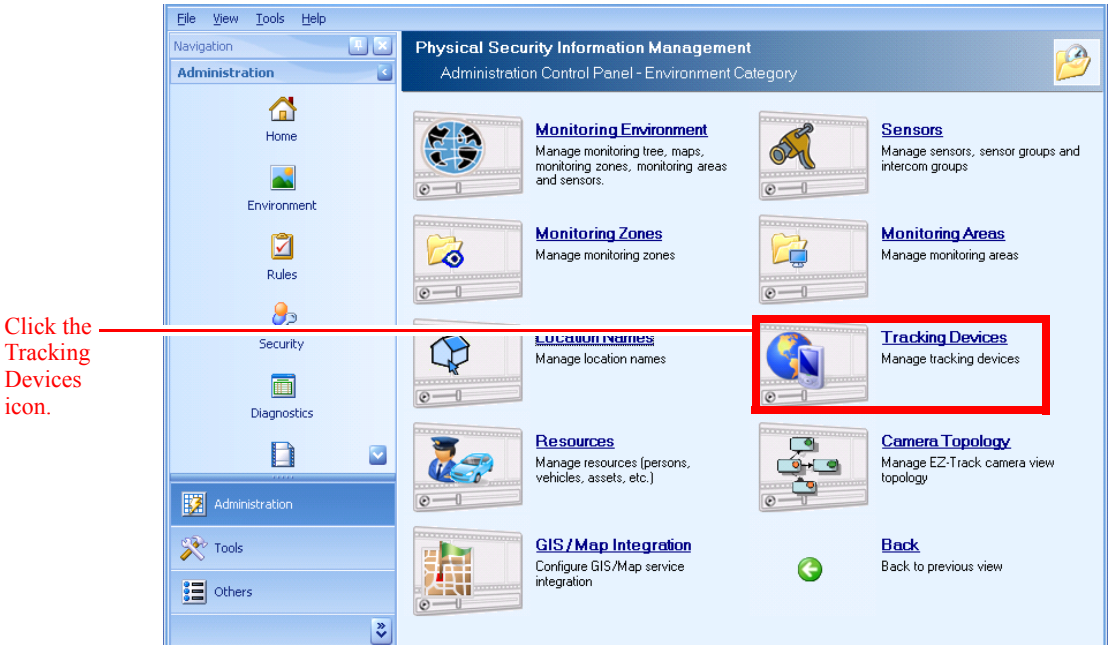
Viewing Tracking Devices in PSOM

To view tracking device in PSOM:

Step 1 Click the **Environment** icon in the Administration Console.

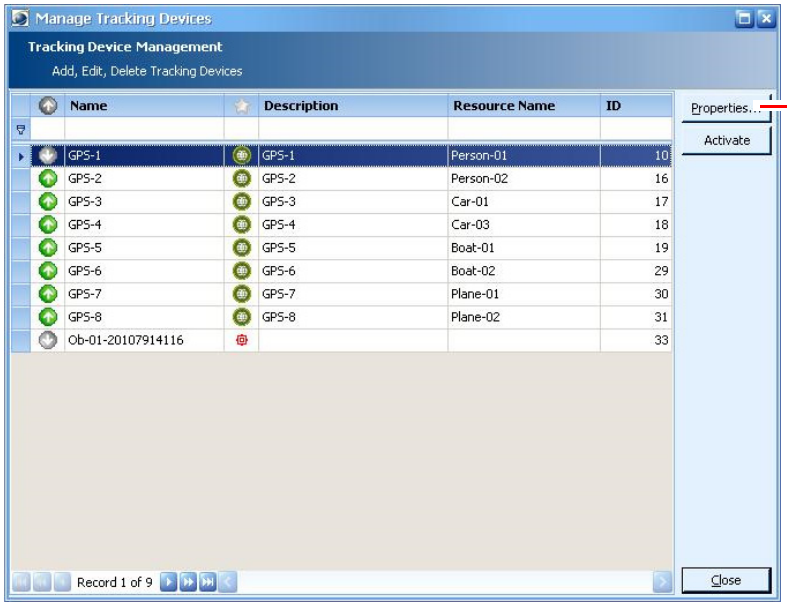


The Environment window appears.



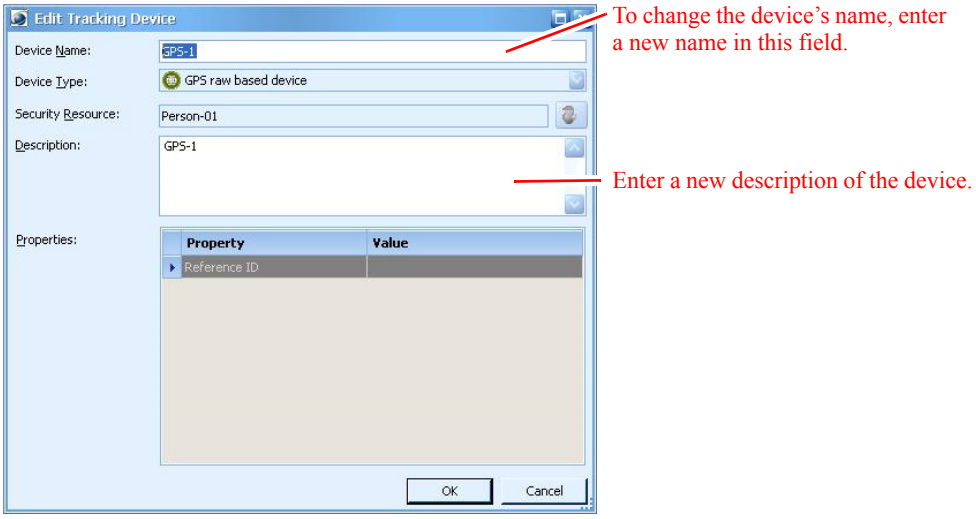
Step 2 Click the **Tracking Devices** icon.

The Manage Tracking Devices window appears.



Step 3 Click **Properties**.

The Edit Tracking Device window appears.



Step 4 To change the device's name, enter a different name in the **Device Name** field.

Step 5 To change the description, enter modifications in the **Description** field.

Step 6 Click **OK**.

Activating or Deactivating a Tracking Device

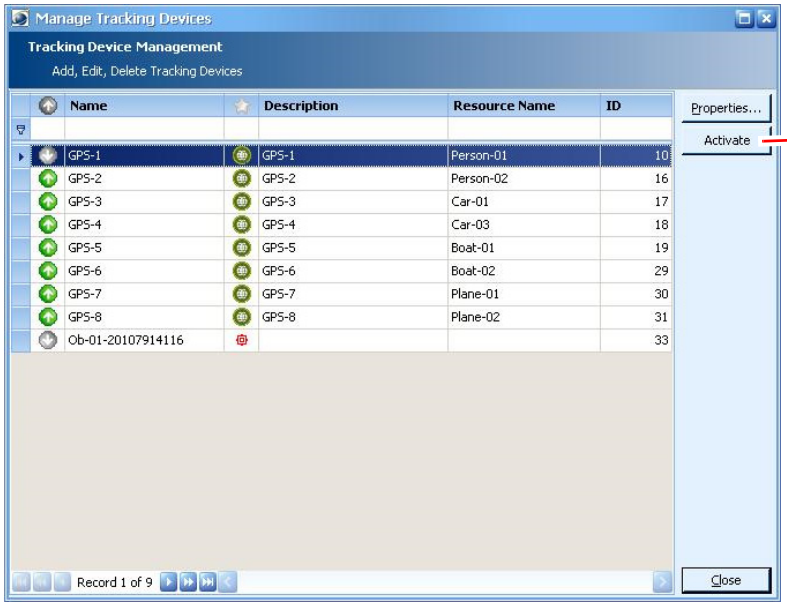
To activate or deactivate a tracking device:

Step 1 Click the **Environment** icon in the Administration Console.

The Environment window appears.

Step 2 Click the **Tracking Devices** icon.

The Manage Tracking Devices window appears.



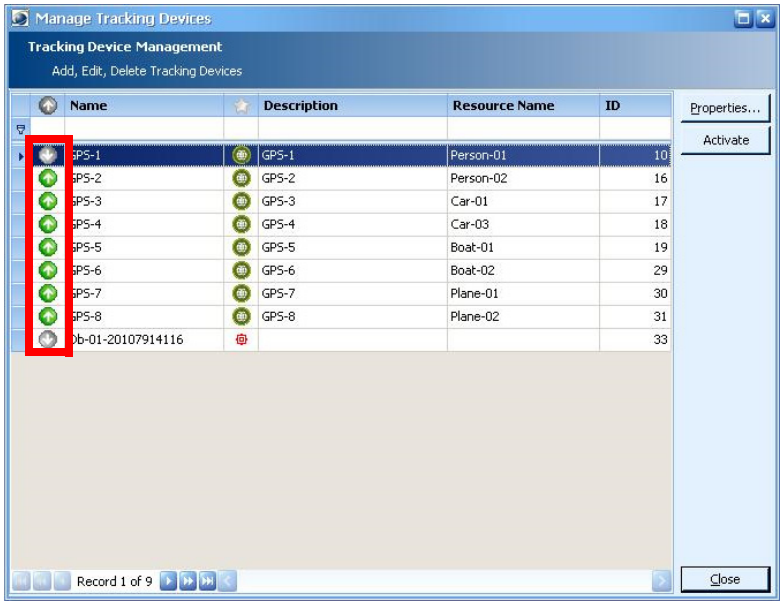
Select the device you want to remove from the list and click the Activate button to enable its use, or the Deactivate button to disable it.

Select the tracking device you want to remove, and click the Deactivate button to disable the device, or the **Activate** button to enable the device.

A confirmation dialog box appears.

Step 3 Click **Yes** to verify the operation.

Tracking devices that have been deactivated appear with a greyed-out icon in the resource list in the Manage Tracking Devices window. Active tracking devices appear with green icons.



CHAPTER 14

Managing Business Logic

In PSOM, business logic is used to raise alerts based on pre-defined conditions and handle post-alert response management actions that should be taken when certain alerts are raised. The business logic templates capture your business processes and requirements for alert creation and response based on the alert's status, schedule, monitoring area or threat level. Business logic allows security personnel to concentrate on execution of planned responses instead of reassessing unfolding situations. It enables optimal response to real-time tasks, reducing vulnerability, and frees the attention of responding individuals so they can better respond to any unplanned turn of events.

PSOM supplies business logic templates that you can customize for your own needs. Once a business logic template is applied to the monitoring tree, it becomes business logic policy.

You can also design and configure business logic rule templates using the Business Logic Rules Designer, and then test and verify their behavior using the Business Logic Designer. The PSOM business logic engine is based on common off-the-shelf (COTS) technology. PSOM uses the advanced business logic engine embedded in the Microsoft .NET Framework version 3.5. This engine was originally built for Microsoft's BizTalk Server and is designed for enterprise use, highly scalable, and extremely flexible.

Note .NET Framework version 3.5 and PowerShell 2.0 are required to use PSOM business logic.

This chapter includes these topics:

- Managing Business Logic using Templates, page 14-1
- Designing Business Logic in the Business Logic Designer, page 14-36
- Testing Business Logic Templates in the Business Logic Designer, page 14-43
- Applying Business Logic Policies, page 14-46
- Importing and Exporting Business Logic Templates, page 14-50
- Using Global System Variables in Business Logic, page 14-51
- Storing PowerShell Scripts for Business Logic, page 14-51

Managing Business Logic using Templates

PSOM supplies business logic templates that you can customize for your own needs. There are several different types of business logic templates:

- Event Business Logic—determines which events from existing alarming systems should be raised as alerts in PSOM. Business logic can be defined so that only certain event types will be raised as alerts, and that different severity and actions will be associated with certain events so that alerts in PSOM have the appropriate severity and associated actions. When applied to the monitoring tree, the default template automatically pulls events from Integration Modules into PSOM as alerts on the corresponding sensors and monitoring areas.
- Alert Business Logic—defines alert response based on the alert's status, schedule, monitoring area, or threat level after an alert has been created.
- Schedule Business Logic—provides a calendar-based execution of business processes. For example, an RSS Alerts activity can be defined to generate alerts from RSS feeds such as severe weather alerts from the Weather Channel or earthquake alerts from U.S. Geological Survey.
- On-Demand Business Logic—enables custom actions to be added to the Operation Console to allow operators to execute functionality such as disarm a sensor or start a group intercom conversation from a monitoring area.
- Alert Status Business Logic—defines business logic that should occur upon status changes for selected alert types.

Inside business logic templates you can add actions (such as sending e-mail or launching programs when certain conditions are met) and you can integrate PowerShell scripts for complex decisions or data correlation with existing systems (such as Microsoft SQL Server or Exchange Server).

Creating an Event Business Logic Template Based on the Default Template

An Event Business Logic template determines which events from an access control device should raise alerts within PSOM, and the appropriate *severity* and *actions* that should be associated with those alerts. For example, when a suspect tampers with a card reader a Critical alert might be raised and a notification e-mail sent to appropriate people; however, in a case involving a sensor that is open too long, a Medium risk alert may be raised without any e-mail notification. Event Business Logic templates can be customized based on the sensor type and location.

You can create a single Event Business Logic template that triggers the same action and assigns the same severity level in PSOM for multiple alert types. Alert types are matched based on the alert description or a customized "event match" string that should correlate to the event's ID or description in the 3rd party system. Matching is performed using exact matching or regular expressions.

A remainder rule enables all unspecified alert types to be handled by this alert, except whatever alerts are specifically excluded using a filter mapping.

The alert generated by Event Business Logic is calculated per sensor, per monitoring area, per business logic policy, per event. For example, assume there is 1 external device that maps to 2 sensors in PSOM, and each sensor resides in 2 monitoring areas (total of 4 monitoring areas containing 2 sensors), and 2 Event Business Logic policies are applied in PSOM related to the device. In this case, 8 alerts will be generated in PSOM for each event generated by the device.

Per device event:

2 sensors x 2 monitoring areas x 2 Business Logic policies = 8 alerts in PSOM

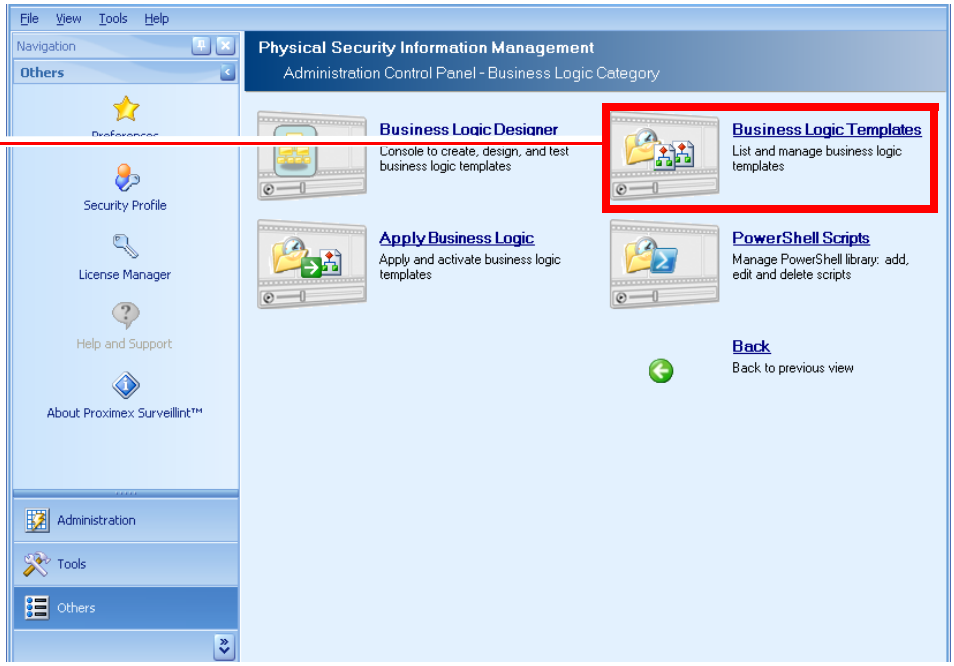
Note

- To create a new business logic template from scratch, see the "Designing Business Logic in the Business Logic Designer" section on page 14-36.
- Because Event Business Logic raises an alert by default on the source sensor, customers of AgentVI or Nextiva may want to use an Event Map Filter activity to specify the target sensor type to be "Camera - Stationary", "Camera - PTZ", or "Camera - Others" so that the alert will be raised on the associated camera sensor instead. See the "Configuring Event Map Filter Properties" section on page 15-51 for details.

To create a new Event Business Logic template based on a default template:

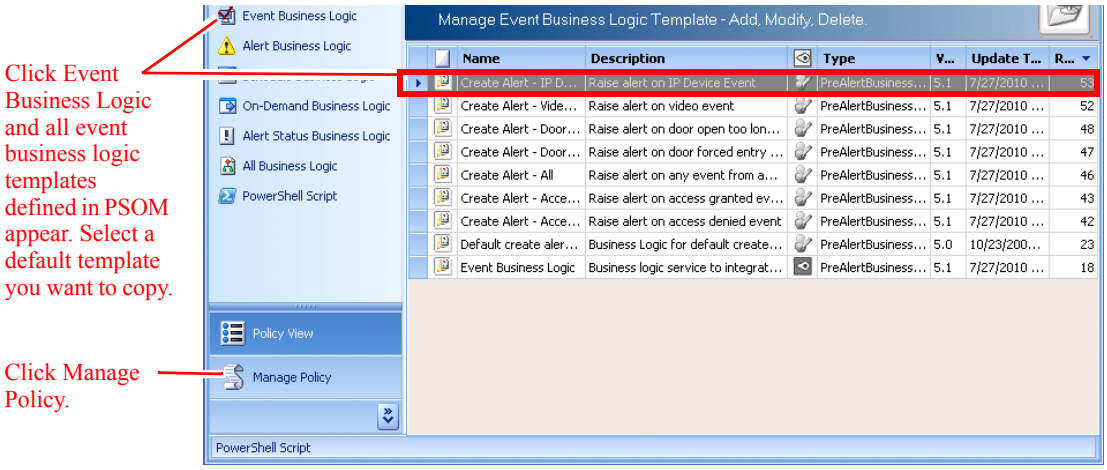
Step 1 Click the **Business Logic** icon in the Administration Console.

Step 2 Click the **Business Logic Templates** icon.

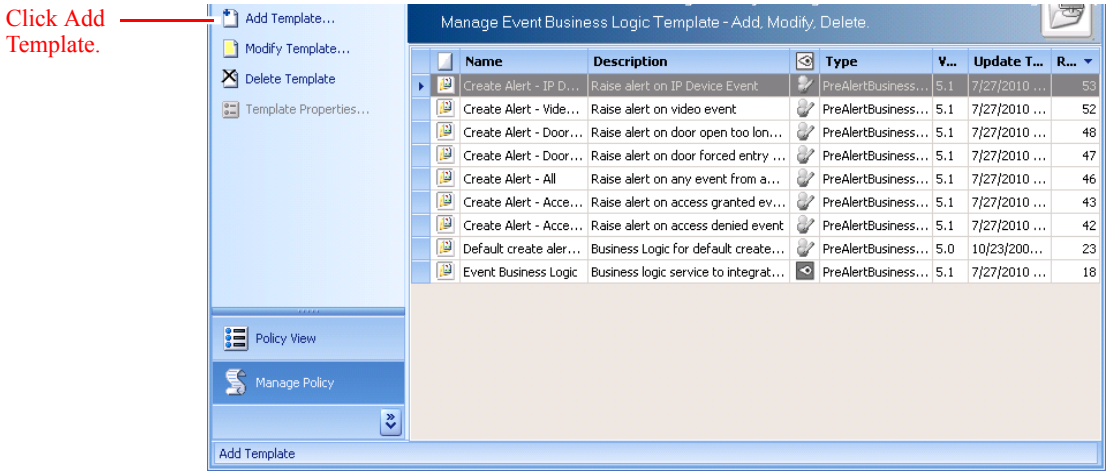


The Business Logic Policy Manager window appears.

Step 3 Click **Event Business Logic** under **Policy View**.

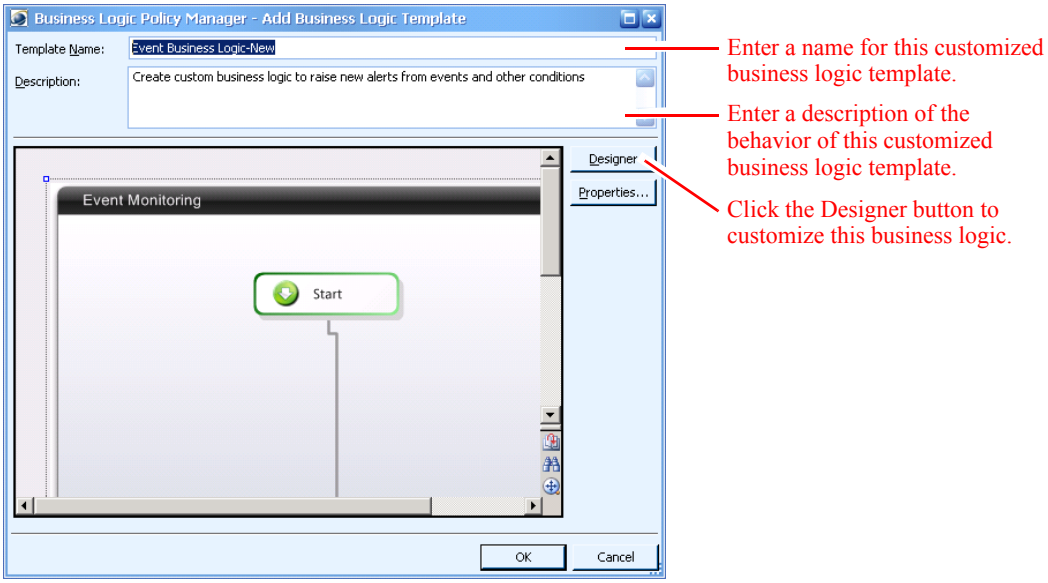


Step 4 Click **Manage Policy** in the left navigation bar.



Step 5 Select the default business logic template you want to copy from the list and click **Add Template**.

The Add Business Logic Template window appears. The bottom of the window shows a graphical read-only representation of the business logic design.



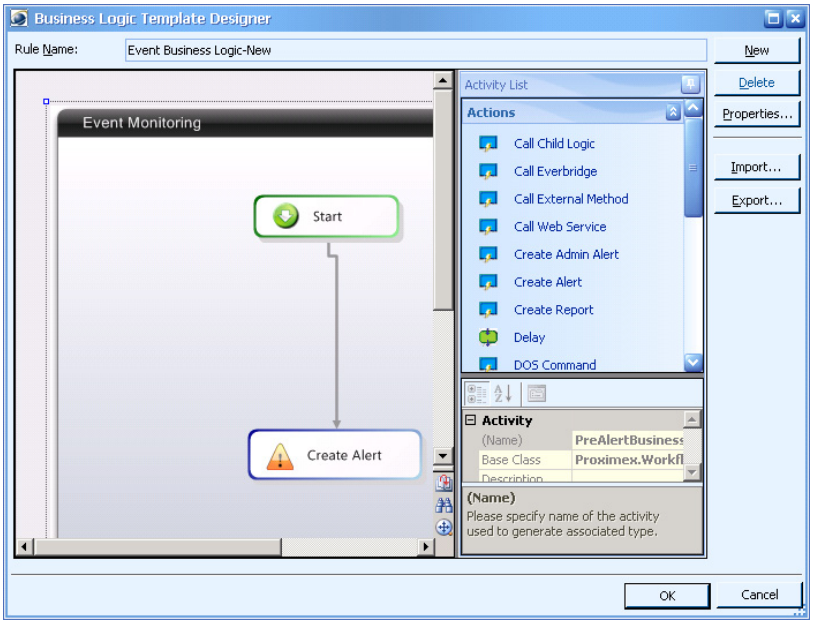
Step 6 In the **Template Name** field, enter a name for this business logic template.

Step 7 In the **Description** field, enter information about the behavior of this business logic template.

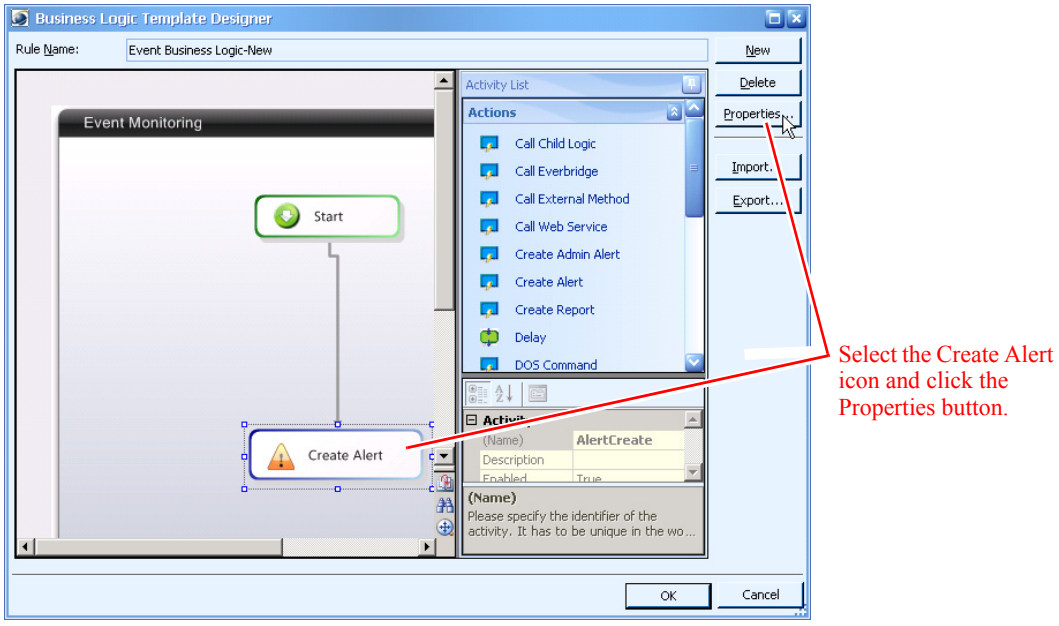
Step 8 As configured, this Event Business Logic simply generates PSOM alerts from raw events generated by an Integration Module.

To customize this business logic to add actions or specify alert severity for generated alerts, click the **Designer** button.

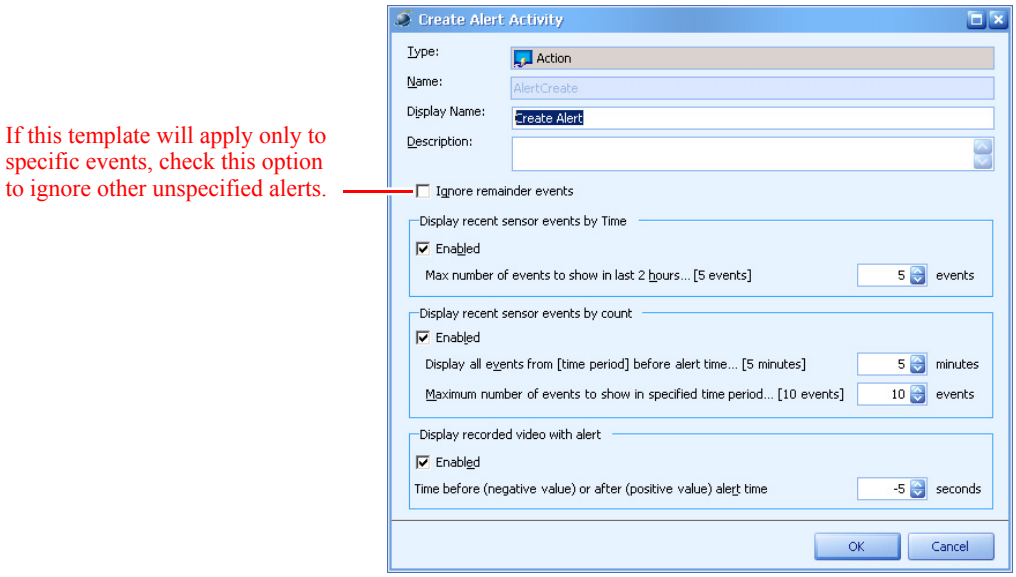
The Business Logic Template Designer window appears.



Step 9 In the business logic design area, select the **Create Alert** icon and click the **Properties** button.



The Create Alert Activity window appears.



Step 10 If you plan to customize the Event Business Logic for specific types of events, and do not want actions to be triggered for other unspecified alert types, click the **Ignore remainder events** option. If you want this business logic to apply to all events generated by the Integration Module, leave this option unchecked.

Step 11 To enable recent events to be displayed based on occurrence time, check the **Enabled** option in the **Display recent sensor events by Time** area. Then set the maximum number of events that can be returned for this type of query.

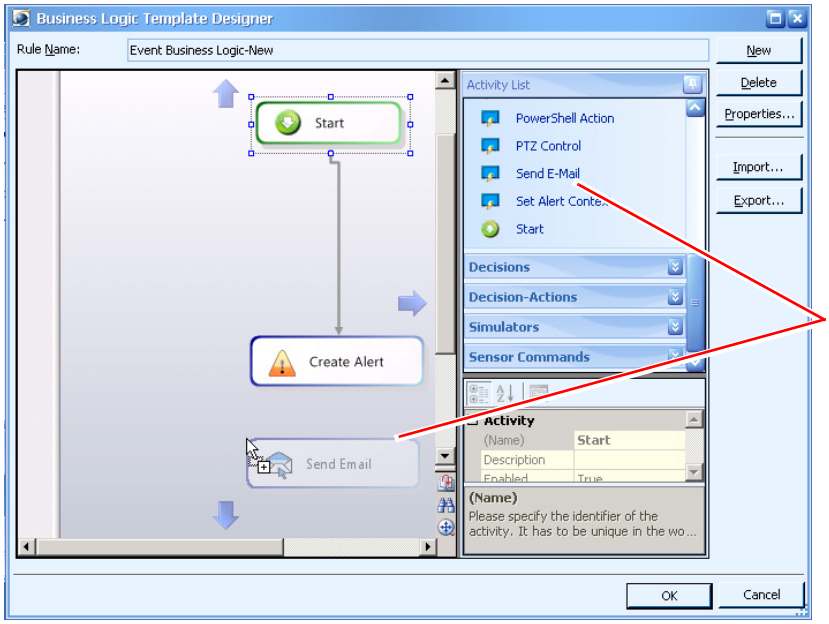
Step 12 To enable recent events to be displayed based on a count of alerts occurring within a specified time frame, check the **Enabled** option in the **Display recent sensor events by count** area. Then set the maximum number of events that can be returned for this type of query.

Step 13 To enable recorded video to be displayed for alerts created by this business logic, check the **Enabled** option in the **Display recorded video with alert** area. Then set the number of seconds of recorded video that will be returned with alerts by this business logic.

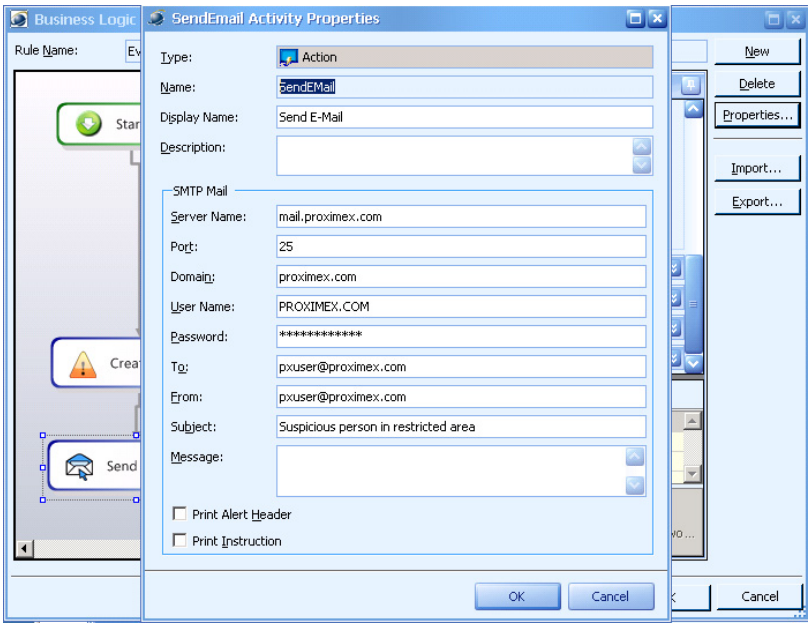
Step 14 Click **OK**.

Step 15 If you want to define an action that should occur when the specified events are raised, you can drag the appropriate action icon to the workspace. For example, to automatically e-mail alert details to certain individuals when this event occurs:

a. Drag a **Send Email** activity to the workspace.



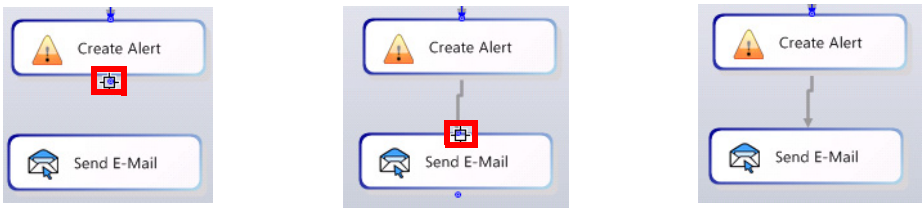
b. Select the **Send Email** icon in the workspace and click the **Properties** button. The Send Email Activity Properties window appears.



c. Complete the fields as necessary and click **OK** to save your changes. See the "Configuring Send Email Properties" section on page 15-31.

d. Connect the **Create Alert** icon to the **Send Email** icon so that the **Send Email** icon will execute after the **Create Alert** icon executes.

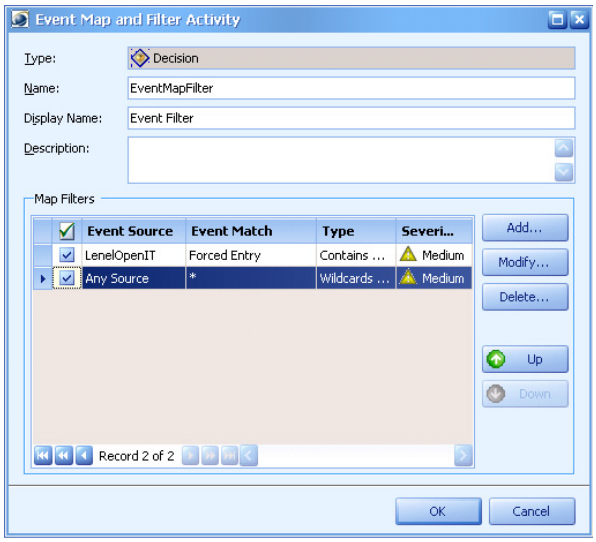
To connect two icons, select the first icon and drag one of the circles on its outside border to the second icon, then release.



Step 16 If you want to specify the events to which this business logic will apply:

a. Expand the **Decisions-Actions** group in the **Activity List**, click the **Event Map Filter** icon, and drag it to the workspace.

b. Select the **Event Map Filter** icon in the workspace and click the **Properties** button. The Event Map and Filter Activity window appears.

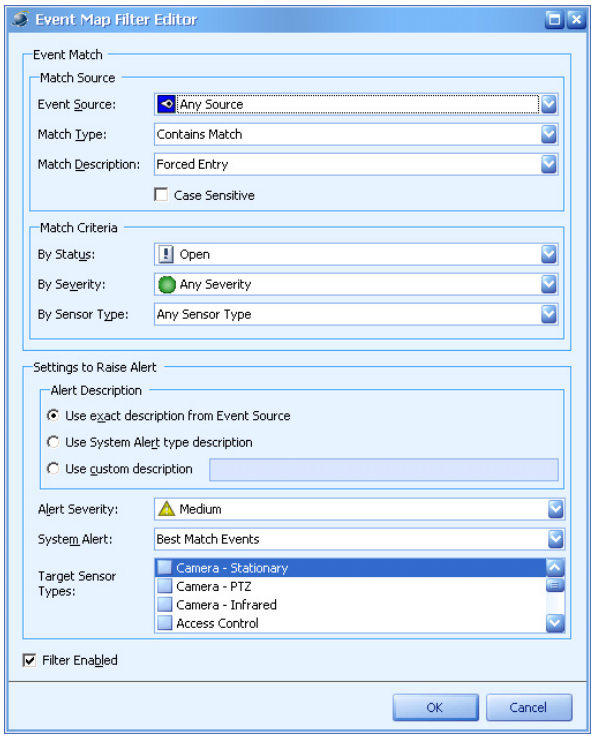


c. Enter a new name for the component in the **Name** field.

d. Enter a new display name for the component in the **Display Name** field.

e. Enter information about the component in the **Description** field.

f. Focus the business logic on a specific event by clicking the **Add** button and creating a new filter for that event.



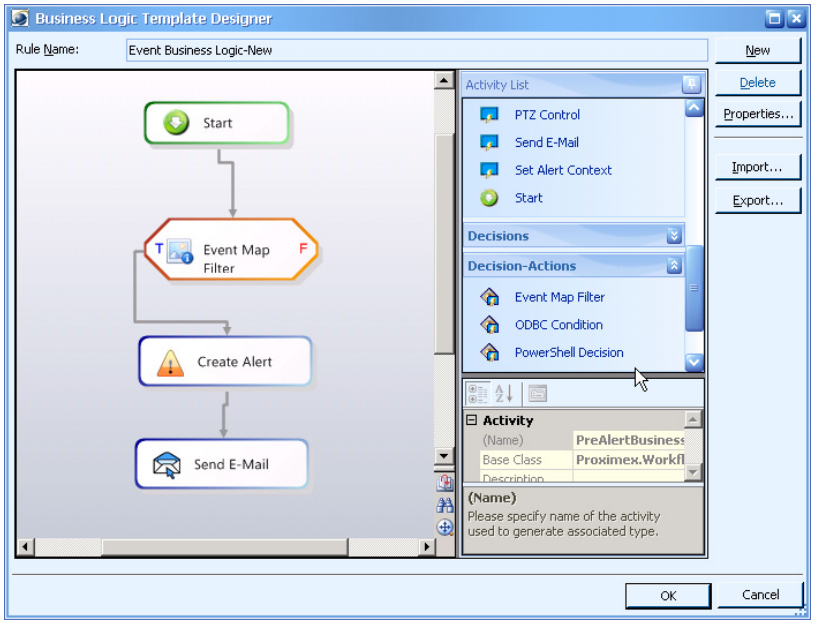
See the "Configuring Event Map Filter Properties" section on page 15-51 for how to define filters that specify certain events to which this business logic should apply.

g. Click **OK** to save your changes.

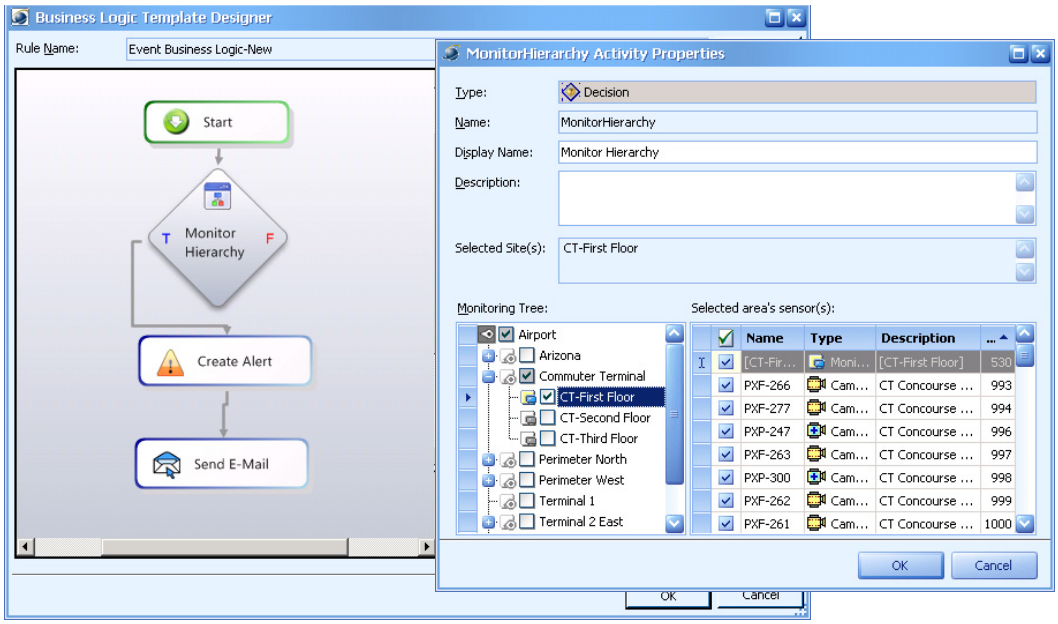
h. Delete the connection between the **Start** icon and the **CreateAlert** icon by selecting the connection line and pressing the **Delete** key.

i. Connect the **Start** icon to the top of the **Event Map Filter** icon.

j. Connect the **True** segment of the **Event Map Filter** icon to the top of the **Create Alert** icon.



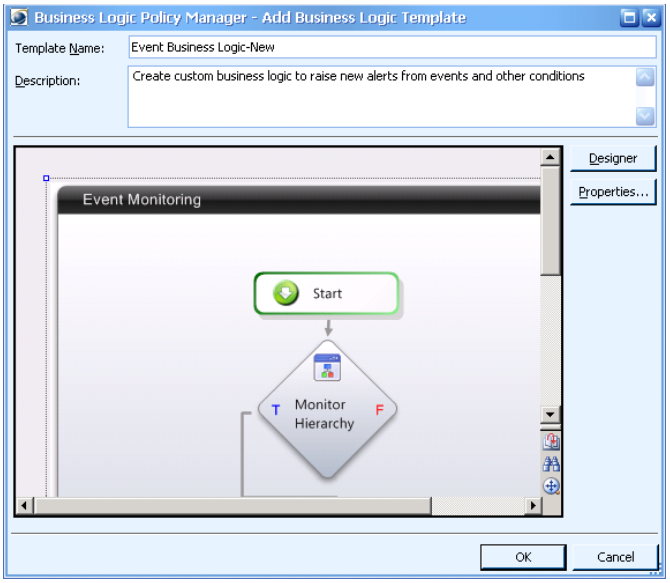
Step 17 If you want to only generate alerts when the sensor is in a monitoring area in the monitoring hierarchy, add the **Monitor Hierarchy** icon to the workspace in between the **Start** icon and **Create Alert** icon. Then set its properties so that the particular monitoring area is selected; for example, CT-First Floor.



Step 18 Once you've added and connected all icons for your modified business logic, click **OK** in the Business Logic Template Designer window.

Step 19 Your business logic will be verified. If it is sound logic, you will be notified. Click **OK** to confirm.

The Business Logic Policy Manager window re-appears showing your customized logic.



Step 20 Click **OK** to save your changes.

Step 21 Apply your business logic template to expose the commands to the Operation Console. See the "Applying Business Logic Policies" section on page 14-46.

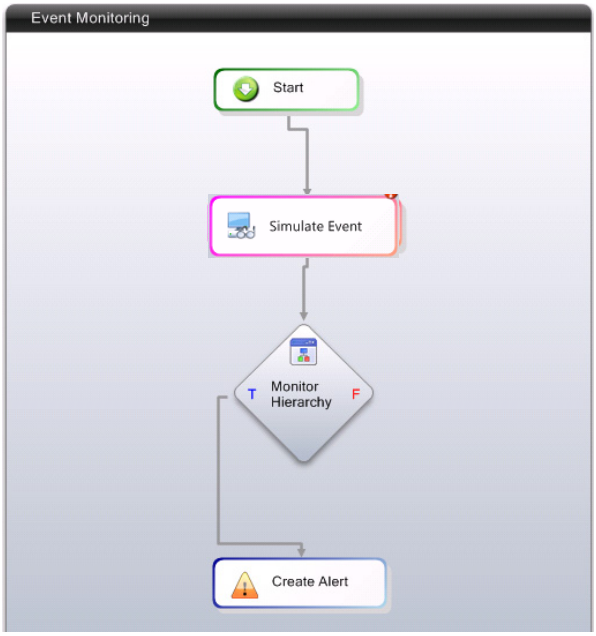
Applying Event Monitoring Business Logic in your Environment

You can apply as many Event Monitoring business logic templates as you need. However the recommended optimal number of applied business logic templates is less than 10 templates at a time. When you deploy more than 10 templates at the same time, it can degrade the performance of the event monitoring process.

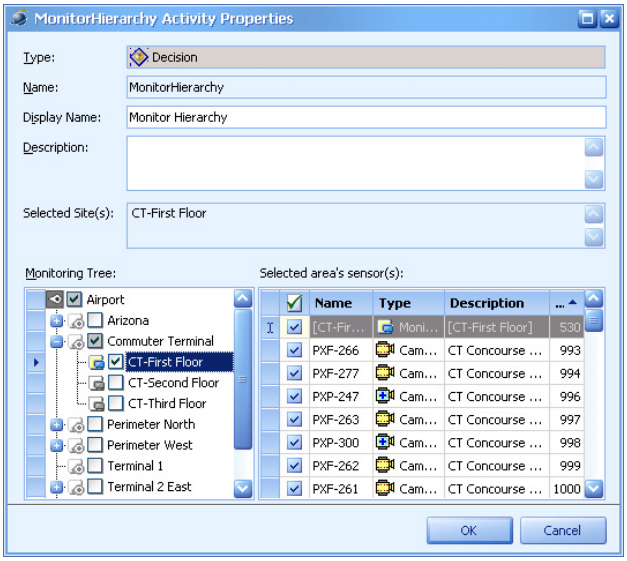
Caution When you have multiple Event Monitoring business logic templates deployed, each applied template will run for every event polled from any of the connected Integration Module. This means that if you have "Create Alert" activity in more than one of these deployed templates, and if these "Create Alert" activities are not logically mutually exclusive from each other; you may get duplicate alerts in PSOM.

Restricting Event Monitoring Business Logic to Monitoring Areas or Zones

By default all Event Monitoring business logic templates are applied globally to the Global Zone. However there are situations that you want to restrict a particular Event Monitoring business logic to a particular section of the hierarchy. In these cases, you can use the Monitor Hierarchy Decision to restrict the business logic to a particular zone or area in the monitoring hierarchy.

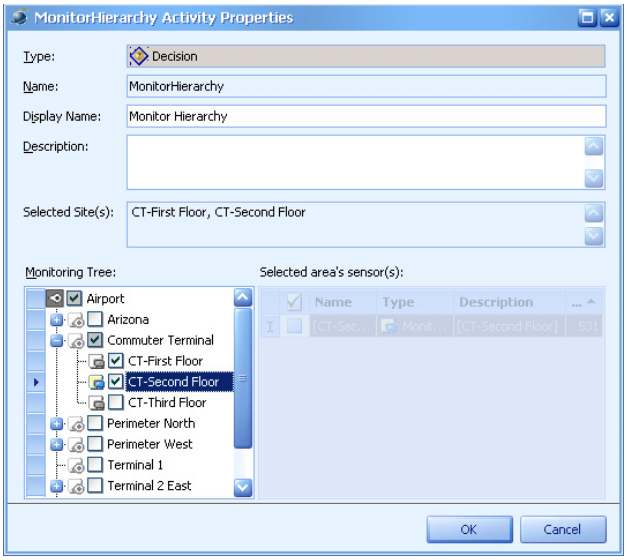


In the Monitor Hierarchy activity you specify the area or zone to which you want this business logic template applied.



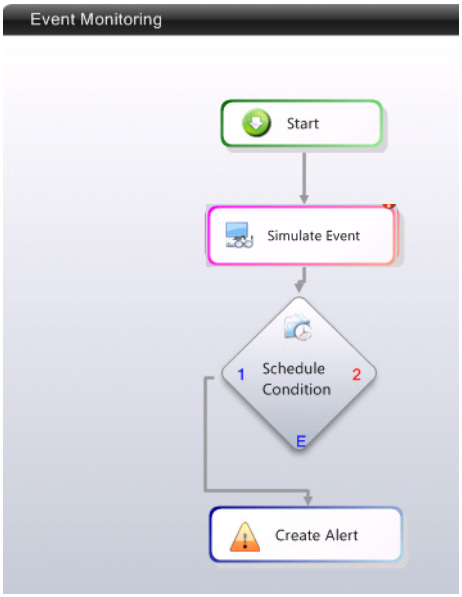
In the above example, the Event Monitoring business logic is now restricted only to monitoring area “CT-First Floor”.

You can also restrict an Event Monitoring business logic template to multiple hierarchies. The following example restricts the Event Monitoring business logic to both “CT-First Floor” and “CT-Second Floor”.

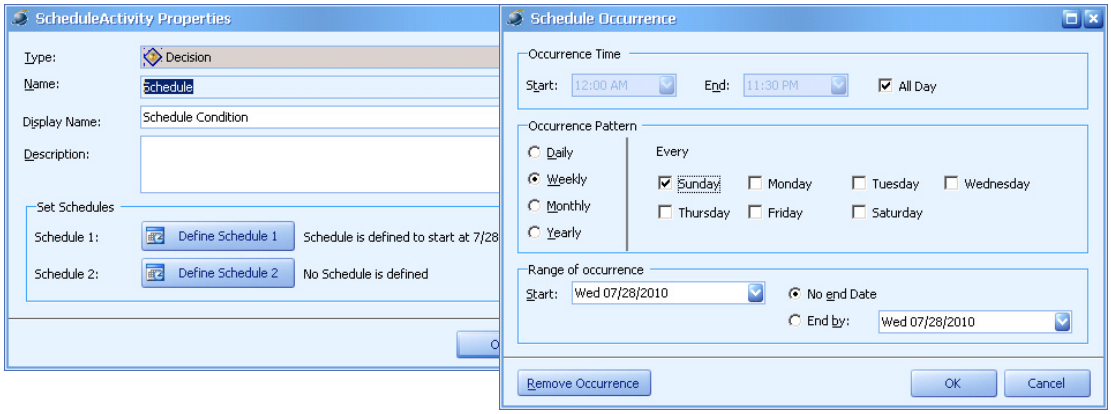


Restricting Event Monitoring Business Logic to a Schedule

By default all Event Monitoring business logic templates are applied globally and run continuously regardless of date and time. However there are situations that you may want to restrict a particular business logic template to a particular schedule. In these cases, you can use the Schedule Condition activity to restrict the Event Monitoring business logic to a particular schedule.



Inside the Schedule Condition activity, you can specify the schedule that you want applied to this business logic template.

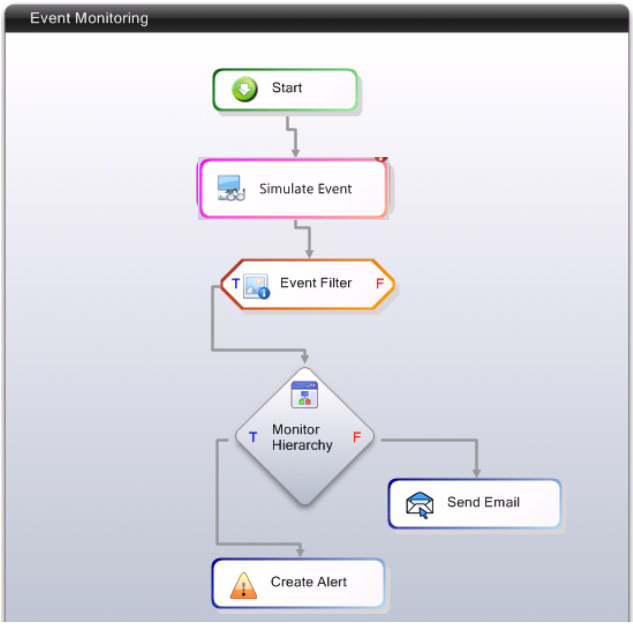


The above example shows the schedule is set to every Sunday. Therefore only events that happen on Sundays will be pulled into PSOM as alerts.

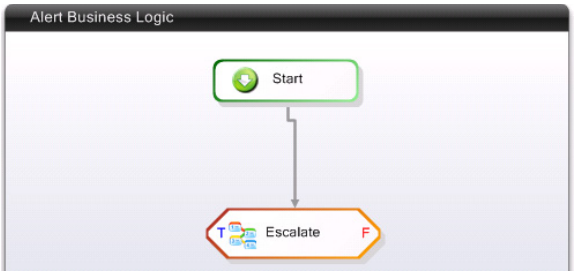
Note Do not confuse the Schedule Condition activity with the Schedule Business Logic type. The Schedule Condition activity is only an activity that determines whether the current input time is within the specified schedule. The Schedule Business Logic will run at the specified schedule repetitively.

Taking Actions Before and After Alert Creation

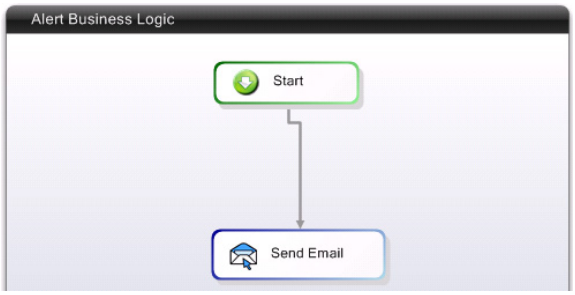
You can execute actions before alert creation in an Event Monitoring business logic template, such as send an email, invoke a remote command, or run a PowerShell script. In the following example, the Send Email activity sends an email notification when an event does not fall into the specified monitor hierarchy.



To execute actions after an alert has been created, you need to use the Alert Business Logic template to deploy these actions. For example, escalate an alert to certain personnel after the alert has been created.



Or send email notifications after an alert has been created.



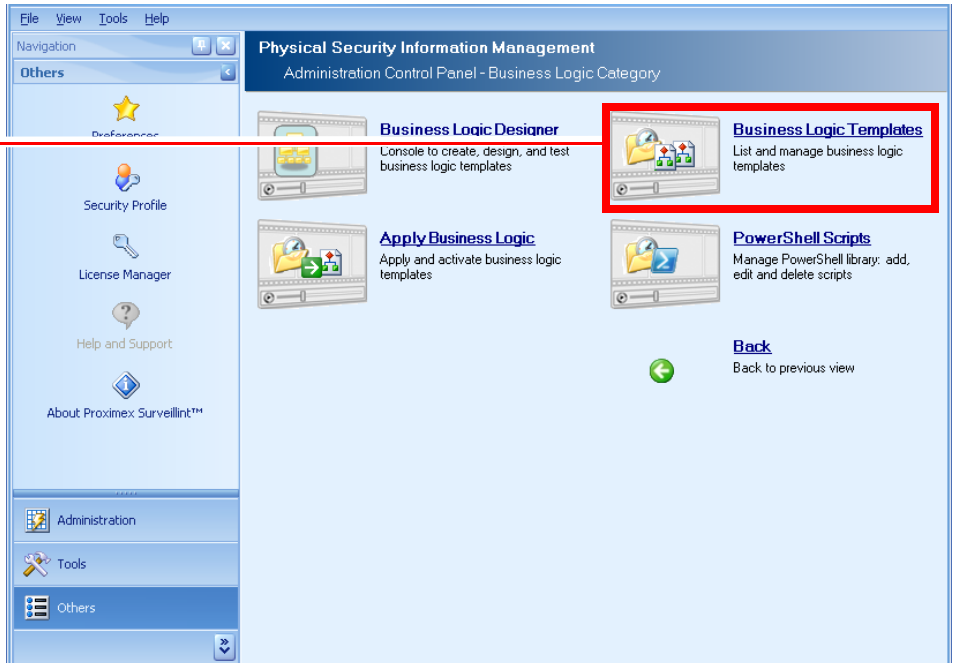
Creating an Alert Business Logic Template Based on the Default Template

An Alert Business Logic template determines the specific actions, decisions, and activities that should be occur when alerts are raised in PSOM. The default Alert Business Logic template contains only a **Start** icon.

To create a new Alert Business Logic template based on a default template:

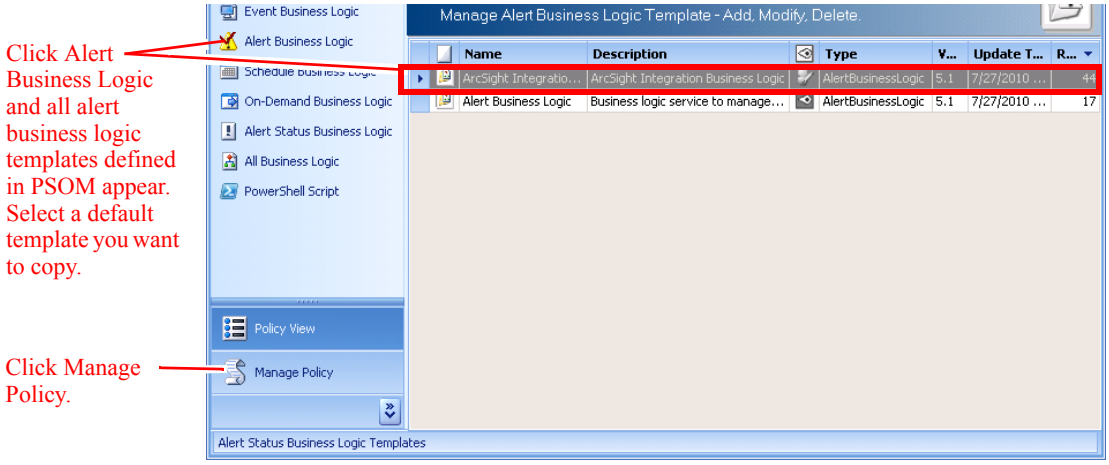
Step 1 Click the **Business Logic** icon in the Administration Console.

Step 2 Click the **Business Logic Templates** icon.

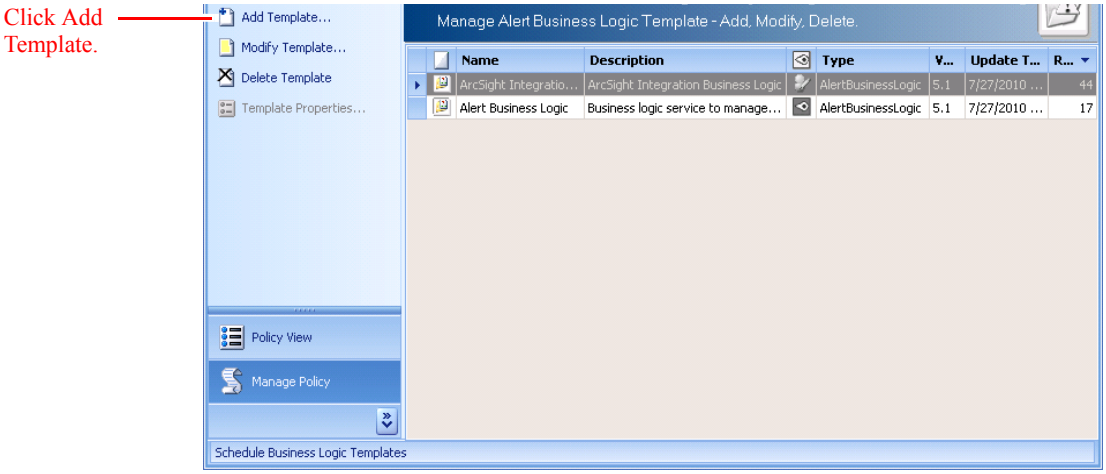


The Business Logic Policy Manager window appears.

Step 3 Click **Alert Business Logic** under **Policy View**.

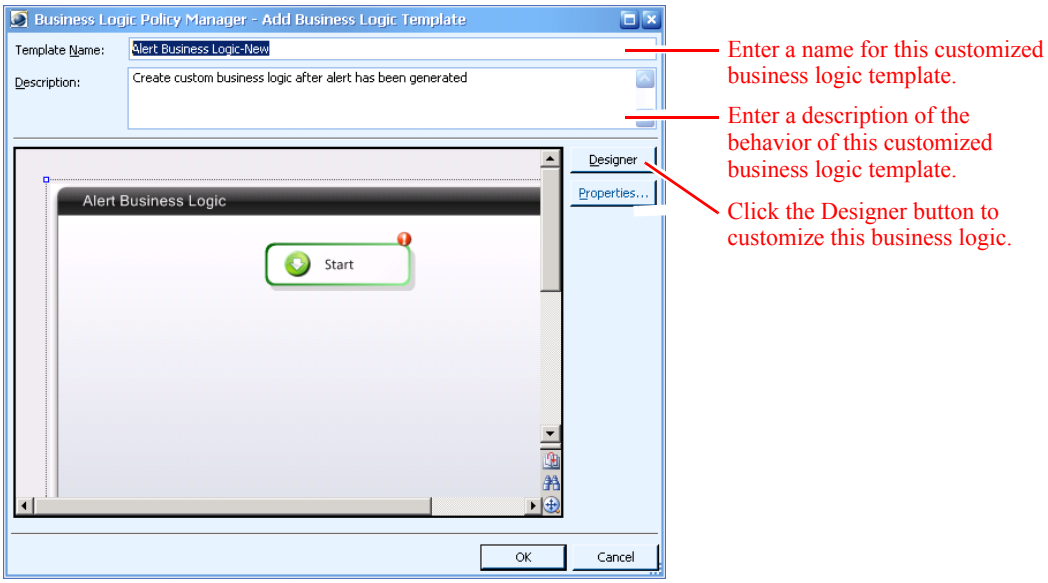


Step 4 Click **Manage Policy** in the left navigation bar.



Step 5 Select the default business logic template you want to copy from the list and click **Add Template**.

The Add Business Logic Template window appears. The bottom of the window shows a graphical read-only representation of the business logic design.



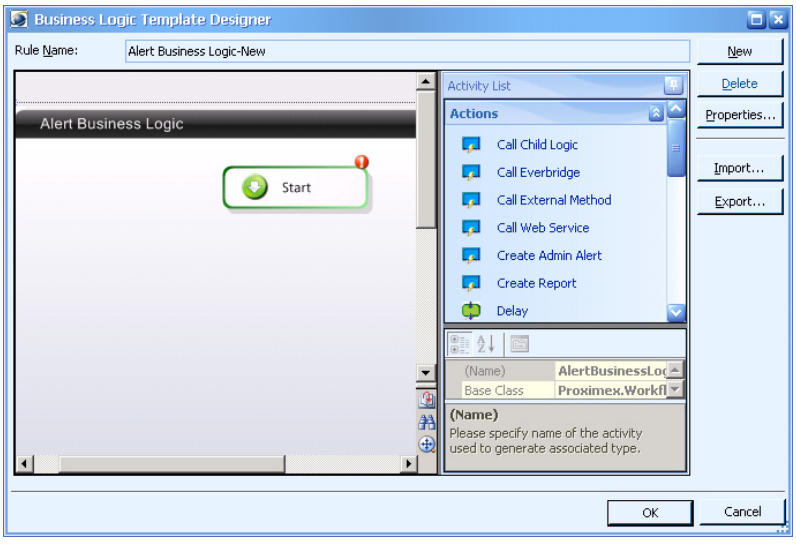
Step 6 In the **Template Name** field, enter a name for this business logic template.

Step 7 In the **Description** field, enter information about the behavior of this business logic template.

Step 8 As configured, this Alert Business Logic simply starts an empty business logic action once an alert has been generated in PSOM.

To customize this business logic to add actions or specify alert severity for generated alerts, click the **Designer** button.

The Business Logic Template Designer window appears.



Step 9 Add action, decision, and sensor icons to your business logic as needed to respond to raised alerts. For example, you could add an **Alert Condition** icon to determine whether a Critical alert has occurred, and if so, use a **Send Email** icon to alert authorities.

Step 10 Once you've added and connected all icons for your modified business logic, click **OK** in the Business Logic Template Designer window.

Step 11 Your business logic will be verified. If it is sound logic, you will be notified. Click **OK** to confirm.

The Business Logic Policy Manager window re-appears showing your customized logic.

Step 12 Click **OK** to save your changes.

Step 13 Apply your business logic template to expose the commands to the Operation Console. See the "Applying Business Logic Policies" section on page 14-46.

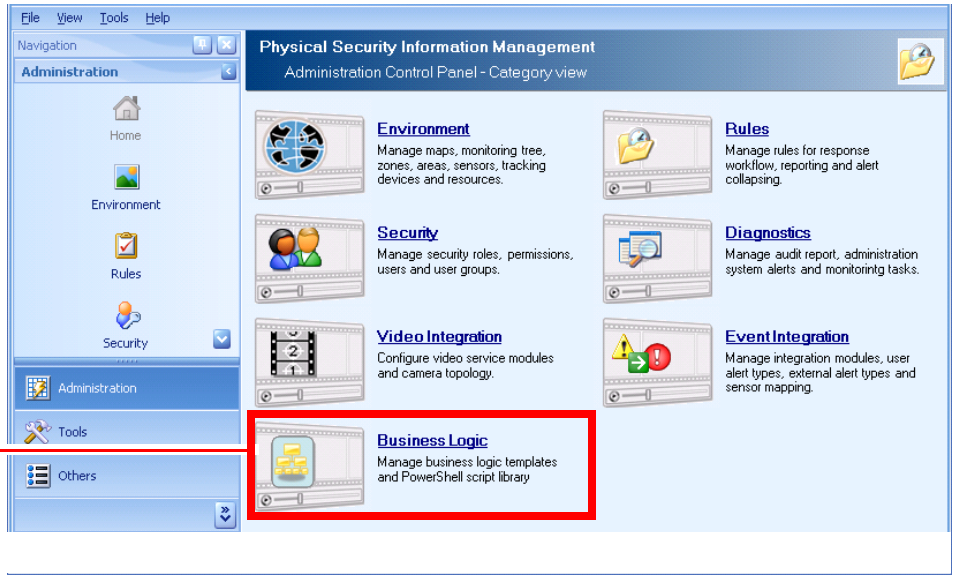
Creating a Schedule Business Logic Template Based on the Default Template

A Schedule Business Logic template provides a calendar-based execution of business processes. For example, an RSS Alerts activity can be defined to generate alerts from RSS feeds such as severe weather alerts from the Weather Channel or earthquake alerts from U.S. Geological Survey.

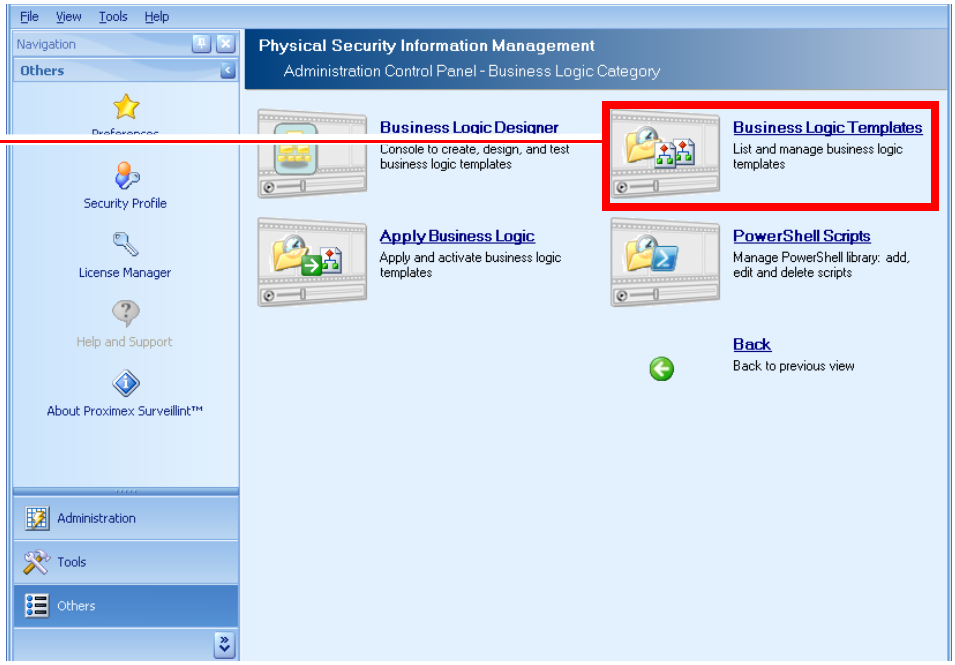
Note To create a new business logic template from scratch, see the "Designing Business Logic in the Business Logic Designer" section on page 14-36.

To create a new Schedule Business Logic template based on a default template:

Step 1 Click the **Business Logic** icon in the Administration Console.

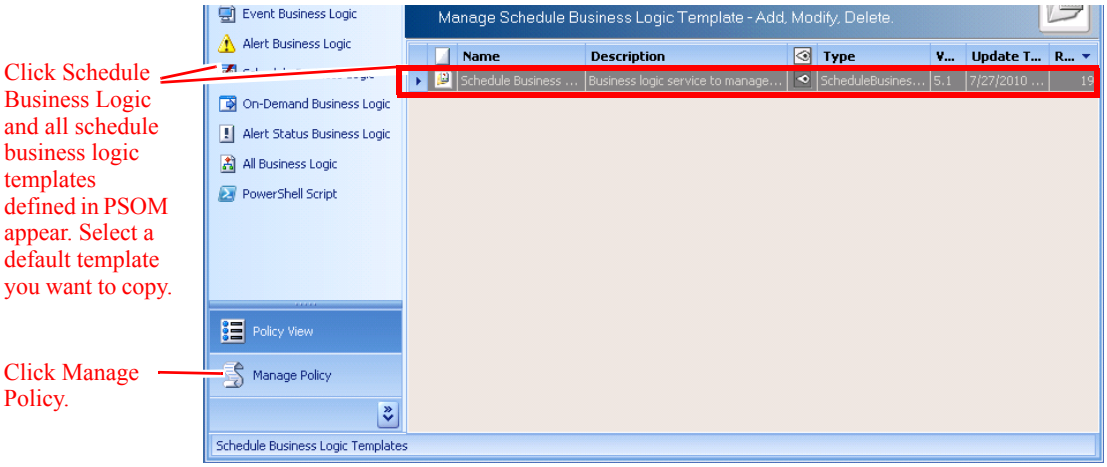


Step 2 Click the **Business Logic Templates** icon.

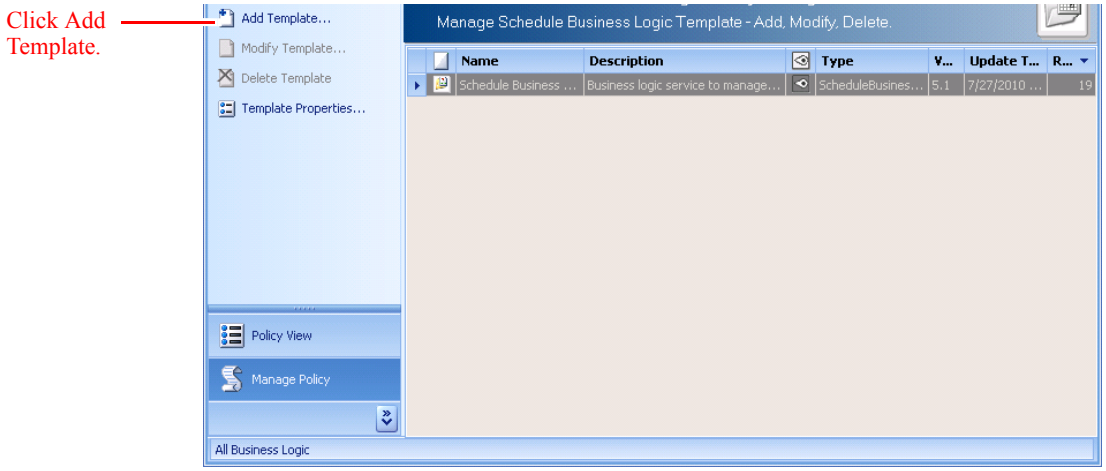


The Business Logic Policy Manager window appears.

Step 3 Click **Schedule Business Logic** under **Policy View**.

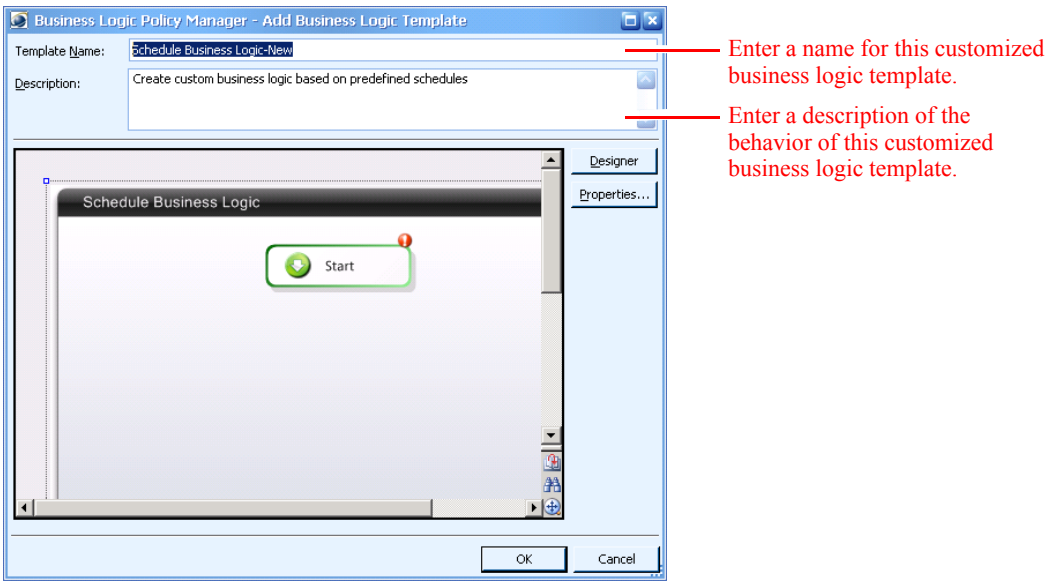


Step 4 Click **Manage Policy** in the left navigation bar.



Step 5 Select the default business logic template you want to copy from the list and click **Add Template**.

The Add Business Logic Template window appears. The bottom of the window shows a graphical read-only representation of the business logic design.

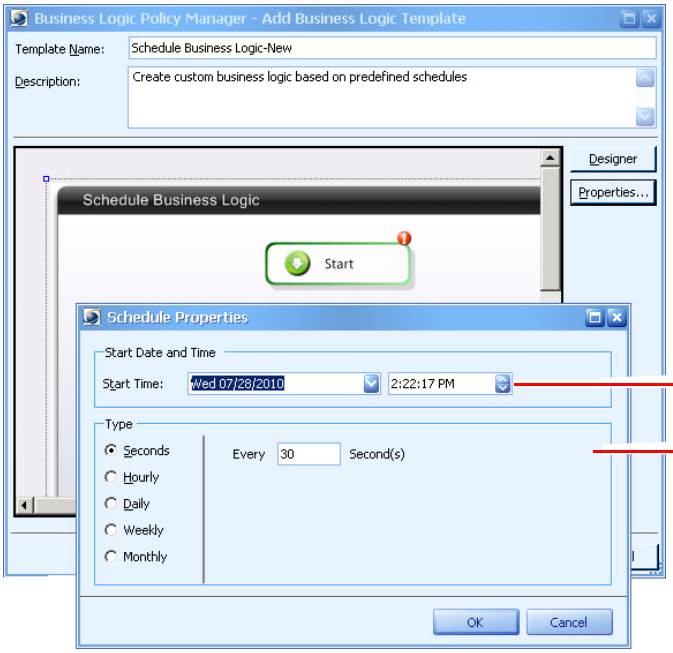


Step 6 In the **Template Name** field, enter a name for this business logic template.

Step 7 In the **Description** field, enter information about the behavior of this business logic template.

Step 8 Click **Properties** to set scheduling for this business logic template.

The Schedule Properties window appears.



Step 9 Choose when you want this business logic template to begin executing from the **Start Date and Time** area.

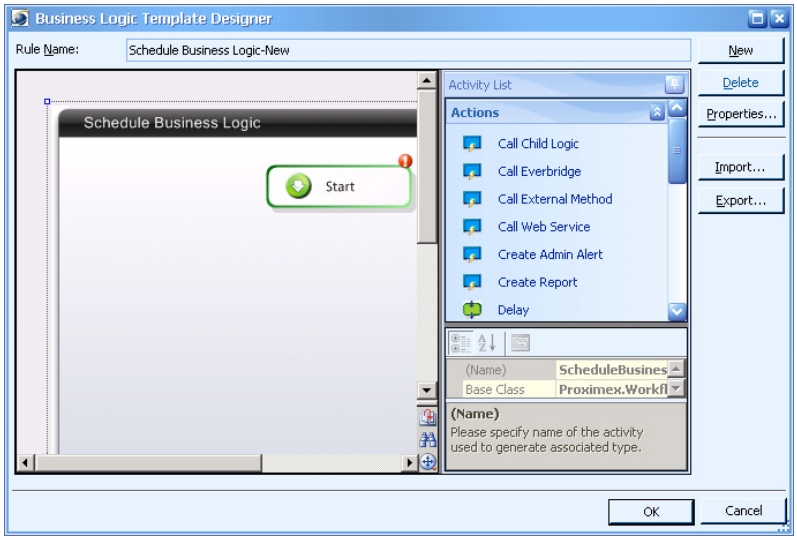
Step 10 Configure how often this template should run by choosing **Second**, **Hourly**, or **Daily** from the **Type** area, and then entering the number of time units that should pass between executions of this template.

Step 11 Click **OK** to save your schedule settings.

Step 12 As configured, this Schedule Business Logic simply starts empty business logic.

To customize this business logic to add actions that should occur on a scheduled basis, click the **Designer** button.

The Business Logic Template Designer window appears.



Step 13 Add action, decision, and sensor icons to your business logic as needed to perform necessary functions on a scheduled basis. Some ideas include:

- Send Email
- Execute a PowerShell script command
- Poll an RSS feed for earthquake alerts
- Close doors at scheduled times

Step 14 Once you've added and connected all icons for your modified business logic, click **OK** in the Business Logic Template Designer window.

Step 15 Your business logic will be verified. If it is sound logic, you will be notified. Click **OK** to confirm.

The Business Logic Policy Manager window re-appears showing your customized logic.

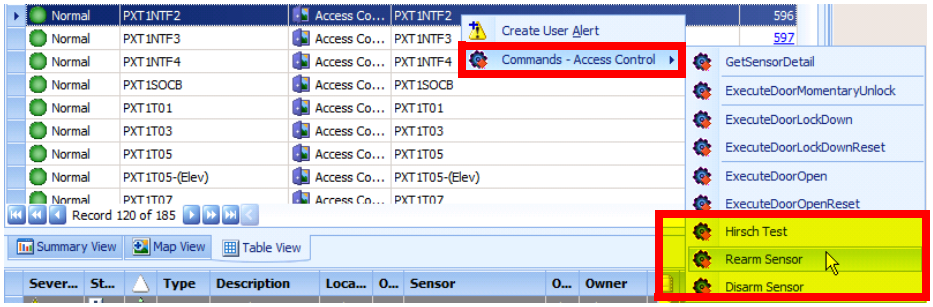
Step 16 Click **OK** to save your changes.

Step 17 Apply your business logic template to expose the commands to the Operation Console. See the "Applying Business Logic Policies" section on page 14-46.

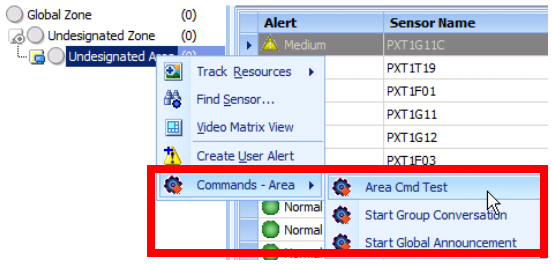
Creating an On-Demand Business Logic Template Based on the Default Template

An On-Demand Business Logic template provides access to custom functionality from the Operation Console. For example, an operator can right-click a door sensor and disarm it, or right-click a monitoring area and start a group intercom conversation. You can define on-demand business logic for:

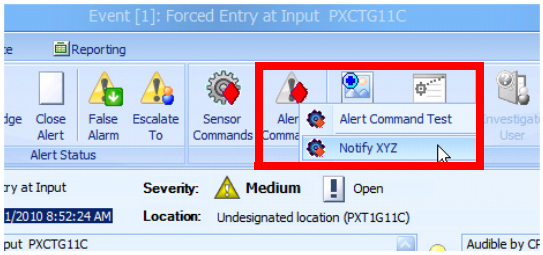
- Sensors—The custom action is added to the right-click menu for the sensor icon on a map, or the sensor name in a list, or from the **Sensor Commands** menu in the Alert Details window. You must specify the type of sensor when defining sensor-based on-demand business logic.



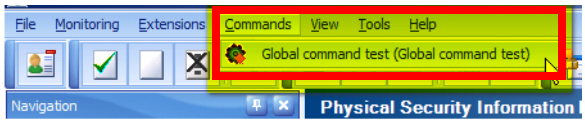
- Monitoring Areas and Zones—The custom action is added to the right-click menu for the monitoring area or zone in the Operation Console.



- Alert Details—The custom action is added to the **Alert Commands** menu in the Alert Details window.



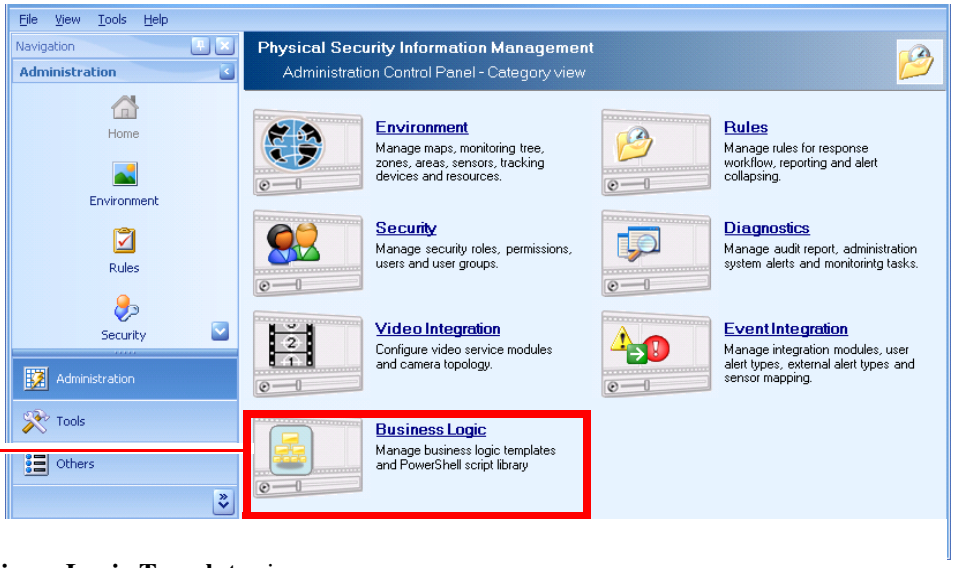
- Global Commands—The action is added to the **Commands** menu in the Operation Console window and applies to the entire PSOM environment.



Note To create a new business logic template from scratch, see the "Designing Business Logic in the Business Logic Designer" section on page 14-36.

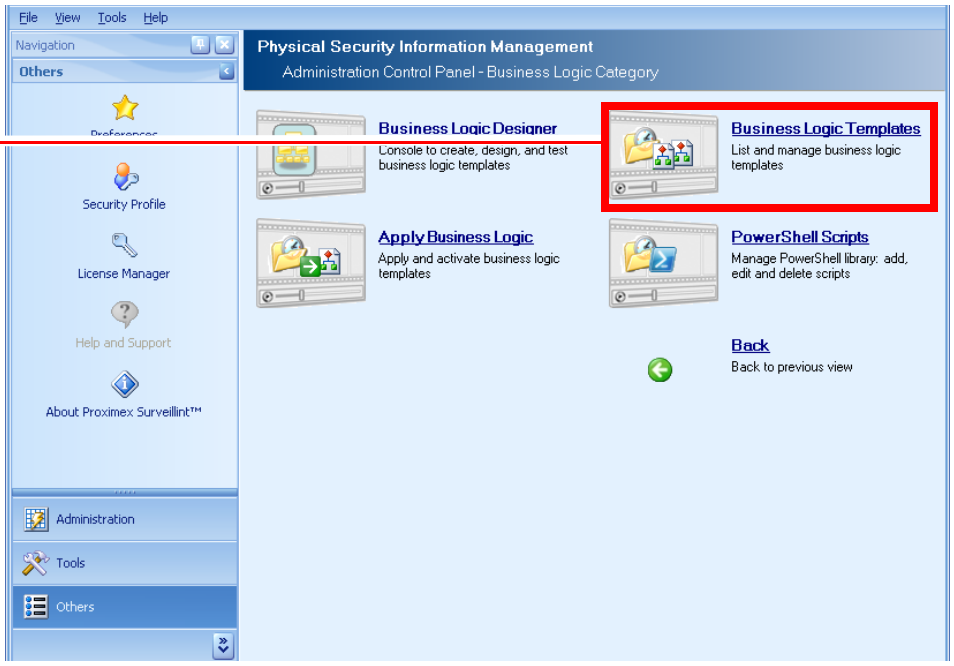
To create a new On-Demand Business Logic template based on a default template:

Step 1 Click the **Business Logic** icon in the Administration Console.



Click the Business Logic icon.

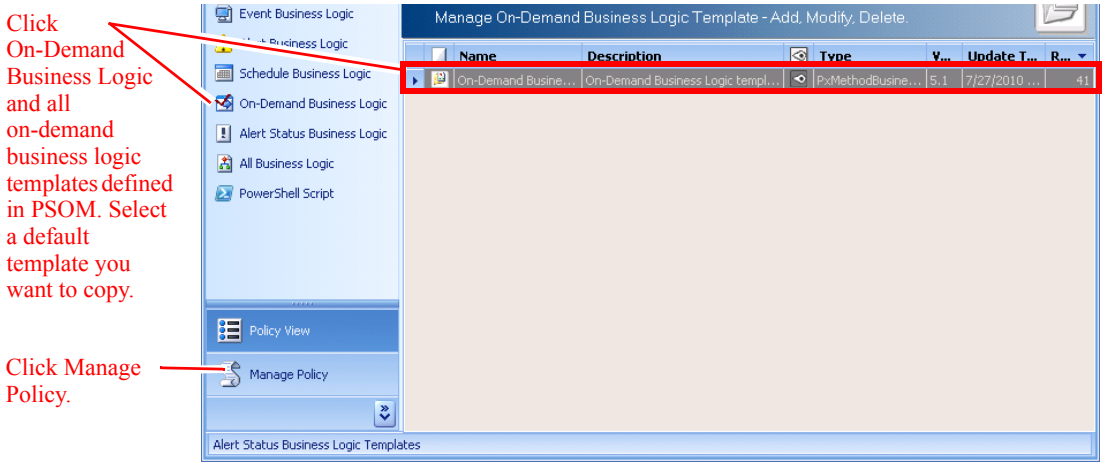
Step 2 Click the **Business Logic Templates** icon.



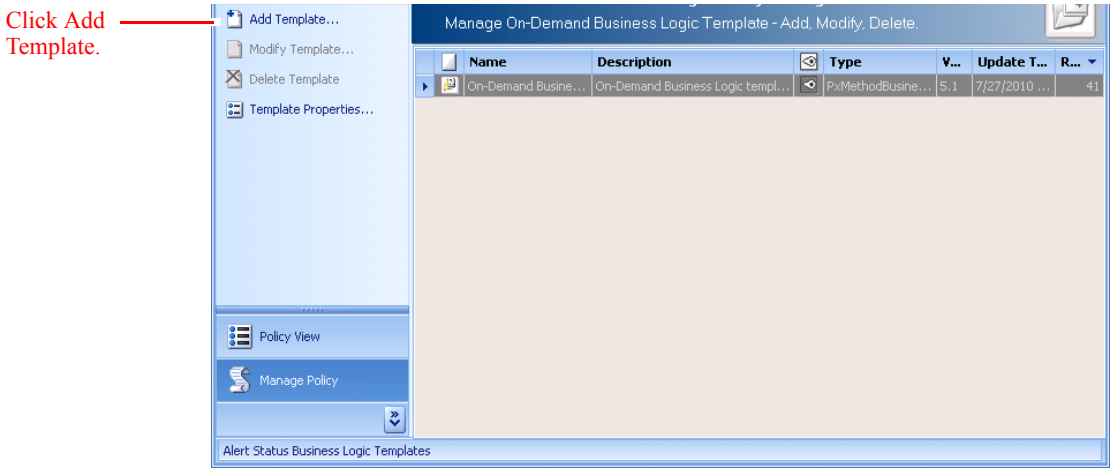
Click the Business Logic Templates icon.

The Business Logic Policy Manager window appears.

Step 3 Click **On-Demand Business Logic** under **Policy View**.

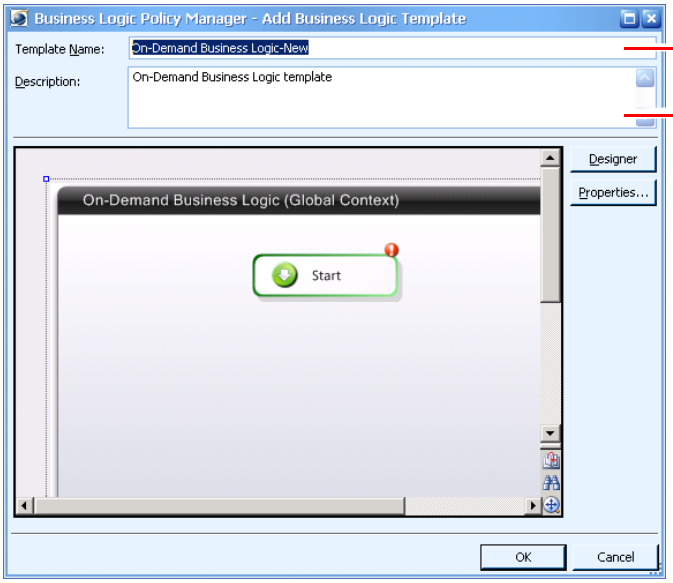


Step 4 Click **Manage Policy** in the left navigation bar.



Step 5 Select the default business logic template you want to copy from the list and click **Add Template**.

The Add Business Logic Template window appears. The bottom of the window shows a graphical read-only representation of the business logic design.

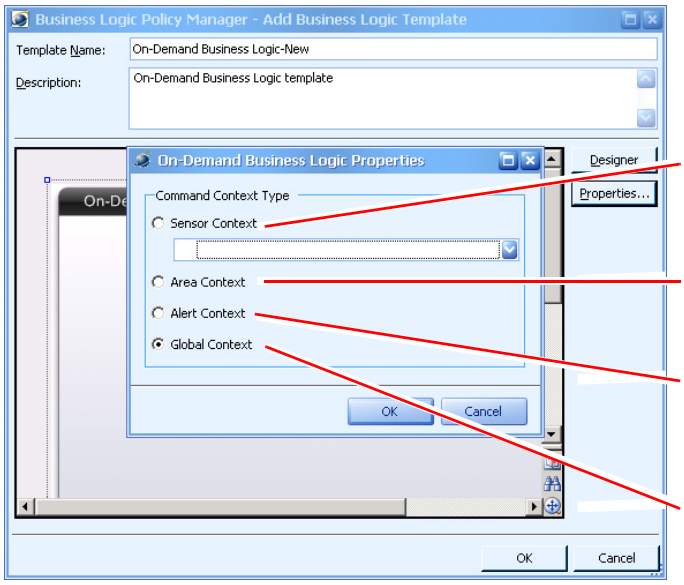


Step 6 In the **Template Name** field, enter a name for this business logic template. The name is what appears as the "action" or command to be performed in the right-click menu.

Step 7 In the **Description** field, enter information about the behavior of this business logic template. The description provided here is the same as the "action" or command description.

Step 8 Click **Properties** to define actions for this business logic template.

The On-Demand Business Logic Properties window appears.



Step 9 Choose what type of on-demand business logic you want to define:

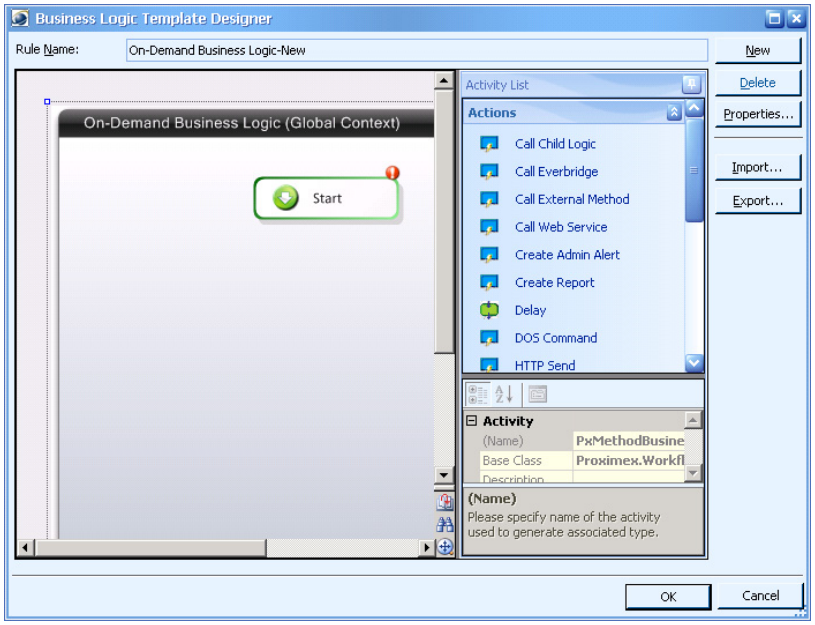
- To define an action that appears when you right-click a sensor icon or name, select **Sensor Context** and choose the sensor type from the field below.

- To define an action that appears when you right-click a monitoring area or zone, select **Area Context**.
- To define an action that appears in the **Alert Commands** menu of the Alert Details window, select **Alert Context**.
- To define an action that appears in the **Commands** menu of the Operation Console, select **Global Context**.

Step 10 Click **OK** to save your on-demand settings.

Step 11 As configured, this On-Demand Business Logic simply starts empty business logic. To customize this business logic to add actions that should occur on-demand, click the **Designer** button.

The Business Logic Template Designer window appears.



Step 12 Add a PowerShell script command to enable the action you want to appear in the right-click menu. For example, add a script to close all doors within a monitoring area by passing the monitoring area context to the Close Door activity, and configuring the Close Door activity to focus on the "Current Hierarchy."

The On-Demand Business Logic leverages the PxMethod funtionality differently depending on the type of context selected for the business logic:

- Sensor contexts—The PxSensor parameter is exposed with a parameter name of Sensor and parameter type of Proximex.Common.Objects.PxSensor.
- Monitoring area and zone contexts—The AreaID or ZoneID parameter is exposed with a parameter name of ZoneOrArea and parameter type of Proximex.Common.Objects.PxZoneAreaContext.
- Alert contexts—The AlertID parameter is exposed with a parameter name of DbAlert and parameter type of Proximex.Common.Database.PxAlert_Header.
- Global contexts—No parameters are exposed to callers.

The following contextual data is available for business logic activities:

- Alert-based commands—Alert object ($pxAlert in PowerShell)
- Area-based commands—context AreaID key and PxSensor category

- Sensor-based commands—context SensorID key and PxSensor category
- All commands—PxMethodCallerContextValue in the root container ($pxMethodCaller in PowerShell)

Some actions you might want to perform to interact with the context include:

- Retrieving the invoke user name and location from the caller context object.

```
$pxLogger.logWarn("Invoked by user " + $pxMethodCaller.InvokeUserName + " from
workstation " + $pxMethodCaller.InvokeHost)
```

- Retrieving the area ID from a monitoring area-based context:

```
$areaID = $pxContext.findContextObject("PxSensor", "AreaID")
```

- Retrieving the sensor ID from a sensor-based context:

```
$sensorID = $pxContext.findContextObject("PxSensor", "SensorID")
```

- Retrieving alert information from an alert-based context:

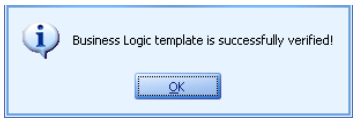
```
$currentAlertID = $pxAlert.AlertID
$currentAlertDescription = $pxAlert.AlertDescription
```

Step 13 Once you've added and connected all icons for your modified business logic, click **OK** in the Business Logic Template Designer window.

Note To simulate and test on-demand business logic, you must add one of the following activity icons to simulate context:

- For alert contexts, use a **Simulate Alert** activity icon.
- For sensor and monitoring area/zone contexts, use a **Simulate Context Activity** icon to simulate a particular sensor type, a particular monitoring area or zone, or a global context (e.g., no context).

Step 14 Your business logic will be verified. If it is sound logic, you will be notified. Click **OK** to confirm.



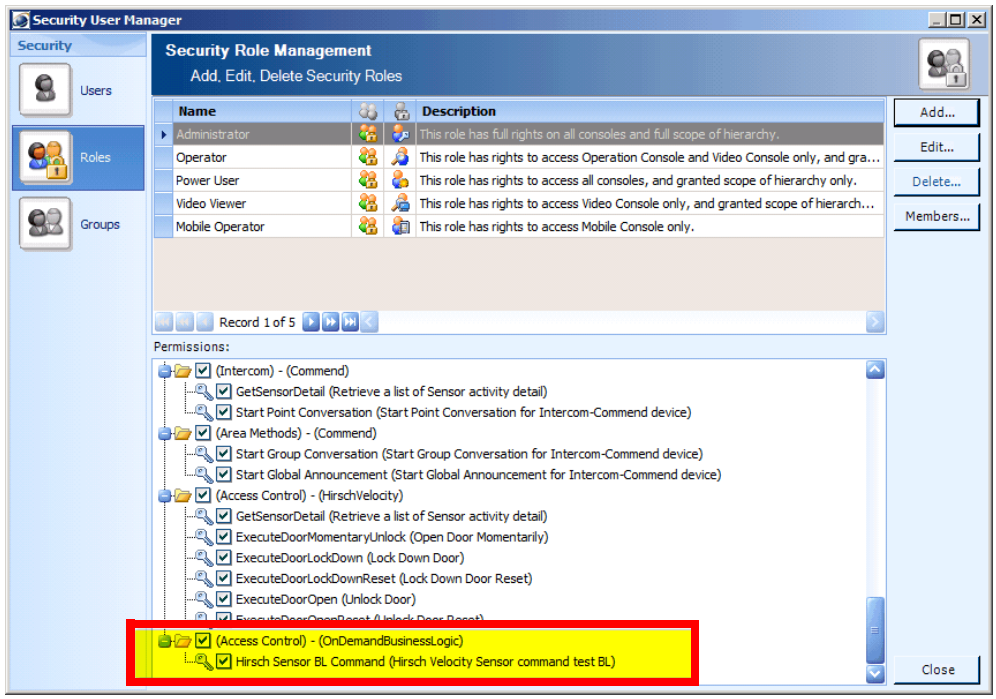
The Business Logic Policy Manager window re-appears showing your customized logic.

Step 15 Click **OK** to save your changes.

Step 16 Apply your business logic template to expose the commands to the Operation Console. See the "Applying Business Logic Policies" section on page 14-46.

Controlling Permissions to On-Demand Business Logic

You can set permissions for deployed on-demand business logic that determine which security roles can access the on-demand business logic. To do so, modify the permissions for the security role(s) to explicitly enable or disable the specific on-demand business logic.



See the "Permissions Within PSOM" section on page 2-20 for details on modifying permissions for a Role in PSOM.

Creating an Alert Status Business Logic Template Based on the Default Template

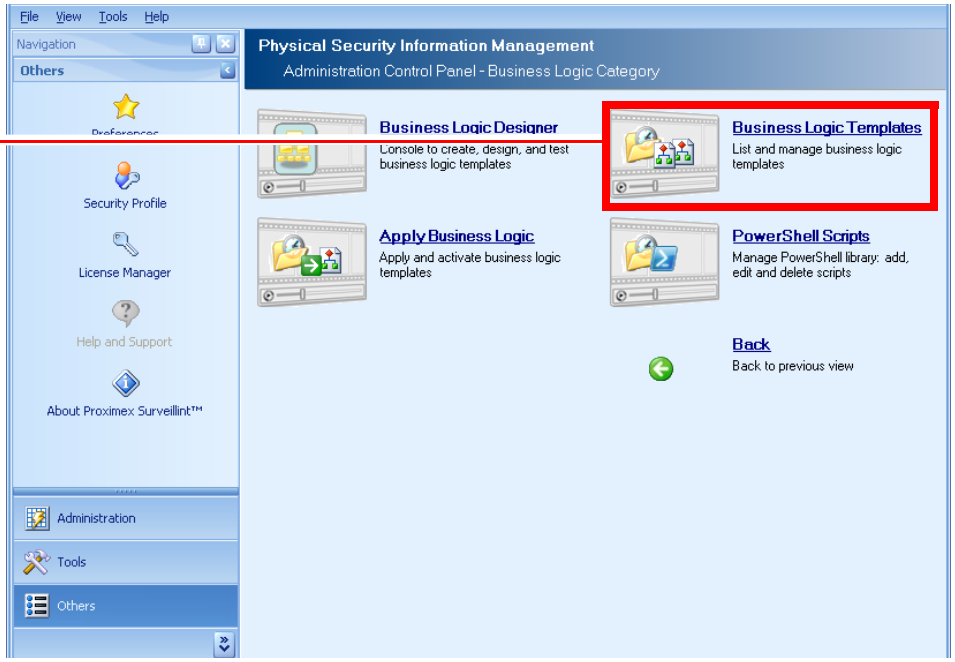
An Alert Status Business Logic template allows custom business logic processing to occur when a specified type of alert changes status.

Note To create a new business logic template from scratch, see the "Designing Business Logic in the Business Logic Designer" section on page 14-36.

To create a new Alert Status Business Logic template based on a default template:

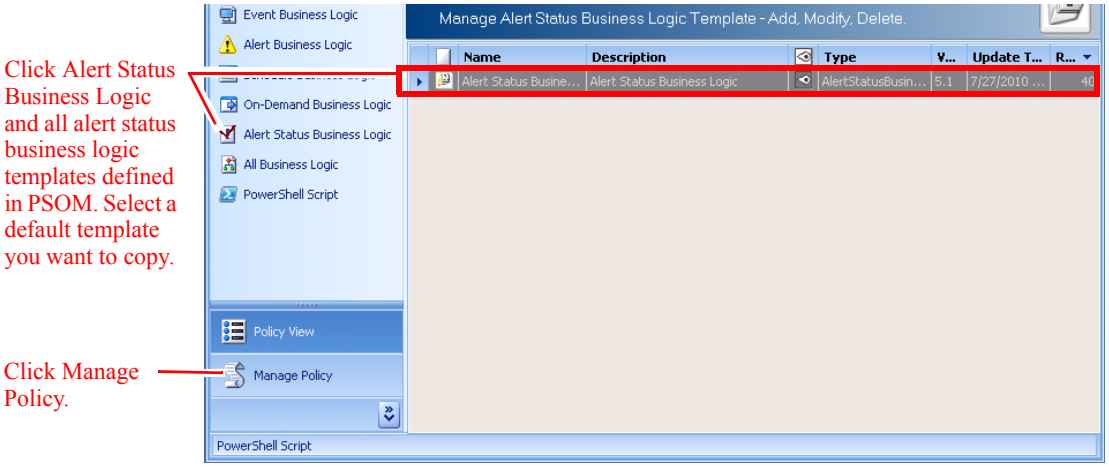
Step 1 Click the **Business Logic** icon in the Administration Console.

Step 2 Click the **Business Logic Templates** icon.

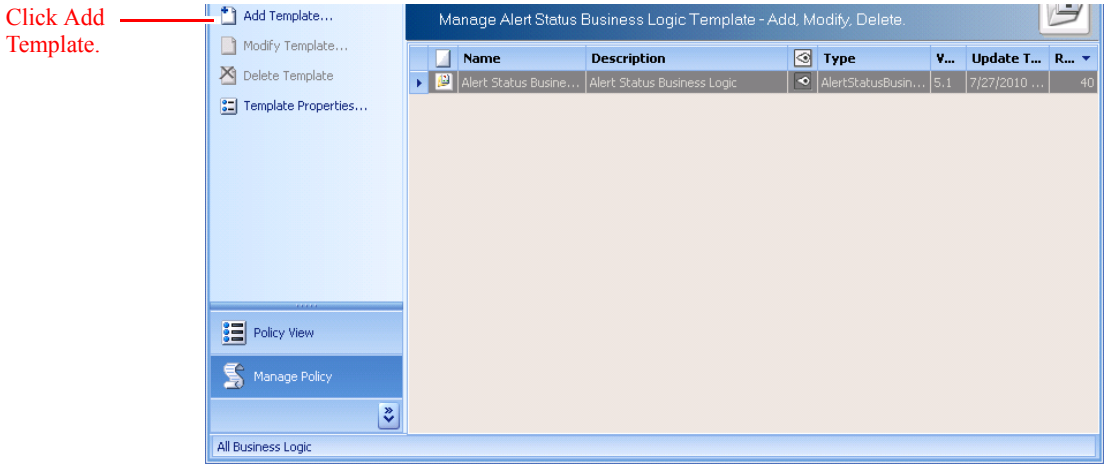


The Business Logic Policy Manager window appears.

Step 3 Click **Alert Status Business Logic** under **Policy View**.

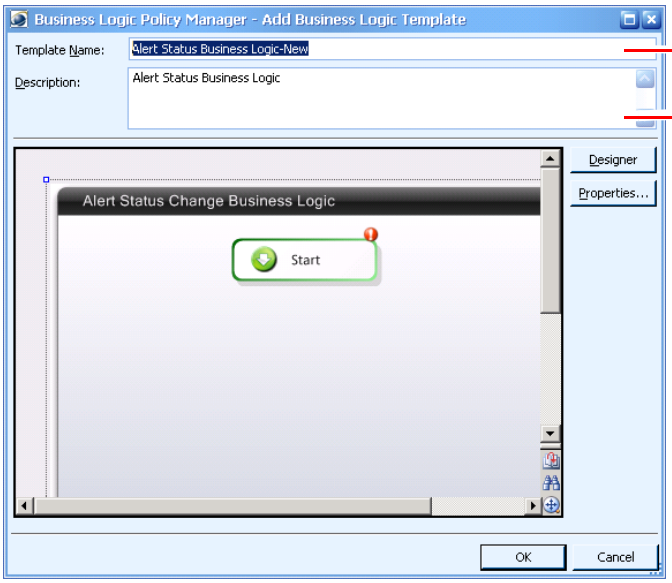


Step 4 Click **Manage Policy** in the left navigation bar.



Step 5 Select the default business logic template you want to copy from the list and click **Add Template**.

The Add Business Logic Template window appears. The bottom of the window shows a graphical read-only representation of the business logic design.

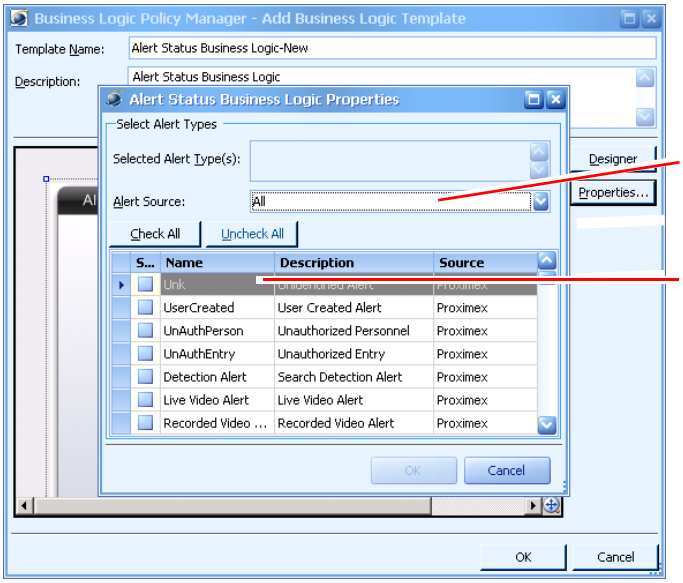


Step 6 In the **Template Name** field, enter a name for this business logic template.

Step 7 In the **Description** field, enter information about the behavior of this business logic template.

Step 8 Click **Properties** to select the alert type for which a status change will trigger this business logic template.

The Alert Status Business Logic Properties window appears.



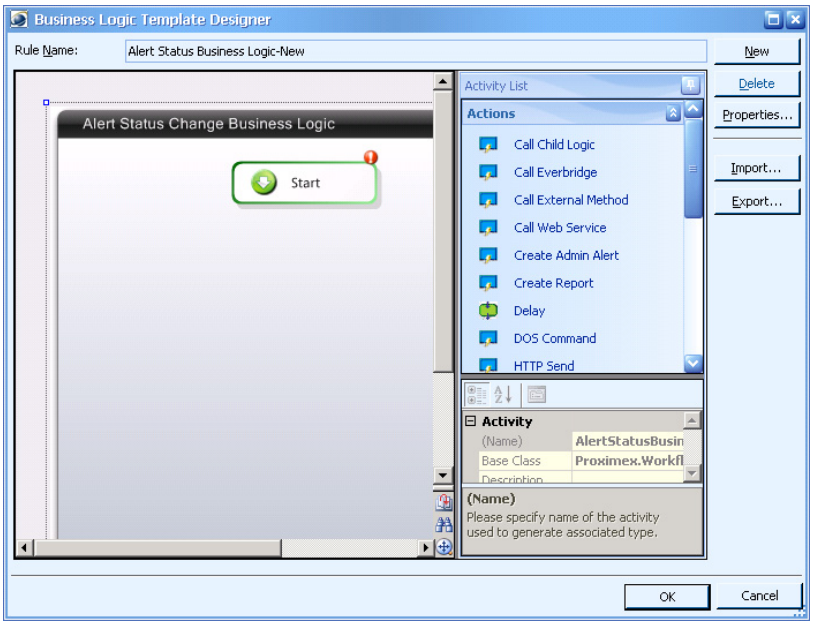
Step 9 Select the third-party system which has sensors that will trigger the specific alert type from the **Alert Source** field. Or you can leave **All** selected.

Step 10 Select all alerts whose change in status will trigger this business logic from the list at the bottom of the window.

Step 11 Click **OK** to save your business logic settings.

Step 12 As configured, this Alert Status Business Logic simply starts empty business logic. To customize this business logic to add actions that should occur when the status of the selected alert types changes, click the **Designer** button.

The Business Logic Template Designer window appears.



Step 13 Add action, decision, and sensor icons to your business logic as needed to perform necessary actions when alert status changes. Some ideas include:

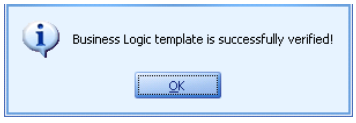
- Dispatch a notification automatically to CISCO IPICS when an alert is acknowledged using the IPICS Notify activity.
- Execute a PowerShell script command. For example, you might use a PowerShell script to retrieve the alert ID, previous status and current status of the alert.

```
$curStatus = $pxAlert.Status
$prevStatus = $pxAlert.PrevStatus
$tempAlertId = $pxAlert.AlertID
$pxLogger.logWarn("Alert " + $tempAlertId + " changed from `" +  $prevStatus + "' to
`" + $curStatus + "'")
```

Note You cannot use the **Set Status** activity in this business logic.

Step 14 Once you've added and connected all icons for your modified business logic, click **OK** in the Business Logic Template Designer window.

Step 15 Your business logic will be verified. If it is sound logic, you will be notified. Click **OK** to confirm.



The Business Logic Policy Manager window re-appears showing your customized logic.

Step 16 Click **OK** to save your changes.

Step 17 Apply your business logic template to expose the commands to the Operation Console. See the "Applying Business Logic Policies" section on page 14-46.

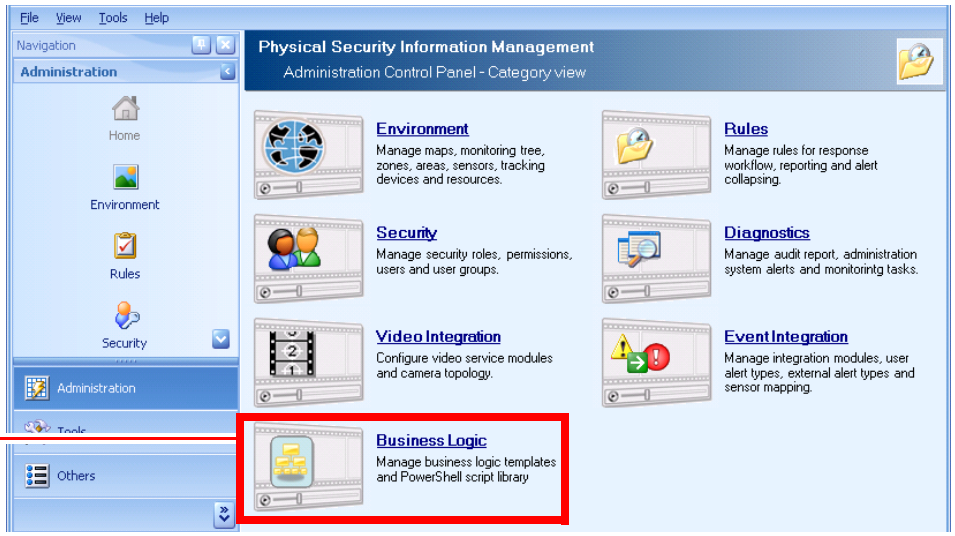
Designing Business Logic in the Business Logic Designer

You can use the Business Logic Designer to design new business logic templates from scratch.

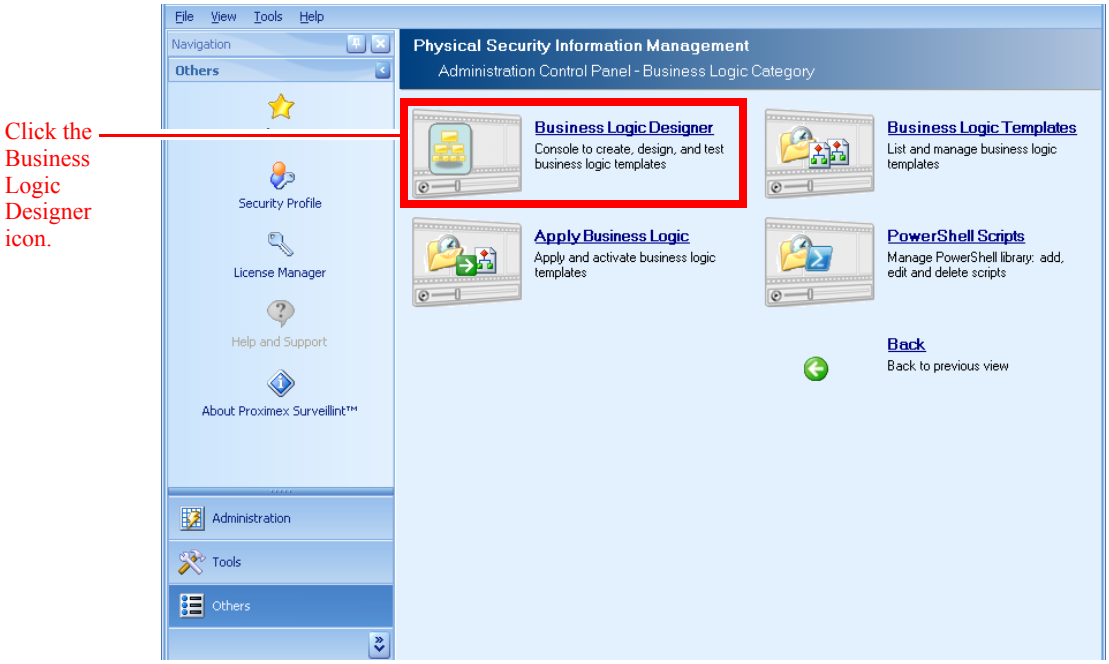
To design business logic in the Business Logic Designer:

Step 1 Select **Start > All Programs > Cisco Physical Security Operations Manager 5.1 > Business Logic Designer**.

Or, click the **Business Logic** icon in the Administration Console.

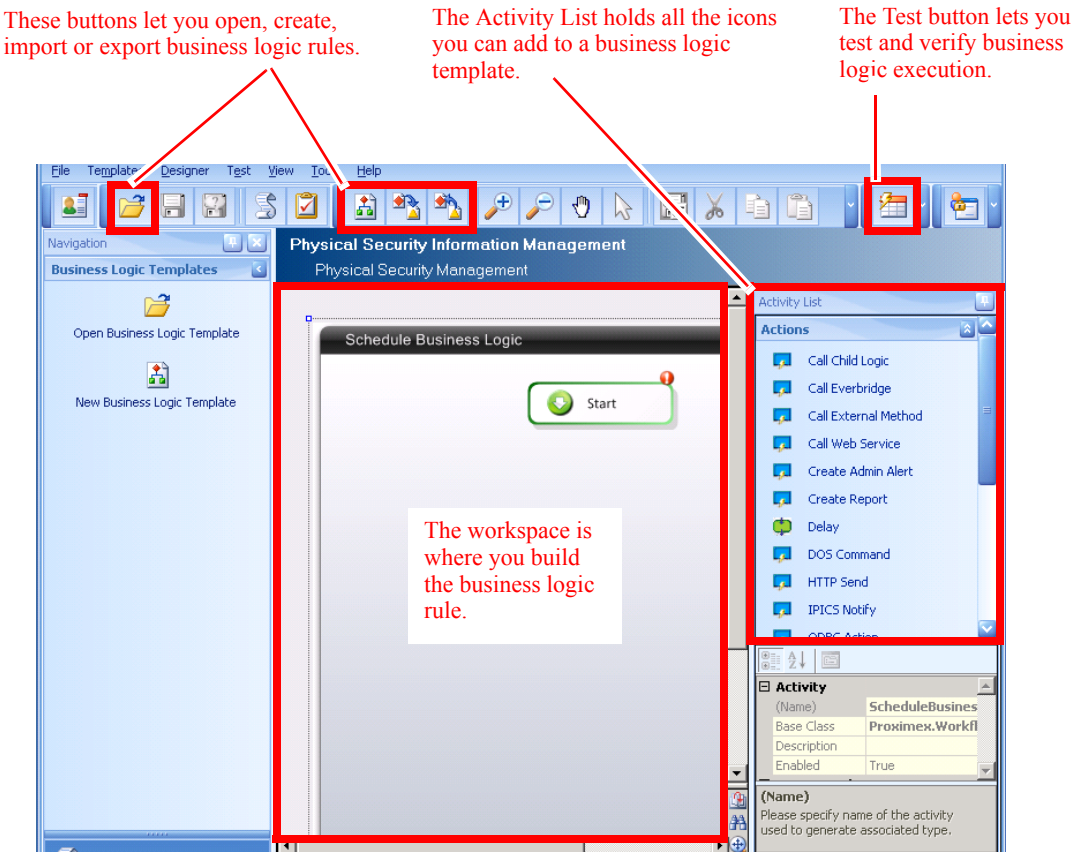


The Business Logic window appears.



Step 2 Click **Business Logic Designer**.

The Business Logic Designer window appears.



Along the top of the window is the Business Logic Designer toolbar which has buttons you can click to open an existing business logic template, create a new business logic template, or import/export business logic templates. It also includes the **Test** area where you can verify the configuration of business logic templates as well as perform a test run.

Along the right side of the window is the **Activity List** which contains the icons you can drag into your workspace to build your business logic template. See the "Understanding Business Logic Components" section on page 15-2 for a description of all the icons.

In the center of the window is the *workspace* where you build your business logic template. At the top of the workspace is the designer toolbar. Table 14-1 provides information about the toolbar and its buttons.

Table 14-1 Buttons in the Business Logic Designer Toolbar

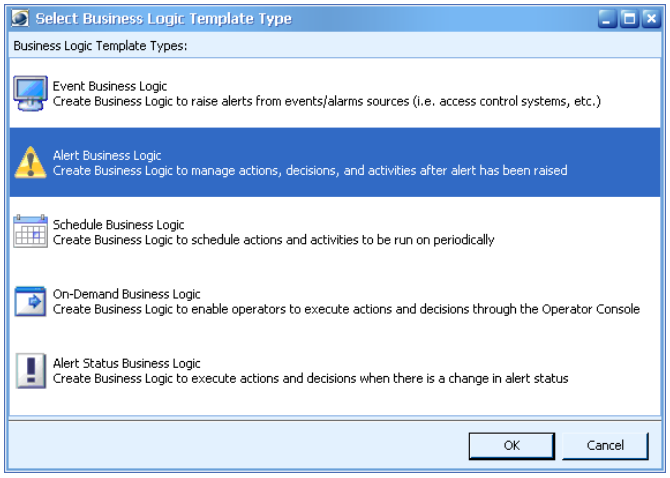
This icon...	Does this to the business logic rule design...
	Opens an existing business logic template.
	Saves the changes to the business logic template.
	Saves the business logic template under a new name.
	Opens the Business Logic Policy Manager window for adding, modifying, or deleting business logic templates.
	Opens the Business Logic Policy Manager window for applying business logic.
	Creates a new business logic template.

Table 14-1 Buttons in the Business Logic Designer Toolbar (continued)

This icon...	Does this to the business logic rule design...
	Imports an XML file that defines a business logic template.
	Exports the current business logic template configuration to an XML file.
	Zooms in to show a closer view of part of the business logic workspace.
	Zooms out to show a larger area of the business logic workspace.
	Grabs and pans around the business logic workspace.
	Selects items in the business logic workspace.
	Saves the selected activity icon after changes have been made to its properties. Creates a custom activity in the Activity List that can be reused in other business logic.
	Cuts the selected item from the workspace.
	Copies the selected item in the workspace.
	Pastes the copied item into the workspace.
	Deletes the selected item from the workspace area, removing it from the business logic rule template.
	Displays the Properties window for the icon that is selected in the workspace.
	Verifies the current configuration of the business logic template.
	Sets or clears a breakpoint for testing purposes. The action is performed on the icon that is selected in the workspace.
	Starts a test of the business logic template.
	Continues a test of the business logic template after a breakpoint.
	Cancels a test of the business logic template.
	Launches the PSOM Administration Console.
	Launches the PSOM Alert Console.

Step 3 A new business logic template should already be open in your workspace. If not, click **New Business Logic Template** under **Business Logic Templates** in the Navigation Pane.

The Select Business Logic Template Type window appears.



Step 4 Select the type of business logic template you want to create and click **OK**.

Your new business logic template appears in the workspace.

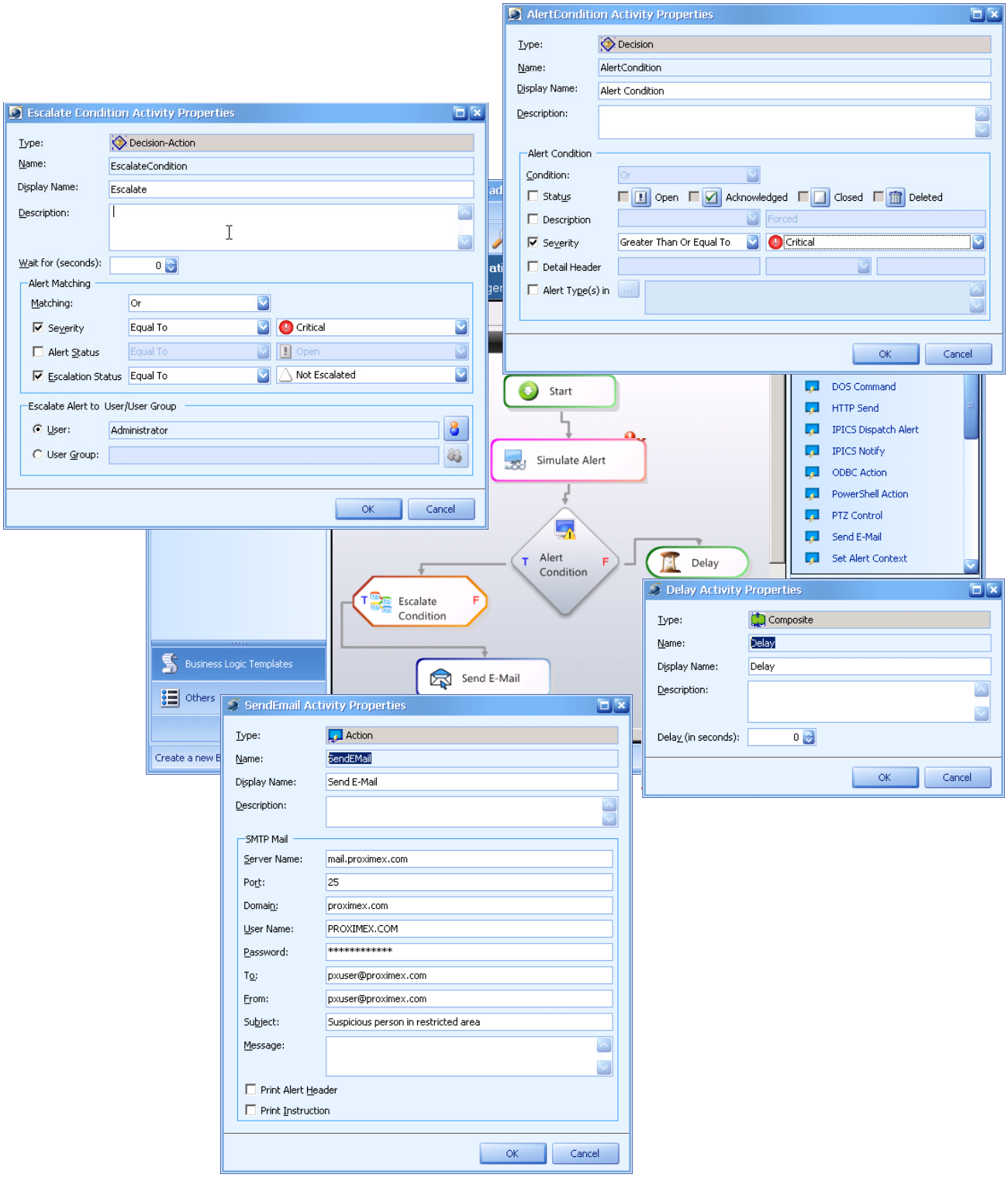
Step 5 Drag icons into the workspace that you will need for the business logic template.

Step 6 Connect the icons in the workspace to create the flow between them.

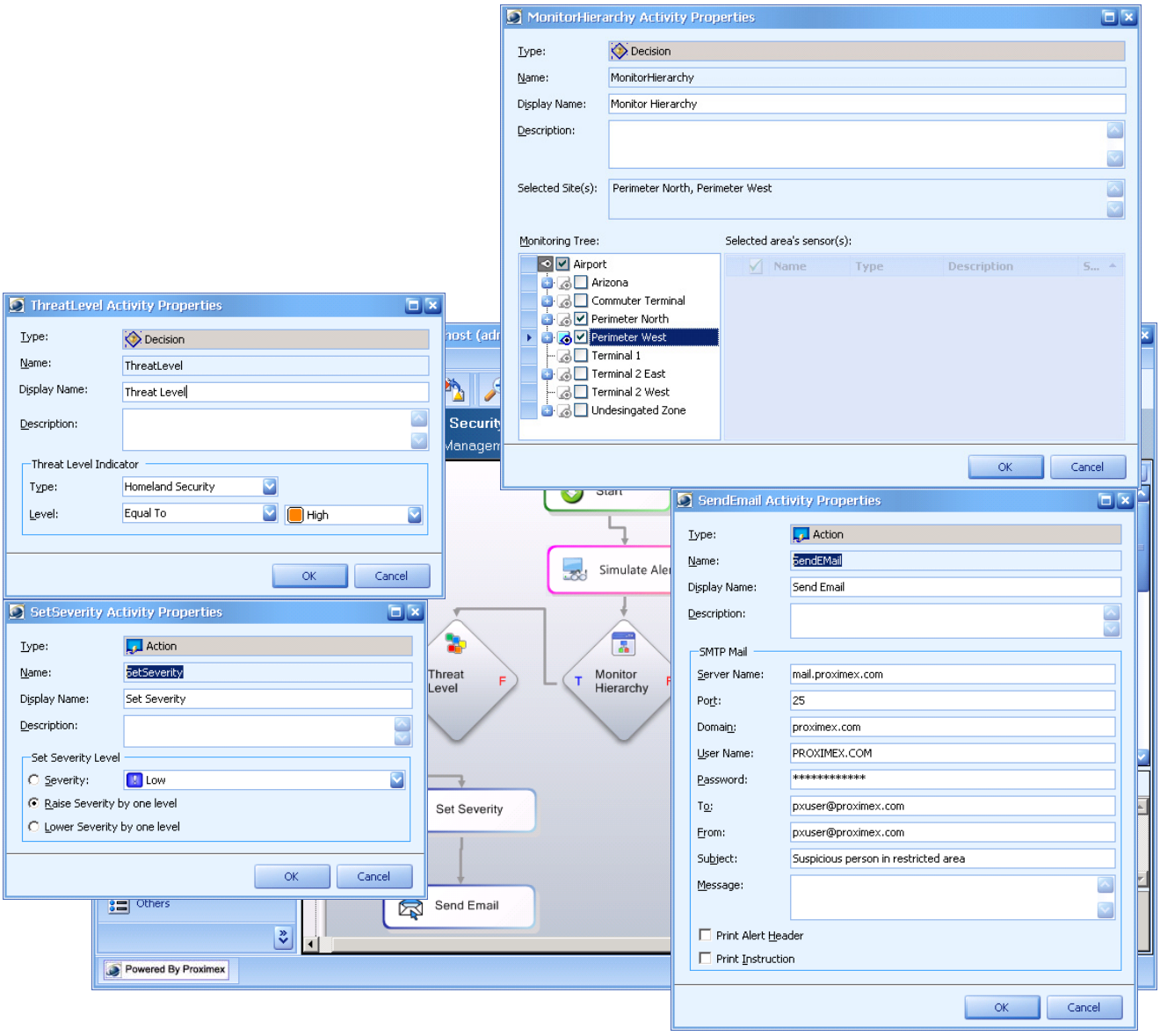
Note Once a component is connected, it cannot be renamed.

In testing and real deployment, not all components need to be connected. Especially for debugging, having multiple versions of the same component that you can alternate for connectivity provides useful information. If a component is not connected, it is not executed. Components do, however, need to be configured properly even if they are not connected.

This example shows a business logic template that escalates alerts based on status; if an alert has critical severity and it has not been escalated after 10 seconds, then it is escalated to the Administrator group, otherwise it is not escalated.



The next example shows a business logic rule in which alert severity is changed based on the Homeland Security threat level. If an alert is raised in the perimeter of the airport, then check the current Homeland Security threat level. If the Homeland Security threat level is at least set to High, then raise the current alert severity one level higher and escalate to the Administrators group.



Step 7 Click the **Save Activity** icon in the toolbar when you make changes to the properties for a component and want to save it. The Activity will be saved as a new component in the **Activity List** and can be reused in other business logic.

Note You must change the name of the Activity in order to save it. Otherwise, you will receive a warning message and you will not be able to save the Activity.

Step 8 Click the **Save Template** icon in the toolbar when you are finished building your business logic template.

Testing Business Logic Templates in the Business Logic Designer

You can test your business logic templates in the Business Logic Designer using the alert simulator to make sure that the flow and design of the business logic template works correctly before you apply it to your security environment.

Step 1 Open your business logic template in the Business Logic Designer.

Step 2 Click the **Verify Template** button in the toolbar to begin a test of the business logic template.

Step 3 If you want to pause test execution of the business logic at certain activities, select the appropriate icon within the business logic and click **Test - Set Breakpoint** in the toolbar. A red dot appears on the icon within the workspace.

Step 4 Click **Test - Start** in the toolbar to begin testing the business logic template. At each breakpoint, the test execution will pause. To resume the test execution after a breakpoint, click **Test - Next Step** in the toolbar.

Step 5 If you want to stop the test execution while it is running, click **Test - Cancel** in the toolbar.

Step 6 Click **Save Template** in the toolbar when you are finished testing your business logic template.

Note You do not need to remove the SimulateAlert icon from your business logic templates before applying them to your PSOM environment. PSOM ignores these icons for actual runtime deployment. However, if the alert used by the SimulateAlert icon is deleted in PSOM, running the business logic template in Test mode may result in incomplete alert details for testing purposes (such as information presented in the Description and Tasks areas of the Alert Details window).

Debugging Business Logic Templates that Include CorrelateCondition Components

Debugging and fine-tuning business logic templates that incorporate CorrelateCondition components is similar to debugging other business logic templates. You should simulate alerts, set breakpoints, and step through the execution of the business logic template to determine the results of each activity.

However, you do need to be sure that PSOM is populated with the types of alerts that you are going to correlate in your business logic template. To do so, you need to set up a test environment on a non-production server. Testing and debugging business logic in a production environment can cause false information to appear to security operators in the Operation Console.

Step 1 On a non-production server, install and configure the PSOM software.

Step 2 Restore a backup of your production database to your testing environment.

Step 3 Remove the application of existing applied business logic templates to avoid distracting interactions that will inhibit your ability to debug the current business logic template; do not delete these templates, but remove their application within the environment.

Step 4 In your business logic template, create multiple SimAlert components, each based on relevant pre-existing alerts. A CorrelateCondition must have at least two alerts available for correlation. Therefore, you should create SimAlert components for all relevant alerts so that they can be used for debugging.

Note You can use a Delay component between SimAlert components to simulate a realistic flow of alert messages.

When your business logic template is deployed, all SimAlert components will be ignored. However, any activities that are placed between SimAlerts will be executed.

Having names and descriptions that characterize the purpose of each component in your business logic template helps with debugging and enhances self-documentation.

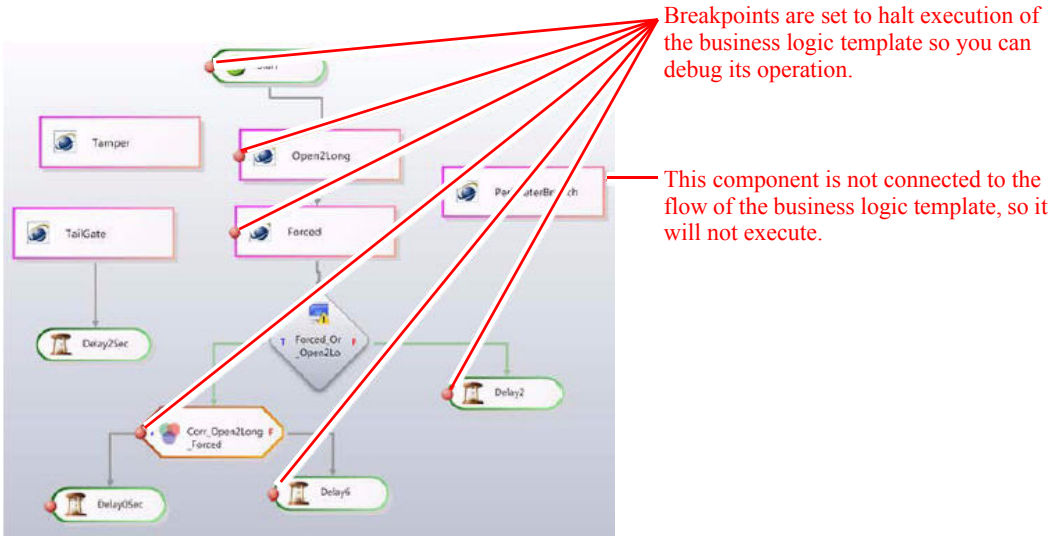
Step 5 Add the components you need for your business logic template, set their parameters, and connect the components as needed for the flow.

Note In testing and real deployment, not all components need to be connected. Especially for debugging, having multiple versions of the same component that you can alternate for connectivity provides useful information. When you are finished testing one version of a component, you can remove the connections to that component version, connect a different component version, and retest. If a component is not connected, it is not executed. Components do, however, need to be configured properly even if they are not connected.

Step 6 Define CorrelateCondition components to perform the conditional analysis that your business logic template needs. CorrelateCondition components should normally follow an AlertCondition component so that a non-relevant alert does not invoke the CorrelateCondition component.

Step 7 For Decision or Decision-Action components, make sure that all exit conditions flow into a valid component; for example, a Delay component set to 0 delay. You can then place breakpoints at the exit condition component during debugging to evaluate the condition.

Step 8 Place breakpoints on all connected components by selecting the appropriate icon within the business logic and clicking **Test - Set Breakpoint** in the toolbar . Once you evaluate and approve components and their effects, you can remove the breakpoints.



Step 9 Click **Test - Start** to begin testing the business logic template. At each breakpoint, the test execution will pause. To resume the test execution after a breakpoint, click **Test - Next Step**.

Step 10 During testing, keep the Operation Console window open and examine the results of your business logic template as you step through it.

Step 11 Once you are satisfied, open the Administrator Console and reapply the business logic templates that are normally deployed on the production server.

Step 12 Click **Test - Start** to begin testing the business logic template in a simulated production environment. Now you will verify that your business logic template behaves appropriately and does not impact other executing business logic templates.

Note You may need to modify the business logic template slightly to change the AlertCondition components so as to minimize the "crosstalk" between business logic templates.

Step 13 One you have verified your business logic template in a production environment, save it by clicking **Save Template** in the toolbar.

Step 14 Click **Export Business Logic** in the toolbar to save the business logic template to an XML file on your network.

Step 15 In your production PSOM system, launch the **Business Logic Designer**.

Step 16 Click **Import Business Logic** in the toolbar, and select the XML file you saved from the test environment.

Step 17 Click **Save Template** in the toolbar.

Step 18 Apply your business logic template as described in the "Applying Business Logic Policies" section on page 14-46.

Debugging Business Logic Templates that Include Delay Loops

Avoid infinite loops by ensuring that there is an exit condition for the decision component with which the Delay component is looping. Please debug your business logic carefully before deploying it to servers. You can verify whether your business logic is in an infinite loop by examining the log located at: C:\Program Files\Cisco PSOM\Managed Services\log\PxBLService_log.txt.

If the business logic is stuck in an infinite loop, you can stop it by removing the application of the business logic template in PSOM.

Applying Business Logic Policies

Once you have a business logic template configured, you need to apply it to the global zone in PSOM so that it will take effect as a business logic policy.

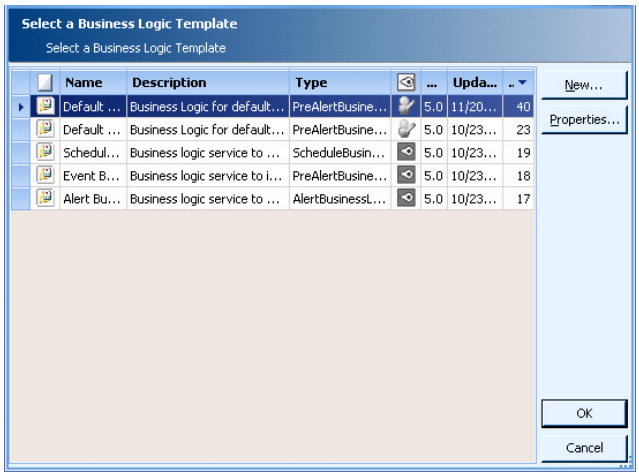
To apply a business logic policy from the Business Logic Designer:

Step 1 From the **Business Logic Designer**, click the **Apply Policies** button in the Business Logic Designer toolbar.

The Business Logic Policy Manager window appears.

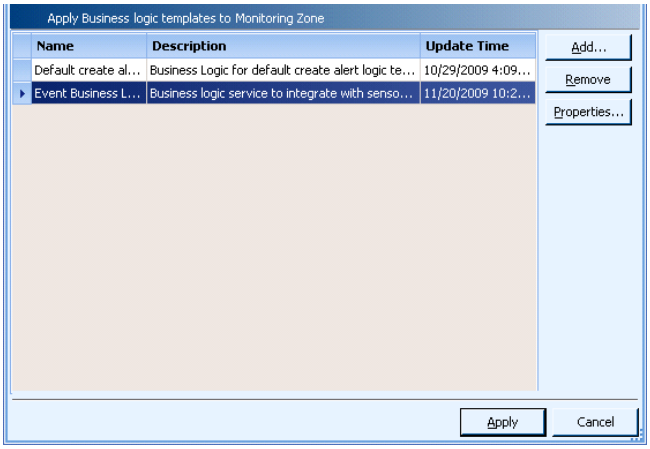
Step 2 Click **Add**.

The PSOM Business Logic Policy Manager window appears.



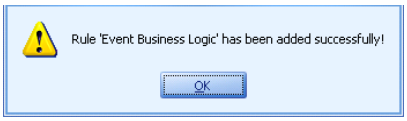
Step 3 Select the business logic template you want to apply and click **OK**.

The Business Logic Policy Manager window reappears with your selected template.



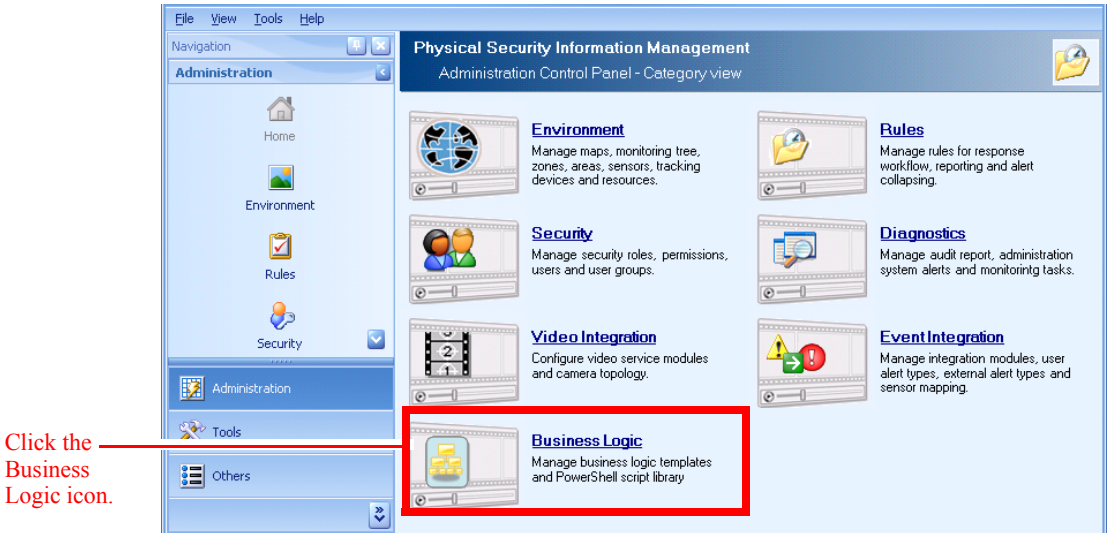
Step 4 Click **Apply**.

A confirmation message appears that the template has been applied.

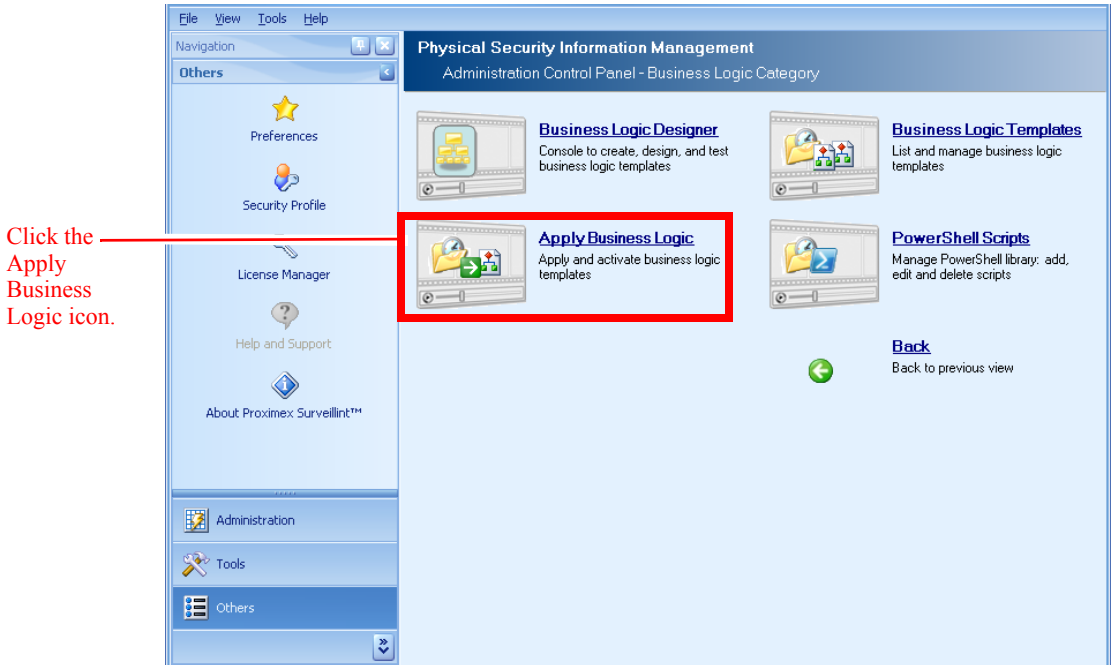


To apply a business logic template from the Administration Console:

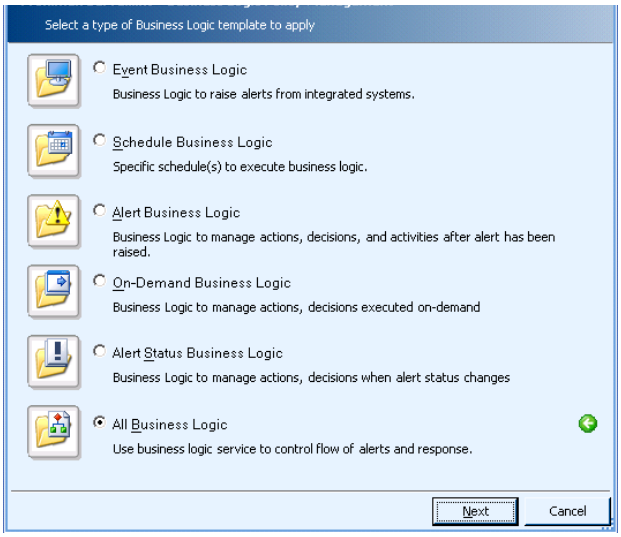
Step 1 Click the **Business Logic** icon.



Step 2 Click **Apply Business Logic**.



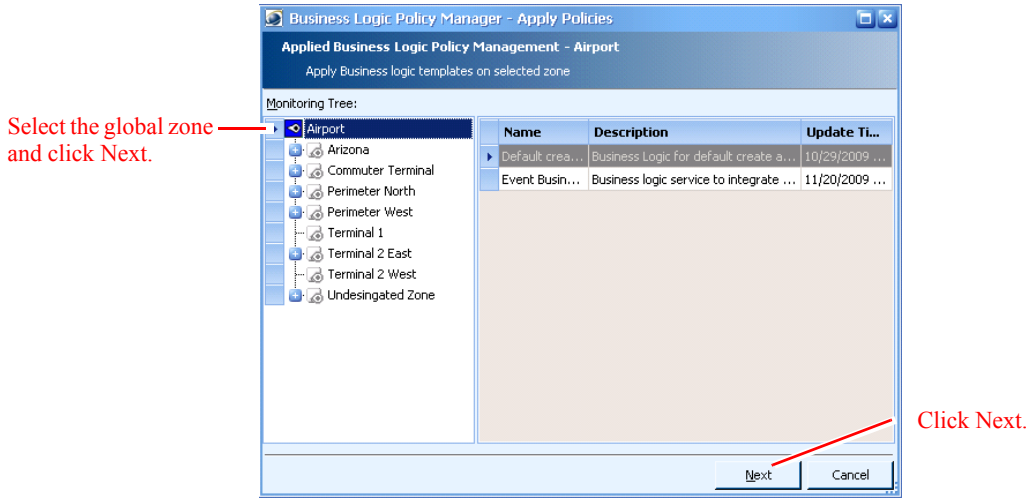
The Apply Policies window appears.



Step 3 Select the type of business logic template you want to apply: **Event Business Logic**, **Schedule Business Logic**, **Alert Business Logic**, **On-Demand Business Logic**, **Alert Status Business Logic**, or **All Business Logic**.

Step 4 Click **Next**.

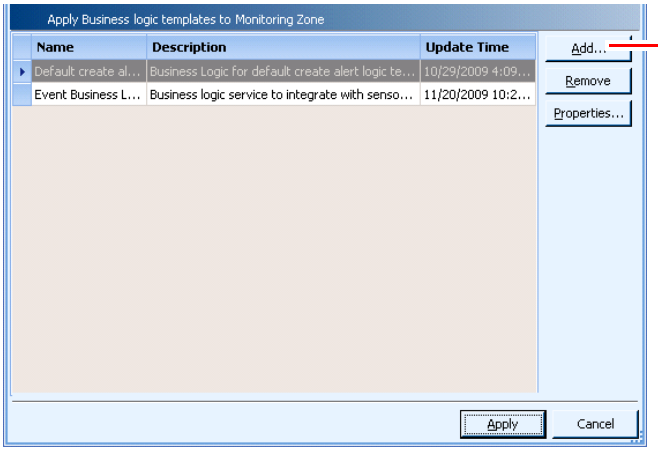
The Apply Policies window appears.



Step 5 Select the global zone and click **Next**.

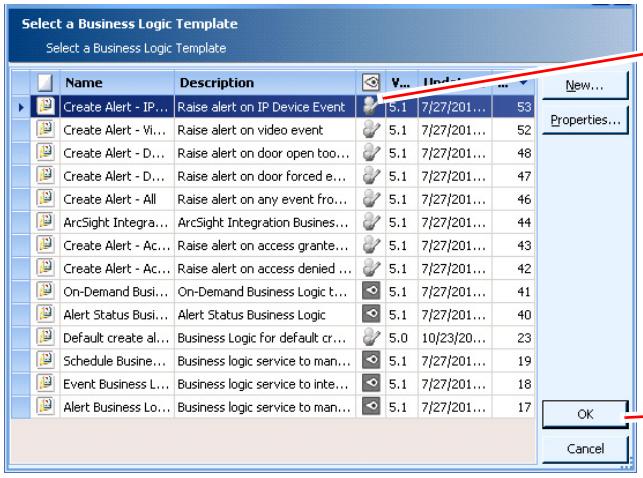
Note Business logic templates can only be applied to the global zone (top node).

The Business Logic Policy Manager window appears.



Step 6 Click the **Add** button.

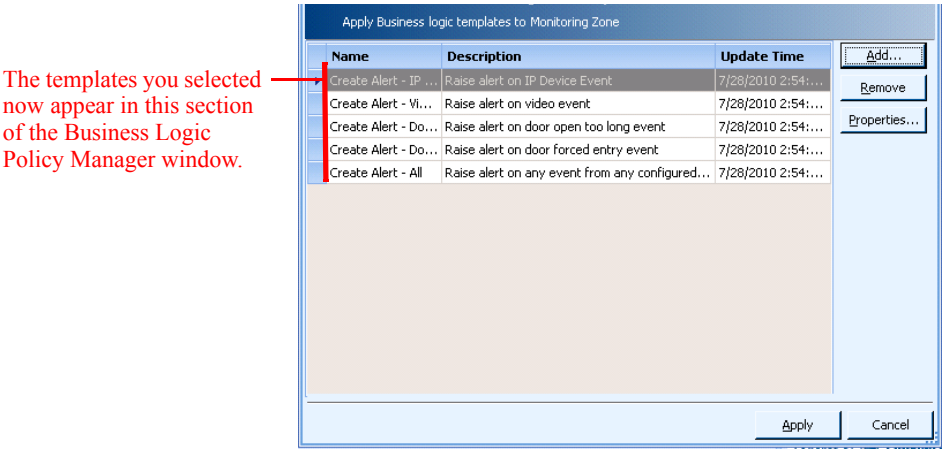
The Select a Business Logic Template window appears.



Step 7 Select the business logic templates you want to apply. You can select multiple templates using the SHIFT or CTRL keys.

Step 8 Click **OK**.

The templates you selected appear in the Business Logic Policy Manager window.



Step 9 Click **Apply** to save your changes.

The chosen business logic templates will be applied to the global zone.

Importing and Exporting Business Logic Templates

If you want to copy or transfer business logic templates between PSOM installations, you can use the Import Business Logic and Export Business Logic tools in the Business Logic Designer.

To transfer business logic templates between PSOM installations:

Step 1 Open the business logic template in the Business Logic Designer on the system where the business logic template has been configured.

Step 2 Click **Export Logic** in the Business Logic Designer toolbar.

Step 3 The **Save As** dialog appears. Save the XML file for the business logic.

Step 4 Copy the XML file to the system with the PSOM installation where you want to import this business logic template.

Step 5 Open the Business Logic Designer on the destination system.

Step 6 Click **Import Logic** in the Business Logic Designer toolbar.

Step 7 The **Open** dialog appears where you can select the XML file for the business logic.

The work area in the Business Logic Designer is populated with the imported business logic.

Using Global System Variables in Business Logic

Some Activity icons can leverage PSOM global system variables to seamlessly pull alert information into the business logic. These variables are listed in Table 14-2.

Table 14-2 System Variables for Obtaining Alert Data from PSOM

This command-line argument...	Returns this alert data...
%ALERTID%	The ID for the alert from PSOM.
%DESCRIPTION%	The actual text message of the alert from PSOM.
%SEVERITY%	The risk level assigned to the alert within PSOM: Low, Medium, High, or Critical.
%STATUS%	The current condition of the alert. Open—The alert still needs to be investigated and appropriate actions taken. Acked—The alert has been acknowledged, and an operator is probably taking actions to resolve it. Closed—Appropriate actions have been taken to close the alert.
%TYPE%	The type of alarm that was raised by the sensor. The types of alarms that can be triggered are dependent upon the system that controls the sensors; the system with which PSOM integrates.
%LOCATION%	The location property of the sensor that triggered the alarm.
%OCCURTIME%	The date and time when the alarm was triggered.

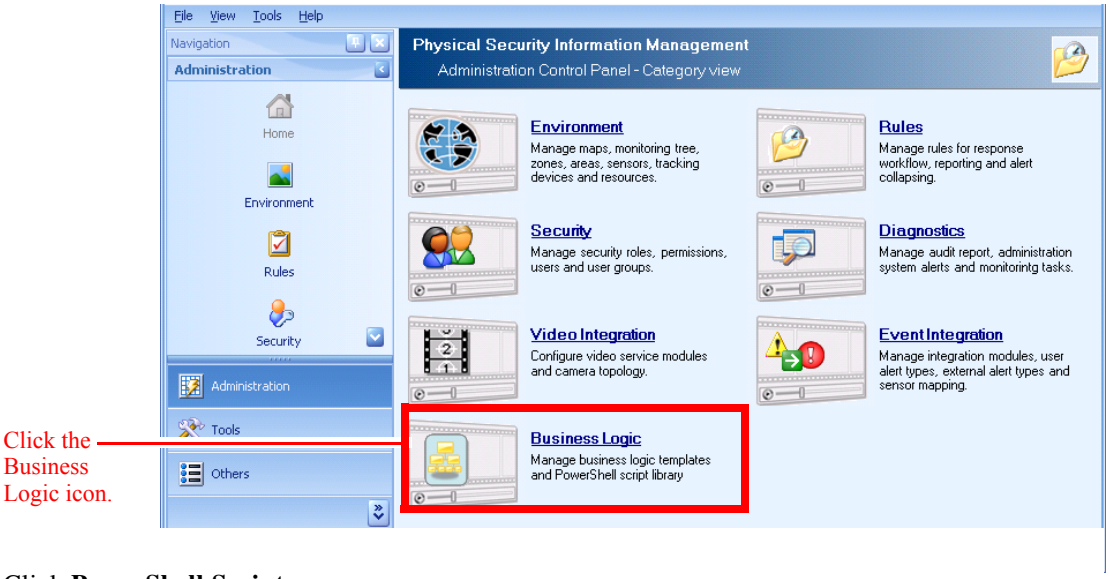
Note These system variables are only applicable when the activity is included in an Alert Business Logic or Alert Status Business Logic template. Other business logic templates do not process these variables.

Storing PowerShell Scripts for Business Logic

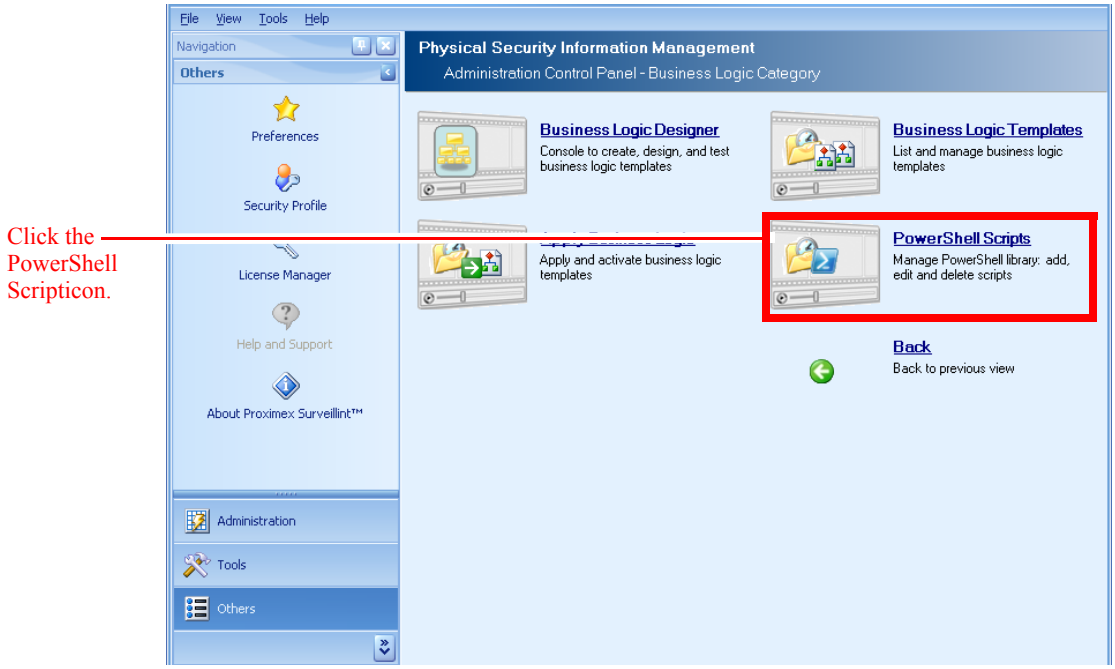
You can define PowerShell scripts and save them in the PowerShell library for reuse in business logic.

To save a PowerShell script:

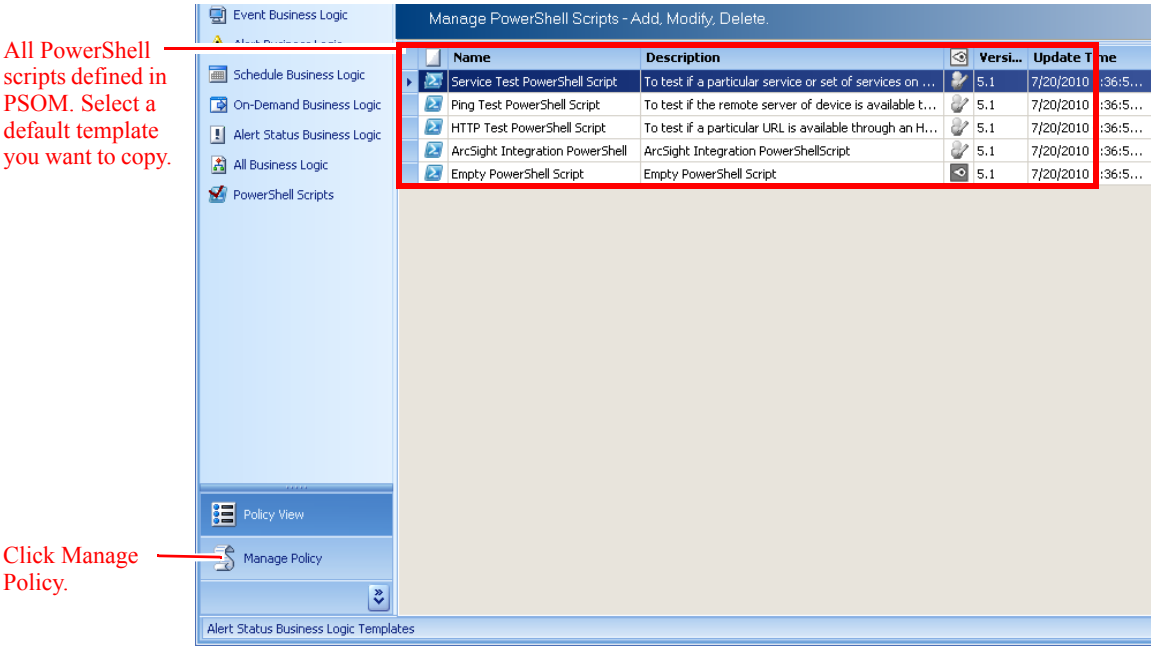
Step 1 Click the **Business Logic** icon.



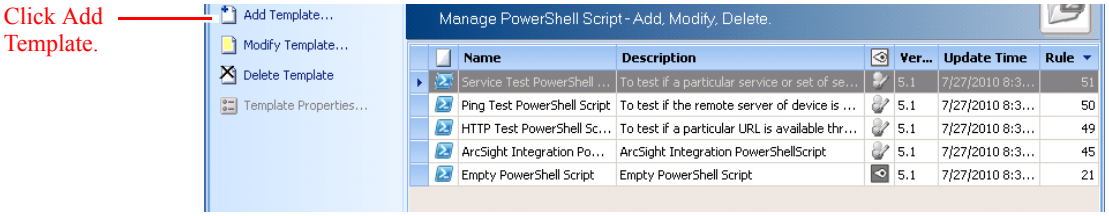
Step 2 Click **PowerShell Scripts**.



The Business Logic Policy Manager window appears.

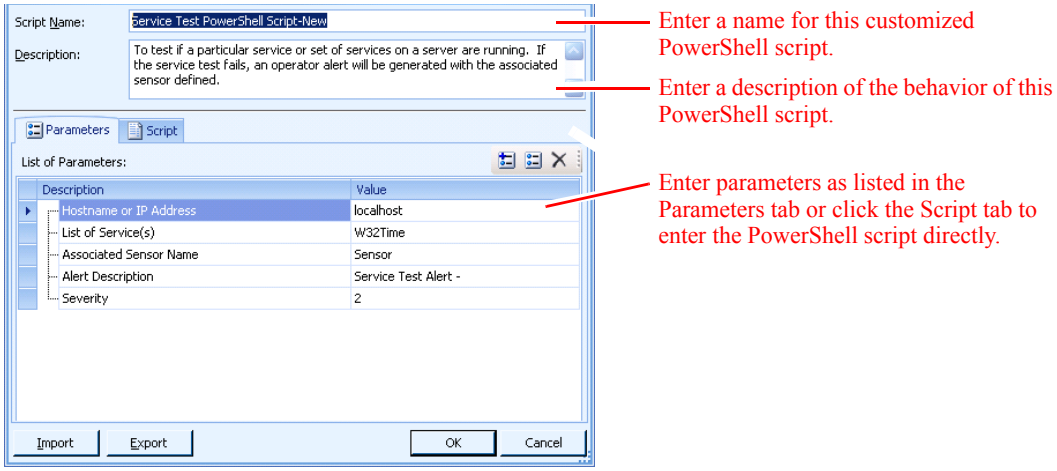


Step 3 Click **Manage Policy** in the left navigation bar.



Step 4 Select the default PowerShell script you want to copy from the list and click **Add Template**.

The Add PowerShell Script window appears.



Step 5 In the **Script Name** field, enter a name for this PowerShell script.

Step 6 In the **Description** field, enter a description of the behavior of this PowerShell script.

Step 7 On the **Parameters** tab, enter the values for each of the parameters.

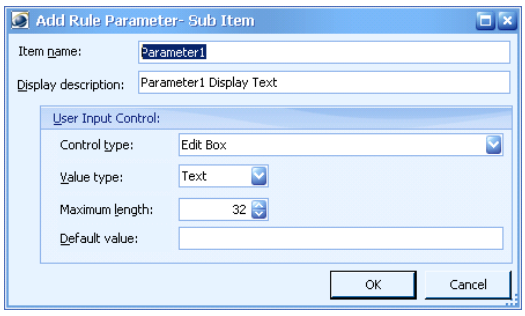
Or click the **Script** tab to enter the PowerShell script directly.

Adding Parameters to Define PowerShell Scripts

To define PowerShell scripts using the Parameters tab:

Step 1 Click the **Add Parameter** button at the top right of the **Parameters** tab.

The **Add Rule Parameter** dialog appears.

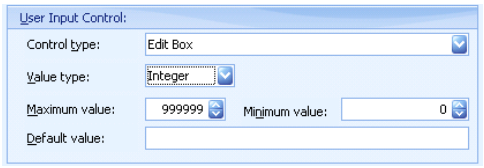


Step 2 Enter a name for the rule in the **Item name** field.

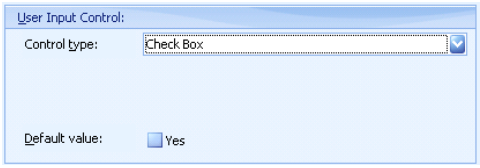
Step 3 Enter a description in the **Display description** field.

Step 4 Select the type of information you want to collect from the **Control type** field. Choices include:

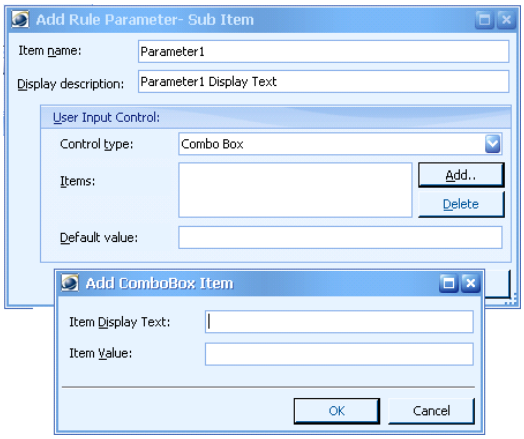
- Edit Box—Allows you to enter text or integer values (choose **Text** or **Integer** from the **Value type** field). For text, you can specify a maximum number of characters. For integers, you can specify the maximum, minimum, and default values.



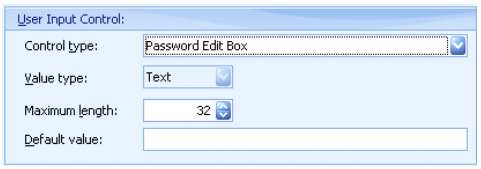
- Check Box—Allows you to accept a check or uncheck as a response.



- Combo Box—Allows you to provide choices for a response. Select **Combo Box** from the **Control type** field, and click **Add** to enter a choice in the **Add ComboBox Item** dialog. For each choice, provide the text and value that are displayed. Keep clicking **Add** to enter as many choices as you need to provide.

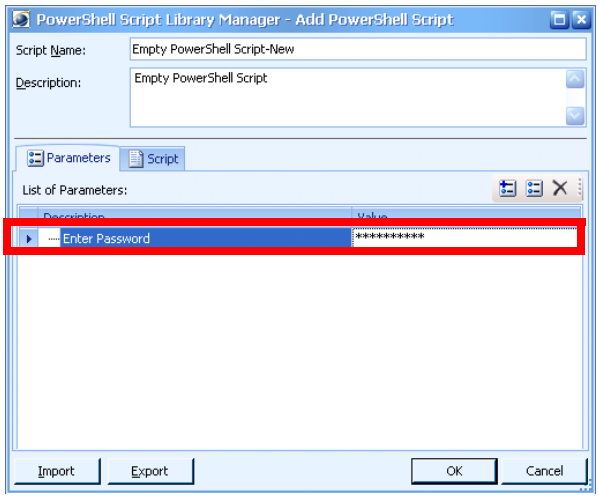


- Password Edit Box—Allows you to accept a password at runtime. You can set a maximum number of characters and provide a default value.



Step 5 Click **OK**.

The parameter appears in the **Add PowerShell Script** dialog.



Step 6 Repeat as many times as needed to define all parameters for the PowerShell script.

Adding Scripts to the Script Area

If you want to write the PowerShell script in a different script editor (such as Notepad or an open source tool like Power GUI Editor), click the button in the **Script** area, and navigate to select your script editor. Once you've finished writing and debugging your code, you can copy and paste it into the text area of the **Add PowerShell Script** window. See the "Setting Up PowerShell Scripts" section on page 14-56, the "PowerShell Script Format" section on page 14-57, the "Passing Objects in PowerShell Scripts Using Script Variables" section on page 14-58, and the "Understanding Activity Contexts" section on page 14-60 for information you'll need to write PowerShell scripts directly in the **Script** area.

Setting Up PowerShell Scripts

You can setup PowerShell Scripts to perform a variety of functions within PSOM. PowerShell Scripts can be used as part of a business logic rule to execute custom scripts. Through Microsoft's scripting language, you can predefine specific logic, or issue commands and actions to be taken on external security or related systems as a part of the security workflow or process. For example, you could use a PowerShell Action component to correlate data with existing systems including Microsoft SQL Server and Exchange Server.

When creating PowerShell Scripts, you can copy and paste code to create the script, and you can add user interface controls to enable script variables to be set at runtime.

PowerShell Scripts are currently deployed as part of a business logic template; therefore, you do not need to apply a PowerShell Script to monitoring areas.

Note You must have PowerShell installed on your system to execute PowerShell Action components. PowerShell requires Windows XP SP2 or later, and Windows Server 2003 SP1 or later. You can download PowerShell from the Microsoft website

In your PowerShell Script, you can issue the global variables shown in Table 14-3 to obtain data from PSOM when using an Alert Business Logic or Alert Status Business Logic template.

For more concise and flexible scripts, you can pass objects into and out of PowerShell components within business logic. See the "Passing Objects in PowerShell Scripts Using Script Variables" section on page 14-58.

Table 14-3 Global Variables for Obtaining Alert Data from PSOM

This global variable...	Returns this alert data...
$global:AlertID	The ID for the alert from PSOM.
$global:AlertDescription	The actual text message of the alert from PSOM.
$global:AlertSeverity	The risk level assigned to the alert within PSOM: Low, Medium, High, or Critical.
$global:AlertStatus	The current condition of the alert. • Open—The alert still needs to be investigated and appropriate actions taken. • Acked—The alert has been acknowledged, and an operator is probably taking actions to resolve it. • Closed—Appropriate actions have been taken to close the alert.
$global:AlertType	The type of alarm that was raised by the sensor. The types of alarms that can be triggered are dependent upon the system that controls the sensors; the system with which PSOM integrates.
$global:AlertLocation	The location property of the sensor that triggered the alarm.
$global:AlertOccurTime	The date and time when the alarm was triggered.

PowerShell Script Format

The format of the PowerShell Script is shown next. The header of the rule contains its name and description. The <GENERALOPTION> area contains all user input parameters, and the <SCRIPT> area contains the actual PowerShell script.

```
<POWERSHELLSCRIPTRULE NAME="Number Of Process" TYPE="Default" VERSION="3.0" TEMPLATEGUID="
D1AF08A4-BA80-41D4-976A-5201C7989D00">
    <DESCRIPTION>Check number of process</DESCRIPTION>
    <GENERALOPTION> <!-- UI Section -->
     <PARAMETERS> <!-- UI Parameters control -->
        <PARAMETER NAME="$ProcName" TYPE="String" REQUIRED="True">
         <UICONTROL TYPE="Edit">
            <MAXLENGTH>128</MAXLENGTH>
         </UICONTROL>
         <DESCRIPTION>Process Name:</DESCRIPTION>
         <VALUE>Notepad</VALUE>
        </PARAMETER>

        <PARAMETER NAME="$Threshold" TYPE="Integer" REQUIRED="True">
         <UICONTROL TYPE="Edit">
            <MIN>1</MIN>
            <MAX>100</MAX>
            <UNIT></UNIT>
         </UICONTROL>
         <DESCRIPTION>Number of Processes is greater than</DESCRIPTION>
         <VALUE>3</VALUE>
```

```
      </PARAMETER>
    </PARAMETERS>
  </GENERALOPTION>

  <SCRIPT> <!-- PowerShell Script -->
   <![CDATA[
      #####[Rule Variables Begin]#####
       $Threshold = 2
       $ProcName = 'notepad'
      #####[Rule Variables End]#####
       $colItems = Get-Process
       $TotalCount = 0
          foreach ($objItem in $colItems)
          {
              # write-host "Name: " $objItem.Name "ID: " $objItem.ID
              if($objItem.Name -eq $ProcName)
              {
               $TotalCount++
              }
          }
          if($TotalCount -gt $Threshold)
          {
           "True"
          }
          else
          {
           "False"
          }
      ]]>
  </SCRIPT>
</POWERSHELLSCRIPTRULE>
```

Passing Objects in PowerShell Scripts Using Script Variables

When using PowerShell scripts in Business Logic templates, you can pass objects into the PowerShell script as well as from the PowerShell script using predefined script variables:

- PxAlert, PxEvent, PxContext and other “objects” can be passed into a PowerShell script in place of simple strings.
- Output streams from a PowerShell activity can be captured. For example, diagnostic messages can be output to the host via the PowerShell activity.

Objects can be passed in these ways between the PowerShell activity and the PowerShell script:

- .NET objects can be passed from the PowerShell activity to the PowerShell script. This allows the PowerShell script to dynamically read property values and take action.
- The PowerShell script can change the .NET object (for example, PxAlert) and pass the object back to the PowerShell activity.

Using pre-defined service objects, you can write PowerShell scripts to perform actions and query data on the PSOM Web Service as well as other services (ASMX or WCF). PowerShell scripts can also update or set the activity context so that it can update existing context or add new contexts for subsequent activities.

Table 14-4 Predefined Script Variables for Passing Objects using PowerShell Scripts

Script variable	Description
$pxAlert	The alert object. The script can update and change the alert for subsequent activities. **Note** Only applies to post-alert business logic types.
$pxEvent	The event object. You can retrieve the PxSensor object using $PxEvent.Sensor. **Note** Only applies to pre-alert business logic types.
$pxContext	The context registry object shared among all activities. The script can use this context registry object to pass additional data to the next activity in the business logic flow. All data to be passed with the context must be serializable.
$pxWfWs	The WF web service wrapper class defined in the PxObject (workflow objects) project. This should be pre-instantiated with the correct URL.
$pxLogger	The logger object (of data type IPxWFLogger) can be used to log messages from the script to the host's log file. The logger supports multiple levels of logging, including logError, logInfo, and logWarn.
$RuleID	The current Business Logic rule ID. This value is an integer.
$RuleName	The current Business Logic rule name. This value is a string.
$SensorQuery	The common sensor query object which can be used to query sensors or determine monitoring hierarchy. This object adapts itself to either sensor cache or the WS for resolving the query results.
$pxSensorDisarm	The common service to arm/disarm sensors or areas.
$pxOEMInfo	The common OEM related information holder.
$pxMethodCaller	The caller context information when used in On-Demand Business Logic.

For example, the following script dynamically retrieves the alert ID, calls the WF Web Service to obtain the latest alert header, and then outputs the alert header in XML to both the output string (logged by the host) and the context registry. By logging the alert header to the context registry, other activities in the business logic will be able to use the object in context.

```
$AID = $pxAlert.AlertID
$outputString = $pxWfWs.GetAlertHeaderAlertID($AID)
$pxContext.addContextObject("pxScriptData", "Result", $outputString)
"True"
```

You can exchange objects between multiple Powershell activities by using the context registry, as shown in the following script. As long as the object can be serialized, it can be passed between PowerShell activities.

```
$pxContext.addContextObject("pxCondition", "Cond1", $val)
```

You can retrieve an object from the context registry, as shown in the script below:

```
$val2 = $pxContext.FindContextObject("pxCondition", "Cond1")
```

You can log various levels of messages from the script to the host log, as shown in the following script.

```
$pxLogger.logInfo("This is informational level message sample")
$pxLogger.logError("This is error message test")
```

```
$pxLogger.logWarn("This is a warning message"
```

You can execute the methods described in Table 14-5 on the WF Web Service.

Table 14-5 Methods to Execute on the WF Web Service

Method	Description
CorrelateAlert	Correlates multiple alerts.
CreateAdminAlert	Generates a PSOM alert using the pxEvent context.
CreateAuditEntry	Adds an entry to the PSOM audit log.
CreatePxAlert	Creates a new alert in PSOM using the pxEvent context.
DeleteAlert	Deletes an existing alert in PSOM using the pxAlert context.
EscalateAlert	Escalates an alert in PSOM using the pxAlert context.
FindRegisteredService	—
GetAlertHeaderForAlertID	Retrieves the alert header for an alert using the pxAlert context.
GetAlertProperty	Retrieves an alert property using the pxAlert context.
GetAlertStateForAlertID	Retrieves the alert state from the pxAlert context.
GetAlertStateForAlertIDLUTime	—
GetInstructions	Retrieves alert instructions using the pxAlert context.
GetLocationAndSensorName	Retrieves the monitoring area/zone and sensor name associated with an alert from the pxAlert context.
GetSensorForSensorID	—
GetSiblingSensors	Discovers sensors in the same sensor group or monitoring area using the pxEvent context.
GetThreatLevel	Retrieves the current Homeland Security or MARSEC threat level.
GetUserGroups	Retrieves the security groups defined in PSOM.
GetUsers	Retrieves the users defined in PSOM.
IsZoneInHierarchy	Determines whether a monitoring zone exists in the monitoring hierarchy.
SetAlertStatus	Sets the status for an alert by updating the pxAlert object.
SimulateAlert	Simulates an alert in PSOM.
UpdateAlertSeverity	Changes an alert's severity by updating the pxAlert object.

Understanding Activity Contexts

Since you can use PowerShell scripts to interact with any Activity component in a Business Logic flow, you must understand the category and key used for various Activities in PSOM Business Logic.

To save and retrieve the contexts inside an Activity, you can use the IPxActivityContainer.PxContexts object to interact with the contexts. The IPxActivityContainer should be the parent of the current executing activity.

Table 14-6 Activity Context Category and Key Information

Category	Description	Keys
PxAlert	Alert-related information for the context. All alert related global variables can be stored inside this context category	• Alert—The XML serialized string for the alert context. • AlertObject—The object presentation of the WF alert.
PxEvent	Pre-alert related contextual information. All pre-alert related data can be stored in this context category to pass on between activities.	• PxEvent—The XML serialized string of the PxEvent object. • AlertID—The new alert ID created from PxEvent.
PxHealthCheck	Health check related contextual information. Health alerts can be used to create either user alerts or admin alerts.	• PxHealthAlert—XML serialized string of the PxHealthAlert object.
PxData	Other data information that can be passed between activities such as data sets and data query results.	• ResultDataSet—The dataset that can be passed between an ODBC Action activity and the Create Report activity. • ODBCResult—The result data (scalar) from an ODBC Condition activity.
PxWebServiceCallResult	External data result from other data sources.	• Key—The name of the activity.
PxGIS	Current GIS location information stored in the context registry.	• CurrentLocation—The current GIS location as stored in the context registry.
PxWS	Context information related to PxWS.	• PxLoginID—The login ID under which the current activity is operating.
PxMethod	Data related to PxMethod calls in string/xmlstring format.	• ResultString—The result data from a Call External Method activity. • CallerContext—The context of the invoking PxMethod business logic activity (if any).

Table 14-6 Activity Context Category and Key Information (continued)

Category	Description	Keys
PxSensor	Sensor related contextual information.	• SensorID—The sensor ID for the applicable sensor (not DID). • AreaID—The current monitoring area ID for the sensor context. • ZoneID—The current monitoring zone ID for the sensor context.
ScheduleBl	Information for the Schedule Business Logic.	• ScheduledTime—The scheduled time (in UTC) to run the current business logic instance.

Use %Contexts.Category.Key% to refer to the current value of the context object. The value will be replaced with the actual context object's ToString() value during activity runtime.

If you are using a PowerShell Action or Decision activity as a subsequent activity, you can use the $pxContext object to retrieve and send context data.

Performing Health Checks Using PowerShell Scripts

You can perform regular health checks from Schedule Business Logic, including:

- Ping Test—Pings a remote network device. It generates an operator alert when a response is not received within the specified timeframe.
- HTTP Link Test—Verifies whether a connection can be established with a particular URL. HTTPS is also supported. An alert is generated if a connection to the URL cannot be made.
- Service Test—Verifies that a particular service or set of services is running. An alert is generated if one of the service(s) is not running. In order to ping services remotely, the Business Logic Core Service has to be installed using a domain user account with administrative privileges on all monitored machines.

The results of the test determine the decision made by the activity. The results are also output to the context registry for additional actions; for example, creating administrative or user alerts.

These PowerShell scripts are available from **Business Logic > PowerShell Scripts**.

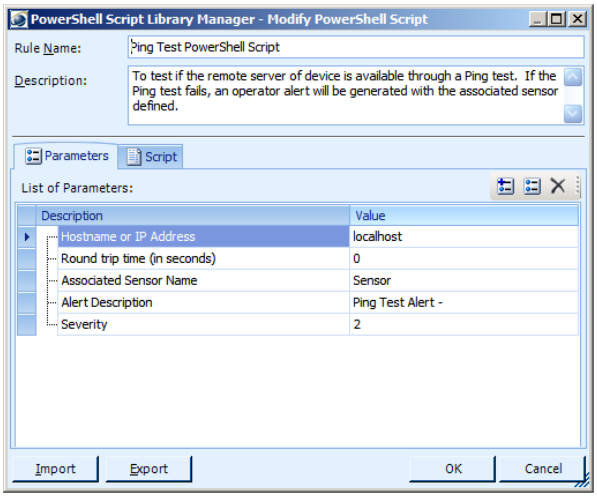
Ping Test

Pings a remote network device. When the device is down, an operator alert is generated.

To set properties for the Ping Test script:

Step 1 Select the **Ping Test** script in the **Business Logic Policy Manager** window, click **Manage Policy**, and click **Modify**.

The Modify PowerShell Script window appears.



Step 2 Enter the hostname or IP address of the server you want to ping in the **Hostname or IP Address** field.

Step 3 Enter the number of seconds to wait for a response before generating an alert in the **Round trip time (in seconds)** field.

Step 4 Enter the name of the sensor or tracking device with which this ping test is associated in the **Associated Sensor Name** field. If an alert is raised, it will be raised against this sensor.

Step 5 Enter the alert message that should be included if an alert is raised in the **Alert Description** field.

Step 6 Enter the severity that should be assigned to the alert in the **Severity** field. The default is 2 (Medium).

Step 7 Click **OK**.

Step 8 Create a Schedule Business Logic and add this Ping Test as a component.

Service Test

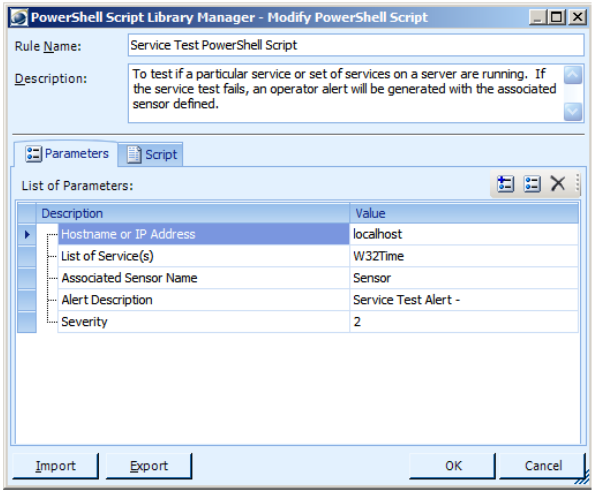
Verifies that a particular service or set of services is running. An alert is generated if one of the service(s) is not running.

Note In order to ping services remotely, the Business Logic Core Service has to be installed using a domain user account with administrative privileges on all monitored machines.

To set properties for the Service Test script:

Step 1 Select the **Service Test** script in the Business Logic Policy Manager window, click **Manage Policy**, and click **Modify**.

The Modify PowerShell Script window appears.



Step 2 Enter the hostname or IP address of the server where the services are running in the **Hostname or IP Address** field.

Step 3 Enter the list of services you want to verify are running in the **List of Service(s)** field.

Step 4 Enter the name of the sensor or tracking device with which this services test is associated in the **Associated Sensor Name** field. If an alert is raised, it will be raised against this sensor.

Step 5 Enter the alert message that should be included if an alert is raised in the **Alert Description** field.

Step 6 Enter the severity that should be assigned to the alert in the **Severity** field. The default is 2 (Medium).

Step 7 Click **OK**.

Step 8 Create a Schedule Business Logic and add this Service Test as a component.

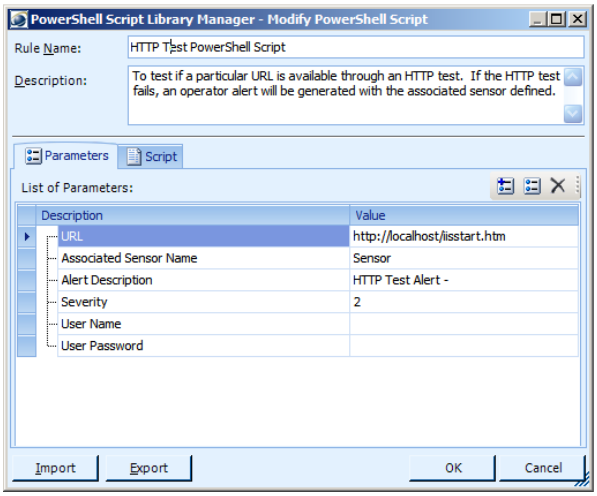
HTTP Test

Verifies whether a connection can be established with a particular URL. HTTPS is also supported. An alert is generated if a connection to the URL cannot be made.

To set properties for the HTPP Test script:

Step 1 Select the **HTTP Test** script in the Business Logic Policy Manager window, click **Manage Policy**, and click **Modify**.

The Modify PowerShell Script window appears.



Step 2 Enter the URL you want to connect to in the **URL** field.

Step 3 Enter the name of the sensor or tracking device with which this HTTP test is associated in the **Associated Sensor Name** field. If an alert is raised, it will be raised against this sensor.

Step 4 Enter the alert message that should be included if an alert is raised in the **Alert Description** field.

Step 5 Enter the severity that should be assigned to the alert in the **Severity** field. The default is 2 (Medium).

Step 6 If authentication is required by the URL with which you are connecting, enter login credentials in the **User Name** and **User Password** fields.

Step 7 Click **OK**.

Step 8 Create a Schedule Business Logic and add this HTTP Test as a component.

CHAPTER 15

Business Logic Component Reference

Using business logic templates, you can capture the unique business processes and procedures for responding to alerts within your environment. Business logic templates are built using different components that can be dragged into your workspace to define the conditions that must be met for certain actions to occur.

This chapter includes these topics:

- Understanding Business Logic Components, page 15-2
- Configuring Delay Properties, page 15-7
- Configuring Call Child Logic Properties, page 15-8
- Configuring Call Everbridge Properties, page 15-9
- Configuring Call External Method Properties, page 15-11
- Configuring Call Web Service Properties, page 15-15
- Configuring Create Admin Alert Properties, page 15-16
- Configuring Create Alert Properties, page 15-17
- Configuring Create Report Properties, page 15-18
- Configuring DOS Command Properties, page 15-21
- Configuring HTTP Send Properties, page 15-22
- Configuring IPICS Dispatch Alert Properties, page 15-23
- Configuring IPICS Notify Alert Properties, page 15-24
- Configuring ODBC Action Properties, page 15-25
- Configuring PowerShell Action Properties, page 15-26
- Configuring PTZ Control Properties, page 15-29
- Configuring Send Email Properties, page 15-31
- Configuring Set Alert Context Properties, page 15-33
- Configuring Set Alert Severity Properties, page 15-34
- Configuring Set Alert Status Properties, page 15-35
- Configuring Alert Condition Properties, page 15-35
- Configuring Geo-Location Properties, page 15-37
- Configuring Monitor Hierarchy Properties, page 15-38
- Configuring Schedule Condition Properties, page 15-39

- Configuring Threat Level Properties, page 15-41
- Configuring Simulate Alert Properties, page 15-42
- Configuring Simulate Contexts Properties, page 15-43
- Configuring Simulate Event Properties, page 15-45
- Configuring Correlate Condition Properties, page 15-46
- Configuring Event Map Filter Properties, page 15-51
- Configuring Escalate Condition Properties, page 15-56
- Configuring ODBC Condition Properties, page 15-57
- Configuring PowerShell Decision Properties, page 15-58
- Configuring RSS Alerts Properties, page 15-63
- Configuring Lock Door Properties, page 15-66
- Configuring Open Door Properties, page 15-68
- Configuring Open Door Momentarily Properties, page 15-70

Understanding Business Logic Components

Business logic components include these basic types:

- Action—Shaped like a rectangle, these components define what should happen when conditions are met and have a single output point. For example, the Start component launches the execution of the business logic template; every business logic template must begin with a Start component.
- Decision—Shaped like a Rhombus, these components specify conditions under which certain actions should occur, and have multiple output points.
- Simulators—These components simulate actions for testing purposes. For example, the SimulateAlert component simulates alerts for the business logic.
- Decision+Action—Shaped like a rectangle + rhombus, these components specify conditions under which specific actions should occur, and have multiple output points.
- Sensor Commands—Shaped like a rectangle, these components execute functionality against sensors; for example, LockDoor can be used to lock an access control sensor.

Note While components differ on the number of output points, they all have a single input point; you can, however, have multiple connectors leading to the input point for a component.

Table 15-1 shows and describes the components for designing a business logic template.

Table 15-1 Icons Used in Business Logic Template Design

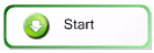
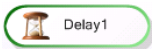
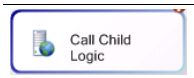
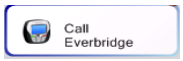
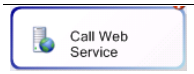
This Icon...	This Type of Component...	Performs this Action...	For Example, When...	For Details See...
	Start	Serves as the starting point of the business logic template.	You want to initiate business logic. The Start icon is a mandatory activity always to be included as the very first activity for business logic.	—
	Delay	Waits for a specified amount of time and then passes action to the next icon.	You want to wait five minutes before rechecking the current status of the alert.	"Configuring Delay Properties" section on page 15-7.
	Call Child Logic	Calls "sub logic" defined in a separate business logic template.	You want to divide business logic into multiple business logic templates and link templates together using CallChildLogic.	"Configuring Call Child Logic Properties" section on page 15-8.
	Call Everbridge	Executes an Everbridge notification service.	You want to call a large group of phone numbers in an emergency and keep track of which numbers reached people, and which were busy.	"Configuring Call Everbridge Properties" section on page 15-9.
	Call External Method	Dynamically invokes a web method on an external 3rd-party system using the External Method Dispatcher Service.	You want to execute a method on an external 3rd-party system directly from PSOM; for example, turn on all the lights in the building.	"Configuring Call External Method Properties" section on page 15-11.
	Call Web Service	Dynamically invokes a web method on a SOAP-based Web Service.	You want to collect information from the user while the business logic is executing.	"Configuring Call Web Service Properties" section on page 15-15.
	Create Admin Alert	Generates PSOM alerts from raw Integration Module events.	You want to create alerts in PSOM when events occur in Integration Modules.	"Configuring Create Admin Alert Properties" section on page 15-16.
	CreateAlert	Generates a PSOM alert.	You want to create an alert in PSOM.	"Configuring Create Alert Properties" section on page 15-17.
	Create Report	Generates the specified report.	You want to create an Alert Details report for the alert that was raised.	"Configuring Create Report Properties" section on page 15-18.

Table 15-1 Icons Used in Business Logic Template Design (continued)

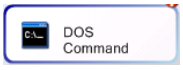
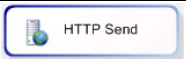
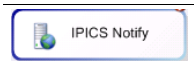
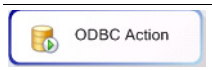
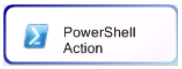
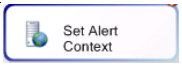
This Icon...	This Type of Component...	Performs this Action...	For Example, When...	For Details See...
	DOS Command	Invokes an external application through the command line.	You want to execute a DOS batch file when a certain type of alert is raised.	"Configuring DOS Command Properties" section on page 15-21.
	HTTP Send	Calls into an HTTP URL and returns an HTTP response.	You want to invoke external data listening services through simple URLs.	"Configuring HTTP Send Properties" section on page 15-22.
	IPICS Dispatch Alert	Dispatches an alert to IPICS via the IPICS Integration Module.	You want to dispatch an alert to IPICS.	"Configuring IPICS Dispatch Alert Properties" section on page 15-23.
	IPICS Notify	Executes IPICS policies on an IPICS Server version 4.0.	You want to notify Emergency Services about an alert in PSOM via IPICS Server.	"Configuring IPICS Notify Alert Properties" section on page 15-24.
	ODBC Action	Runs custom ODBC SQL scripts against the specified data source and returns a dataset to the activity context registry.	You want to update a datasource as part of executing business logic in PSOM.	"Configuring ODBC Action Properties" section on page 15-25.
	PowerShell Action	Allows PowerShell scripts to be executed as part of business logic processing.	You have a PowerShell script that you want to execute as part of your business logic.	"Configuring PowerShell Action Properties" section on page 15-26.
	PTZ Control	Sends PTZ camera control commands to the Camera PTZ Control Service.	You want to move PTZ cameras to certain views on a schedule.	"Configuring PTZ Control Properties" section on page 15-29.
	Send E-Mail	Sends an email to the address configured in its properties.	You want to send an email when a high priority alert is raised.	"Configuring Send Email Properties" section on page 15-31.
	Set Alert Context	Dynamically switches the current alert context to a different alert by specifying a dynamic alert ID.	You want to dynamically change the current alert context or invoke alert-based business logic from other business logic types using a CallChildLogic activity (for example, from a Scheduled Business Logic).	"Configuring Set Alert Context Properties" section on page 15-33.

Table 15-1 Icons Used in Business Logic Template Design (continued)

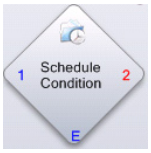
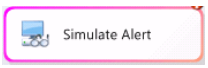
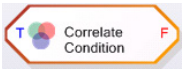
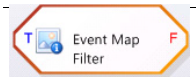
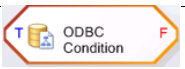
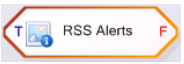
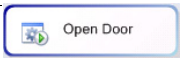
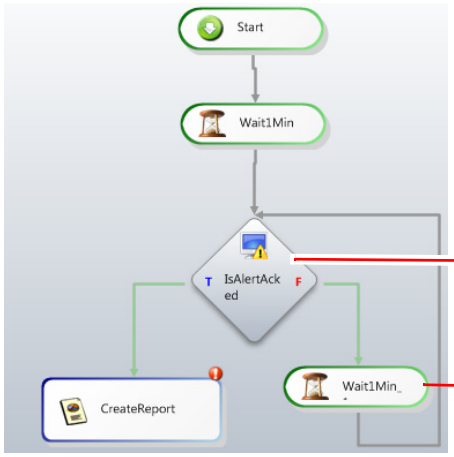
This Icon...	This Type of Component...	Performs this Action...	For Example, When...	For Details See...
	Set Alert Severity	Changes the current alert's severity level.	You want to upgrade the severity of an alert based on the current Homeland Security level.	"Configuring Set Alert Severity Properties" section on page 15-34.
	Set Alert Status	Changes the current status of the alert (Acknowledged, Closed, Deleted).	You want to automatically change an alert's status to Deleted during system-wide testing.	"Configuring Set Alert Status Properties" section on page 15-35.
	Alert Condition	Decides which branch of the business logic to execute based on the severity and description of the alert passed to it.	You want to execute alternate business logic for alerts with a High severity level, or alerts of a certain type.	"Configuring Alert Condition Properties" section on page 15-35.
	Geo-Location	Decides which branch of the business logic to execute based on whether the current GPS location is within the specified boundary.	You want to take different actions for alerts that occur within and outside a certain area.	"Configuring Geo-Location Properties" section on page 15-37.
	Monitor Hierarchy	Decides which branch of the business logic to execute based on the monitoring zones or areas issuing the alert passed to it.	You want do take different actions for alerts that occur in tight security zones versus public zones.	"Configuring Monitor Hierarchy Properties" section on page 15-38.
	Schedule Condition	Decides which branch of the business logic to execute based on the schedule specified within it.	You want take different actions for alerts that occur during the dayshift versus the nightshift.	"Configuring Schedule Condition Properties" section on page 15-39.
	Threat Level	Decides which branch of the business logic to execute based on the Homeland Security or MARSEC threat level and the alert passed to it.	You have different security policies when Homeland Security levels are high versus low.	"Configuring Threat Level Properties" section on page 15-41.
	Simulate Alert	Simulates an alert during testing in the Business Logic Designer.	You want simulate the creation of an alert for testing purposes.	"Configuring Simulate Alert Properties" section on page 15-42.
	Simulate Contexts	Simulates a context during testing of On-Demand business logic in the Business Logic Designer.	You want to simulate a monitoring area context to test on-demand business logic.	"Configuring Simulate Contexts Properties" section on page 15-43.

Table 15-1 Icons Used in Business Logic Template Design (continued)

This Icon...	This Type of Component...	Performs this Action...	For Example, When...	For Details See...
	Simulate Event	Simulates an event during testing of Event Business Logic.	You want to simulate the creation of an event for testing purposes.	"Configuring Simulate Event Properties" section on page 15-45.
	Correlate Condition	Allows multiple alarms to be correlated across multiple systems to raise additional alarms, raise severity of alarms, or close or acknowledge existing alarms.	You want to correlate a fence system alert with an intelligent video system alert.	"Configuring Correlate Condition Properties" section on page 15-46.
	Escalate Condition	Escalates the alert to a specified user or group based on certain criteria.	You want to enforce an automated alert escalation policy for open alerts.	"Configuring Escalate Condition Properties" section on page 15-56.
	Event Map Filter	Allows you to filter through Integration Module events in an event monitoring business logic template.	You want to execute business logic for certain events, but not others.	"Configuring Event Map Filter Properties" section on page 15-51.
	ODBC Condition	Runs custom ODBC SQL scripts against the specified data source and returns true/false to make a decision.	You want to use values in a datasource to make a decision within business logic.	"Configuring ODBC Condition Properties" section on page 15-57.
	PowerShell Decision	Allow a PowerShell scriptblock to be executed inside a component and return the result (TRUE or FALSE) to the business logic template for decision.	You have a PowerShell script that you want to execute as part of your business logic.	"Configuring PowerShell Decision Properties" section on page 15-58.
	RSSAlerts	Aggregates RSS or ATOM feeds.	You want to filter through RSS or ATOM feed items and create corresponding alerts in PSOM.	"Configuring RSS Alerts Properties" section on page 15-63.
	Lock Door	Issues a "Lock Door" command to Integration Module door sensors.	You want to lock an access control sensor remotely.	"Configuring Lock Door Properties" section on page 15-66.
	Open Door	Issues an "Open Door" command to Integration Module door sensors.	You want to open an access control sensor remotely.	"Configuring Open Door Properties" section on page 15-68.
	Open Door Momentarily	Issues an "Open Door Momentarily" command to Integration Module door sensors.	You want to open an access control sensor remotely for just a moment.	"Configuring Open Door Momentarily Properties" section on page 15-70.

Configuring Delay Properties

When you add a Delay component to your business logic template, you can configure the amount of time it should wait before passing action to the next icon. Delay components are useful for constructing loops whereby you repeatedly check to see if a condition is true—for example, whether an alert has been acknowledged—before taking an action. Delay loops are most useful in conjunction with the AlertCondition component which can be used to recheck the state of an alert, as shown next.

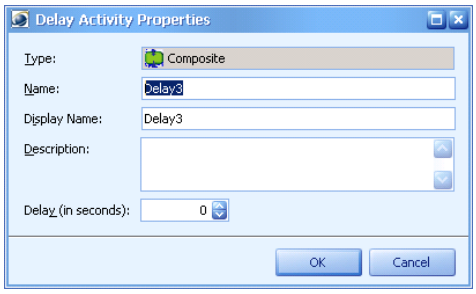


Note When using a Delay loop, be sure to set the delay to some number of seconds to prevent the loop from running continuously, which will impact the performance of PSOM.

To set properties for the Delay component:

Step 1 Select the **Delay** icon in the workspace and click **Properties**.

The Delay Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter the amount of time that action should be delayed in the **Delay (in seconds)** field.

Step 6 Click **OK**.

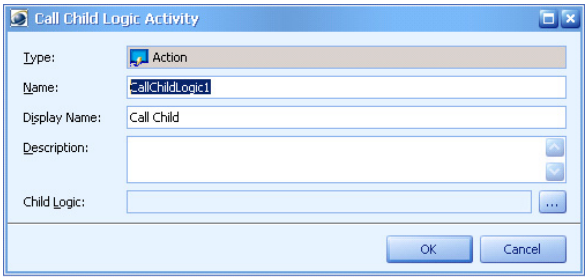
Configuring Call Child Logic Properties

The Call Child Logic activity can make calls to "sub logic" defined in separate business logic templates. You can divide business logic into multiple business logic templates and then link them together using the Call Child Logic activity.

To set properties for the Call Child Logic Activity component:

Step 1 Select the **Call Child Logic** icon in the workspace and click **Properties**.

The Call Child Logic Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Click the button next to the **Child Logic** field to browse and select the child logic template.

Step 6 Click **OK**.

Note You can nest a Call Child Logic activity inside a business logic template. This allows you to create complex business logic flows using multiple levels of composition.

When you debug or test a Call Child Logic activity inside the Business Logic Designer, the Call Child Logic within the business logic template will not actually run. This limitation will be addressed in future releases. Currently you have to apply the business logic template that contains the Call Child Logic activity before it will take effect.

Each time you change the definition or parameters of a Call Child Logic activity, the business logic template that contains it will be affected as well. Keep this in mind when you modify a Call Child Logic activity.

If the Call Child Logic activity is part of an Alert Business Logic template, the alert audit trail will record the Call Child Logic activity's name with an extra GUID postfix. This postfix is needed to uniquely identify the activities across all levels of the template, regardless whether it is defined in the parent template or the child template.

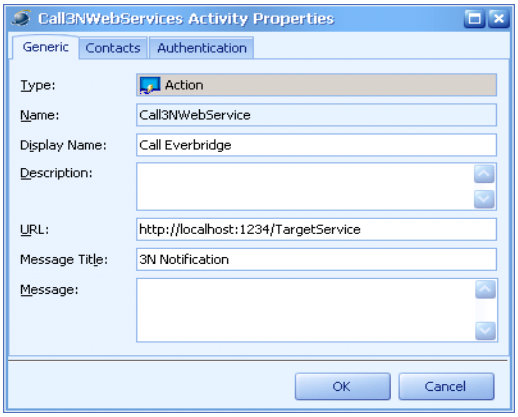
Configuring Call Everbridge Properties

When you add a Call Everbridge component to your business logic template, you can generate an Everbridge notification service for mass notification via multiple channels such as e-mail, phone, or SMS text. For example, you can call a set of numbers and keep track of which numbers reached people, which numbers were busy, and so on. Access to Everbridge is through a URL/Web Service to which PSOM passes parameters—such as whether you want voice or text messages, or which groups you want to send the communication.

To set properties for the Call Everbridge component:

Step 1 Select the **Call Everbridge** icon and click **Properties**.

The Call Everbridge Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

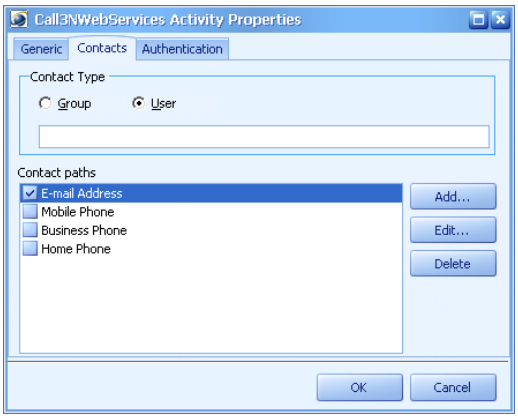
Step 5 Enter the web service URL for the Everbridge software in the **URL** field.

Step 6 Enter a title for the message in the **Message Title** field.

Step 7 Enter the message you want to send in the **Message** field.

Note The message cannot contain invalid characters such as: & < > / " "

Step 8 Click the **Contacts** tab.

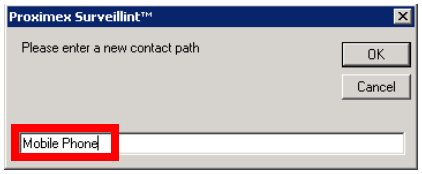


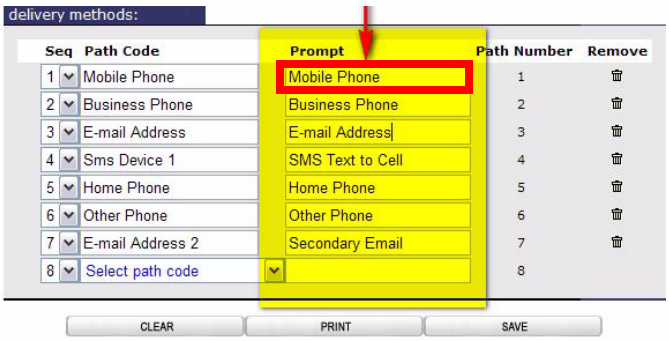
Step 9 In the **Contact Type** area, determine whether to send a notification to a group of users (**Group**), or to specific users (**User**).

Step 10 In the field provided, enter group or user names separated by semicolons. For user names, use the format of *FirstName LastName; FirstName LastName*

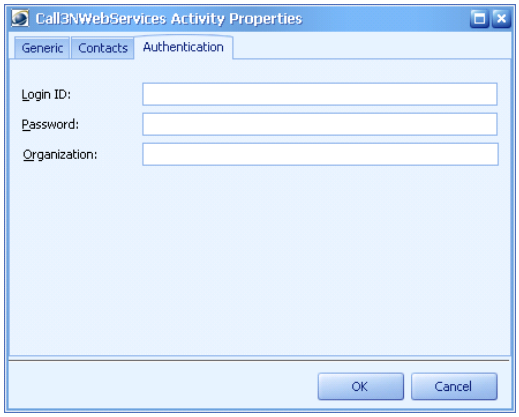
Step 11 In the **Contact Path** area, determine what kind of notification to send: **Email**, **Mobile Phone** (SMS text), **Business Phone**, or **Home Phone**.

You can add a contact path by clicking **Add**. Enter the contact path (for example, "Email-Home"), and click **OK**. The contact path needs to have the exact wording as the "Prompt" specified in the delivery method within Everbridge.





Step 12 Click the **Authentication** tab.



Step 13 In the **Login ID** field, enter your numerical ID to the Everbridge website.

Step 14 In the **Password** field, enter the corresponding password for your Everbridge account.

Step 15 In the **Organization** field, enter the organization assigned to your login for Everbridge.

Step 16 Click **OK**.

Configuring Call External Method Properties

The Call External Method Activity is an Action activity that can dynamically invoke any external commands statically or dynamically registered with PSOM Bus Service. When the business logic executes, contexts are dynamically converted into actual values (i.e. PxSensor, PxAlert) by the Call External Method activity, before it calls the PSOM Bus Service to invoke the method on the target 3rd party system or PSOM Services.

You need to configure PSOM Bus Service before configuring the Call External Method Activity. See the *Installing Cisco Physical Security Operations Manager* guide for instructions.

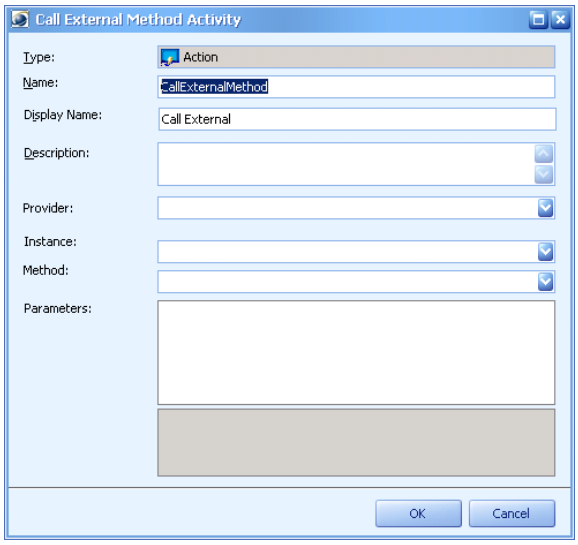
Since the Call External Method Activity component communicates with the PSOM Bus Service to retrieve the provider and method lists, the PSOM Bus Service must be running before you can configure this component.

If the call is successful, the returned result is added to the context register under the PxMethod category and ResultString key. You can use a PowerShell activity to retrieve the returned result.

To set properties for the Call External Method component:

Step 1 Select the **Call External Method** icon in the workspace and click **Properties**.

The Call External Method Activity window appears.

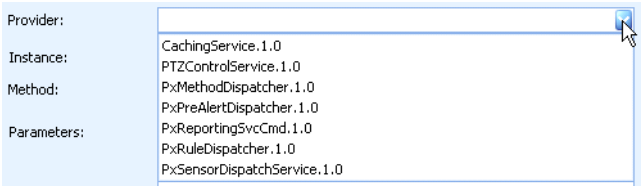


Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

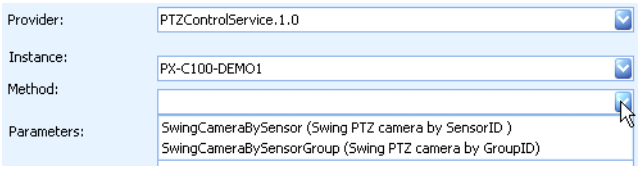
Step 4 Enter information about the component in the **Description** field.

Step 5 Select the provider you want to access using this component from the **Provider** field. The provider might be an external 3rd-party system, or it might be a PSOM Service.

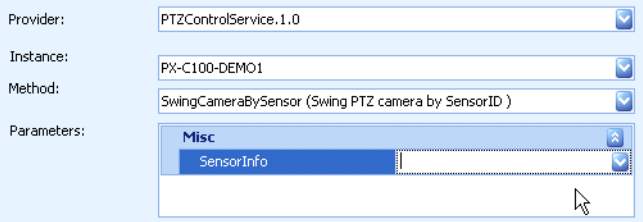


Step 6 Select the instance of the 3rd-party system or PSOM Service you want to access using this component from the **Instance** field.

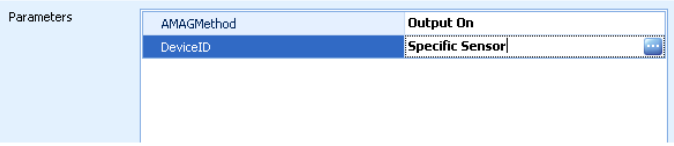
Step 7 Select the method you want to invoke from the **Method** field. This field is populated based on your selections from the **Provider** and **Instance** fields.



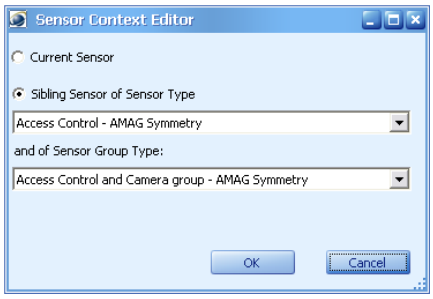
Step 8 Provide values for parameters in the **Parameters** area.

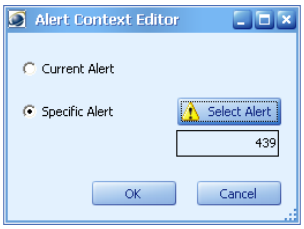


If the parameter is a complex data type (i.e. a sensor or an alert), you will see the "..." button when you double click on the parameter.

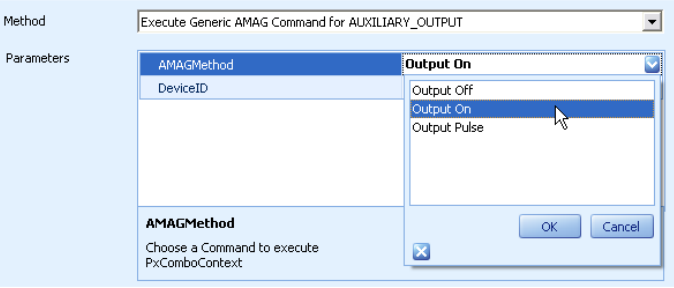


Click the ... button to make a selection. One of the following windows appears depending on whether you're selecting a sensor or an alert.





If the parameter is defined as a pick list, select a value from the drop-down menu.



Step 9 Click **OK**.

Table 15-2 lists methods you can invoke on PSOM Services using the Call External Method activity in business logic.

Table 15-2 External PSOM Commands

Method	Provider	Description
AdHocUpdateSensor	PxSensorDispatchService	Requests that the PSOM Sensor Management Services synchronize its list of sensors on-demand.
DeployRule	PxRuleDispatcher	Deploys an existing business logic rule. The RuleID parameter takes a string that is the name of the business logic rule to be deployed.
GetAlertMiniMap	PxReportingSvcCmd	Retrieves the mini map JPG for the associated alert from the PSOM Reporting Services and then encodes the JPG as a Base64 string for the return result. The CommandText parameter contains the detail command in XML format to the PSOM Reporting Services. The return result is similar to the following: <ReportingServiceResult> <REPORTTYPE>AlertMiniMap</REPORTTYPE> <RESULT><![CDATA [/9j/4AAQSkZJRgABAQE2siyzmQRZZD5hCkGUkLhuB17100Og6Tb y3EsGl2UT3EiyTPHbopkdTuVmIHR3MFleyJaCJVmkx91mn3fxo2B GwRA2S3T29qKKQH/9k=]]></RESULT> </ReportingServiceResult> Where CDATA is the UUencoded image binary data.
RefreshCache	CachingService	Refreshes the cache maintained by the PSOM Caching Service.
RefreshCommandsList	PxMethodDispatcher	Refreshes the list of commands registered with the dispatcher (PSOM BUS Service).
RefreshSysAlertCache	PxPreAlertDispatcher	Refreshes the cache of system alerts for monitoring business logic maintained by the Business Logic Services.
RequestCacheRefresh	PxReportingSvcCmd	Requests that the PSOM Reporting Services refresh its cache of sensors, monitoring hierarchies, area maps, and so on. The cache will be refreshed after a 30 second delay.
RequestReport	PxReportingSvcCmd	Requests that a specified report be generated by the PSOM Reporting Services. The CommandText parameter contains the detail command in XML format to the PSOM Reporting Services.
SwingCameraBySensor	PTZ Control Service	Swing a PTZ camera to a specified view. Takes the SensorInfo parameter which is an XML string containing a single sensor ID and a single sensor view ID. <SensorInfo> <SensorID>101</SensorID> <SensorViewID>102</SensorViewID> </SensorInfo>

Table 15-2 External PSOM Commands (continued)

Method	Provider	Description
SwingCameraBySensorGroup	PTZ Control Service	Swing all PTZ cameras in one or more sensor groups. Takes the GroupInfo parameter which is an XML string containing one or more sensor group ID(s). <GroupInfo> <SensorGroupID>101</SensorGroupID> <SensorGroupID>102</SensorGroupID> </GroupInfo> Sensor view is specified in the Administration Console when you configure sensor groups that contain PTZ cameras.
UndeployRule	PxRuleDispatcher	Undeploys an existing business logic rule. The RuleID parameter takes a string that is the name of the business logic rule to be undeployed.

Configuring Call Web Service Properties

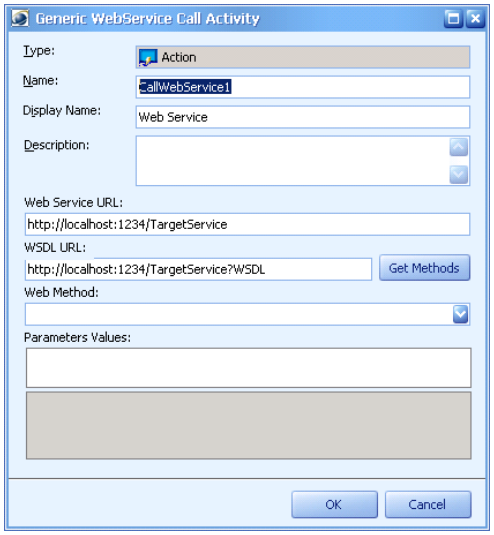
When you add a Call Web Service component to your business logic template, you can dynamically invoke SOAP-based web services by suppling a Web Services Description Language (WSDL) location at design time, and then through introspection allowing the user to invoke a method and pass parameters to it. The parameter values can be specified or determined using templates (template values will be substituted with actual values at runtime).

Return results from this component are stored in the context registry under the PxWebServiceCallResult category where the key is the name of the activity.

To set properties for the Call Web Service component:

Step 1 Select the **Call Web Service** icon in the workspace and click **Properties**.

The Generic WebService Call Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter the URL where the web service is running in the **Web Service URL** field.

Step 6 Enter the URL to the location of the web service's WSDL file in the **WSDL URL** field.

Step 7 Click the **Get Methods** button to retrieve the list of available web methods defined in the target web service. The **Web Method** field is populated with the list of available methods.

Step 8 Select the web method that the activity should call in the **Web Method** field.

Step 9 The list of parameters for the selected web method are populated in the **Parameters Values** area. The dynamic parameter list not only shows the parameter name, but it also shows the data type of the parameter at the bottom of the list.

When specifying parameter values, you can specify either exact values or value templates using available global variables, such as %ALERTID%, %LOGONID%, and so on. These global variables will be replaced with their actual values during runtime. See the "Using Global System Variables in Business Logic" section on page 14-51 for a list of system variables.

Step 10 Click **OK**.

Configuring Create Admin Alert Properties

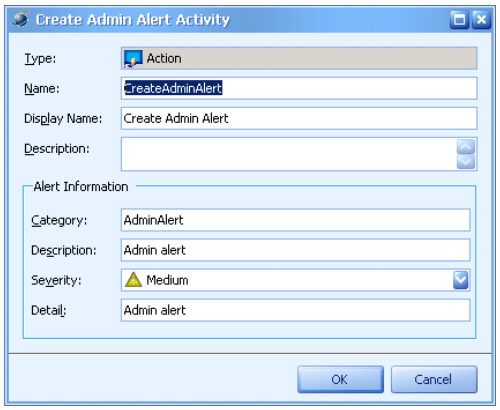
The Create Admin Alert activity allows you to generate PSOM alerts from raw events received from external systems using the Integration Modules.

Note If you want to associate video cameras with alerts, you need to create sensor groups that include cameras and the access control devices to which they relate.

To set properties for the Create Admin Alert component:

Step 1 Select the **Create Admin Alert** icon in the workspace and click **Properties**.

The Create Admin Alert Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter the type of alerts you want to create in the **Category** field. The default value is AdminAlert.

Step 6 Enter a description of the alert type in the Description field.

Step 7 Select the severity level for alerts created by the Create Admin Alert Activity from the **Severity** field.

Step 8 Enter information about the alert to be created in the **Detail** field.

Step 9 Click **OK**.

Configuring Create Alert Properties

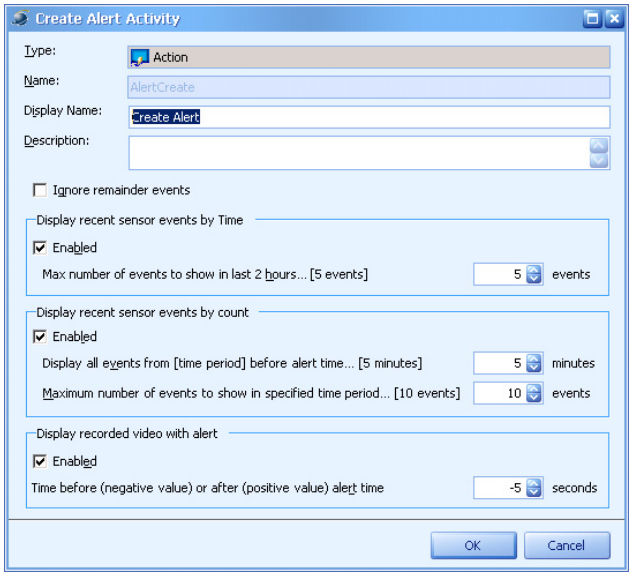
The Create Alert activity allows you to generate PSOM alerts from raw events received from external systems using the Integration Modules.

Note If you want to associate video cameras with alerts, you need to create sensor groups that include cameras and the access control devices to which they relate.

To set properties for the Create Alert component:

Step 1 Select the **Create Alert** icon in the workspace and click **Properties**.

The Create Alert Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 If you check the **Ignore remainder events** option, all Integration Module events that do not match a PSOM sysalert name will be ignored. By default this option is unchecked.

Step 6 If you want to be able to view recent events by time, check the **Enable** option in the **Display recent sensor events by time** area, and specify the maximum number of events to show in the last 2 hours (default to 5).

Step 7 If you want to be able to view recent events by count, check the **Enable** option in the **Display recent sensor events by count** area, and specify the number of minutes duration that you want to display all events that occurred. You can also specify the maximum number of events that can be shown for the duration.

Step 8 If you want to display recorded video with alerts, check the **Enable** option in the **Display recorded video with alert** area, and specify the duration of recorded video that will be associated with the alert.

Step 9 Click **OK**.

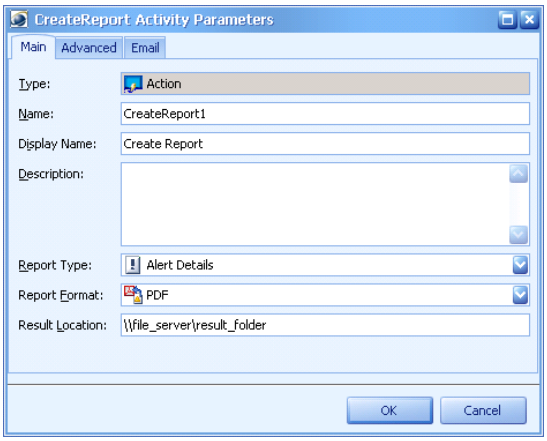
Configuring Create Report Properties

When you add a Create Report component to your business logic template, you can generate an Alert Details report based on the alert being handled by the business logic. This component supports table-based reports; the tabular data can come from the ODBCAction activity (see the "Configuring ODBC Action Properties" section on page 15-25). You can also specify SMTP server locations to have the activity to automatically email the created report once it is created.

To set properties for the Create Report component:

Step 1 Select the **Create Report** icon in the workspace and click **Properties**.

The Create Report Activity Parameters window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

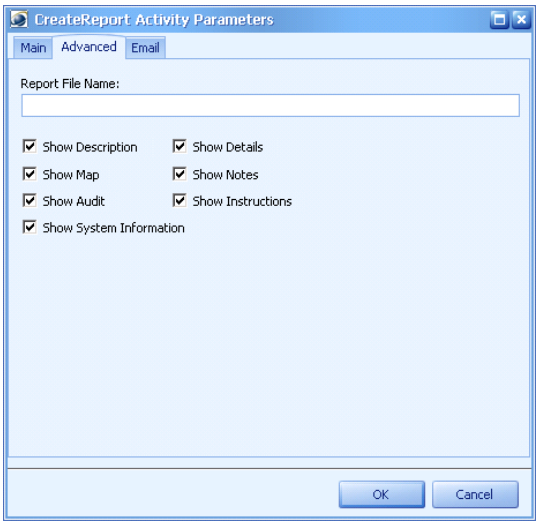
Step 5 Choose the report you want to generate from the **Report Type** field. For this release, only the Alert Details report or a complete DataSet for the alert can be created.

Step 6 Choose the output format for the report from the **Report Format** field: PDF, Image, Text, HTML, or MHT.

Step 7 Enter the location in your network where you want to save the report in the **Result Location** field. If a file with the same specified name exists already, the Reporting Services will overwrite it with the latest report data.

Note Since all reports are actually generated from the Reporting Services, make sure the location you specify is writeable from the Reporting Services' service account. It is recommended that this folder be either a public file share folder or a local folder on the machine that runs Reporting Services.

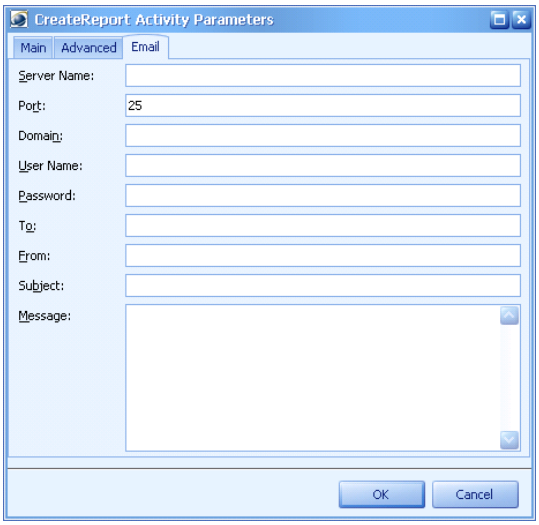
Step 8 To specify the information to be included in the report, click the **Advanced** tab.



Step 9 Enter a specific name to assign to the report in the **Report File Name** field. The correct extension for the type of report will be added; for example, you do not need to specify ".pdf" at the end of the filename.

Step 10 Check options for the information you want included in the report.

Step 11 If you want to automatically email the report once it has been generated, click the **Email** tab. PSOM Reporting Services will email the generated report to the specified recipients.



Step 12 Enter the host name or IP address of your email server in the **Server Name** field.

Step 13 Enter the port number under which the email server is running in the **Port** field.

Step 14 Enter the name of the email server domain in the **Domain** field.

Step 15 Enter the login name of the user account that is used to send out email in the **User Name** field.

Step 16 Enter your email system password in the **Password** field.

Step 17 Enter the email address for the person who is sending the email notification in the **To** field.

Step 18 Enter the email addresses for all persons that should receive this email notification in the **From** field.

Step 19 Enter the subject of the email in the **Subject** field. Global system variables are not supported in the email subject.

Step 20 Enter the message you want to send in the **Message** field. Global system variables are not supported in the email body.

Step 21 Click **OK**.

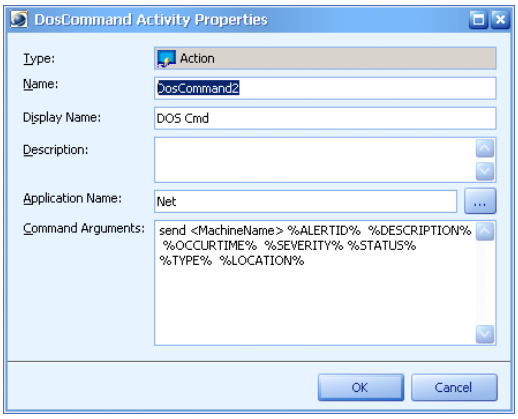
Configuring DOS Command Properties

When you add a DOS Command component to your business logic template, you can select the external application that should be launched through the command-line, and send command-line arguments to that application.

To set properties for the DOS Command component:

Step 1 Select the **DOS Command** icon in the workspace and click **Properties**.

The DosCommand Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Click the button next to the **Application Name** field to select the external batch file or executable that should be launched. The application must be located on the machine where PSOM Server was installed.

Step 6 In the **Command Arguments** field, enter the parameters that will be passed to the application. See the "Using Global System Variables in Business Logic" section on page 14-51 for details.

Note These system variables are only applicable when the activity is included in an Alert Business Logic or Alert Status Business Logic template. Other business logic templates do not process these variables.

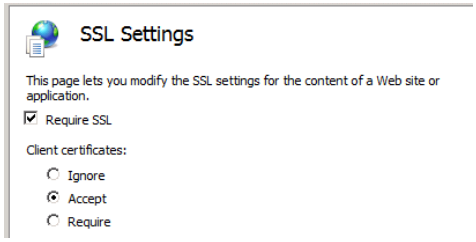
Step 7 Click **OK**.

Configuring HTTP Send Properties

The HTTP Send Activity can make calls into a HTTP URL and return the HTTP response to the business logic. You can use this activity to invoke external data listening services through simple URLs.

The HTTP return result is stored in the context registry under the HttpResult category and ResultString key. Retrieve the result string using a PowerShell script. See the "PowerShell Action Examples" section on page 15-28.

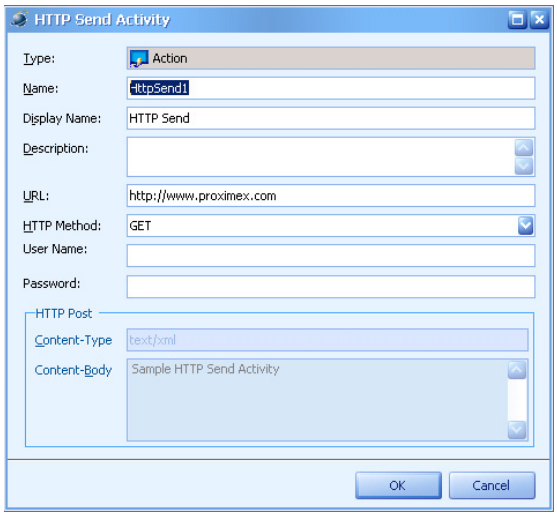
Note The HTTP Send Activity can support some HTTPS calls that require SSL. The exception are those web sites that require client certificate validation. For IIS 7.0, the following site configuration should allow the HTTP Send Activity to function.



To set properties for the HTTP Send Activity component:

Step 1 Select the **HTTP Send** icon in the workspace and click **Properties**.

The HTTP Send Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter the URL that the activity should invoke during execution in the **URL** field. PSOM system variables are supported for the URL. For example:

http://*yourserviceurl***/sendAlert?AlertID=%ALERTID%**

See the "Using Global System Variables in Business Logic" section on page 14-51 for a list of system variables.

Note These system variables are only applicable when the activity is included in an Alert Business Logic or Alert Status Business Logic template. Other business logic templates do not process these variables.

Step 6 Specify the HTTP method from the **HTTP Method** field: GET or POST.

Note GET operations will return text as a result.

Step 7 For HTTP POST operations, enter the content type of the POST in the **Content-Type** field. For this release, **text/html**, **text/plain**, and **text/xml** are supported.

Step 8 For HTTP POST operations, enter sample content in the **Content-Body** field. PSOM system variables are supported for the content. For example:

```
<?xml version="1.0" encoding="utf-8" ?>
<Data>
<AlertID>%ALERTID%</AlertID>
<AlertDescription>%DESCRIPTION%</AlertDescription>
</Data>
```

Step 9 Click **OK**.

Configuring IPICS Dispatch Alert Properties

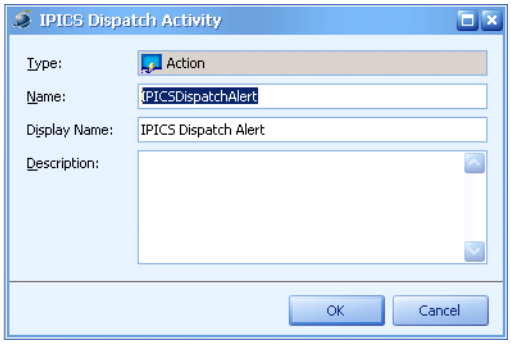
The IPICS Dispatch Alert component can be integrated with PSOM business logic in the Business Logic Designer to enable PSOM to automatically dispatch an alert to an IPICS Server version 4.0 and above. The IPICS Dispatch Alert component forwards alert information to IPICS including alert description, occurrence time, alert severity, alert ID, mini map, associated images, and relevant video (starting from 5 seconds before the alert occurred).

Note The IPICS Integration Module must be installed and configured.

To set properties for the IPICS Dispatch Alert component:

Step 1 Select the **IPICS Dispatch Alert** icon and click **Properties**.

The IPICS Dispatch Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Click **OK**.

Configuring IPICS Notify Alert Properties

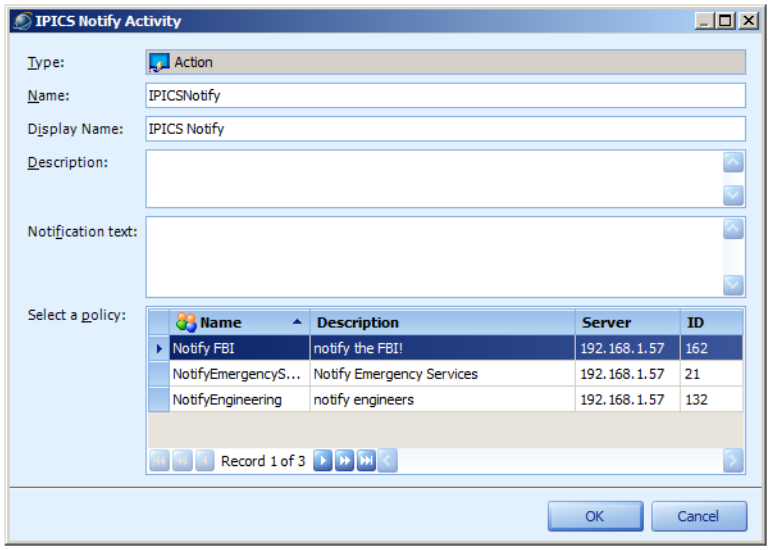
The IPICS Notify Alert component can be integrated with PSOM business logic in the Business Logic Designer to enable PSOM to automatically execute IPICS policies on an IPICS Server version 4.0 and above.

Note The IPICS Integration Module must be installed and configured.

To set properties for the IPICS Notify Alert component:

Step 1 Select the **IPICS Notify** icon and click **Properties**.

The IPICS Notify Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter a message to send from PSOM to IPICS Server along with the notification in the **Notification text** field. This text may be used by IPICS Server to execute the selected IPICS Policy.

Step 6 Select the IPICS Policy to execute as part of this notification from the **Select a policy** list. The list of IPICS policies is generated dynamically by contacting the IPICS Server when this component is opened.

Step 7 Click **OK**.

Configuring ODBC Action Properties

The ODBC Action Activity can run custom ODBC SQL scripts against a specified data source and return the results of the query (as a DataSet) to the activity context registry under the PxData category and ResultDataSet key. You can use PowerShell or other custom activities to retrieve this data from the context.

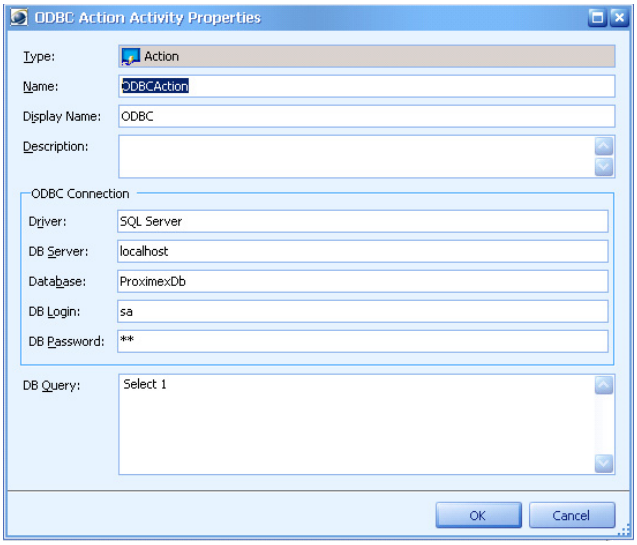
For example, the following PowerShell script retrieves the dataset result from the ODBC query:

```
$r = $pxContext.FindContextObject("PxData", "ResultDataSet")
```

To set properties for the ODBC Action component:

Step 1 Select the **ODBC Action** icon in the workspace and click **Properties**.

The ODBC Action Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter information for the ODBC data source in the **ODBC Connection** area:

a. In the **Driver** field, enter the ODBC driver used to access this data source.

b. In the **DB Server** field, enter the server where the ODBC database is running.

c. In the **Database** field, enter the name of the database you want to access.

d. In the **DB Login** field, enter the login name for accessing the database.

e. In the **DB Password** field, enter the corresponding password.

Step 6 Enter a custom SQL script to execute against the datasource in the **DB Query** area.

Step 7 Click **OK**.

Configuring PowerShell Action Properties

You can configure a PowerShell Action component to execute PowerShell scripts synchronously and asynchronously. The PowerShell Action component supports logging, object passing, calls to a WF Web Service, and passing and creating contextual data between activities in a business logic design.

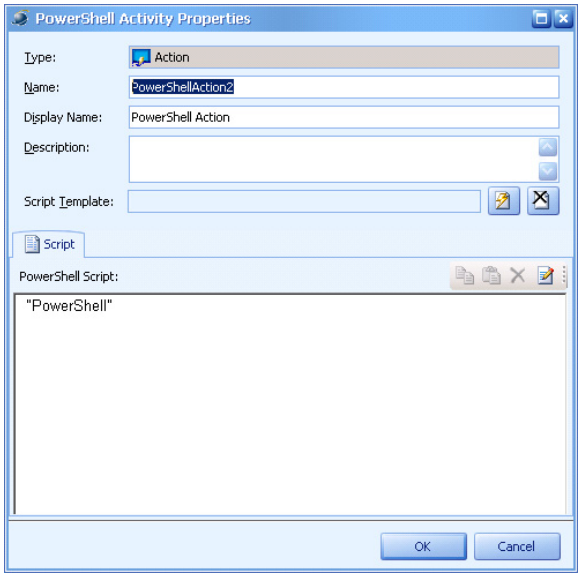
See the "Setting Up PowerShell Scripts" section on page 14-56 for details on defining PowerShell Scripts. This section describes how to add them as components to business logic templates.

Note You must have PowerShell installed on your system to execute PowerShell Action component. PowerShell requires Windows XP SP2 or later, and Windows Server 2003 SP1 or later. You can download PowerShell from the Microsoft website.

To set properties for the PowerShell Action component:

Step 1 Select the **PowerShell Action** icon and click **Properties**.

The PowerShell Activity Properties window appears.



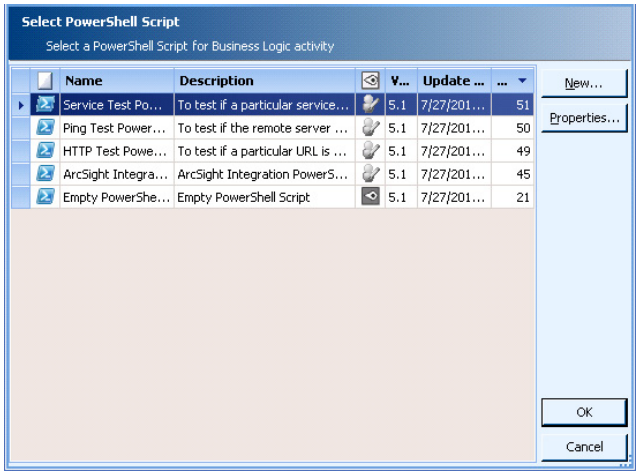
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 To select a PowerShell script, click the button in the **Script Template** field.

The Select PowerShell Script window appears.



Select the PowerShell script you want to use and click **OK**. The **PowerShell Activity Properties** window is populated with the script and parameters that have been defined for the selected script.

Step 6 You can also enter the script directly into the **Script** area of the **PowerShell Activity Properties** window.

If you want to write the PowerShell script in a different script editor (such as Notepad or an open source tool like Power GUI Editor), click the button in the **Script** area, and navigate to select your script editor. Once you've finished writing and debugging your code, you can copy and paste it into the text area of the Add PowerShell Script window.

Step 7 Click **OK** when finished.

PowerShell Action Examples

With the PowerShell Action activity, you can write simple script code to interact with existing business logic activities and achieve a high level of customization. See the "Configuring PowerShell Decision Properties" section on page 15-58 for examples of PowerShell scripts that perform decision processing.

Table 15-3 PowerShell Examples

Task	Script	Types of Business Logic
Setting a contextual value in the context registry This script saves the contents of $variable into the context registry under the "Sample Category" category and "Sample Key" key. This script can be used in all business logic.	`$pxContext.addContextObject("Sample Category", "Sample Key", $variable)`	All
Reading a contextual value from the context registry This script retrieves the value of the "Sample Category" category and "Sample Key" key.	`$pxContext.FindContextObject("Sample Category", "Sample Key")`	All
Retrieving alert detail for the current alert This script returns XML for full alert details in the "myVariable" variable.	`$myVariable = $pxWfWs.GetAlertDetailForAlertID($pxAlert.AlertID)`	Alert
This script returns XML for full alert details within the <RESULT> node.	`$pxWfWs.GetAlertDetailForAlertID($pxAlert.AlertID)`	Alert
Creating an audit entry for the current alert This script appends a "A Test audit entry" to the current alert's audit log.	`$pxWfWs.CreateAuditEntry("A Test audit entry", 27,2, $pxAlert.AlertID)`	Alert
Creating a live video alert on a particular video sensor	`$pxWfWs.CreateAlertSimple(1, $videoSensorId, "", "", "1","-1", $pxEvent.OccurTime,"1", "<DESCRIPTION></DESCRIPTION>","0","0","","0","0")`	Event Monitoring
Obtaining the current sensor context (SensorID)	`$sensorID = $pxContext.findContextObject("PxSensor", "SensorID")`	On-Demand
Obtaining the current area context (AreaID)	`$areaID = $pxContext.findContextObject("PxSensor", "AreaID")`	On-Demand
Obtaining the current alert context (Alert ID)	`$currentAlertID =$pxAlert.AlertID`	Alert Status On-Demand

Table 15-3 PowerShell Examples (continued)

Task	Script	Types of Business Logic
Obtaining the previous alert status for the current alert	`$previousStatus = $pxAlert.PrevStatus`	Alert Status
Obtaining the current alert status	`$curStatus = $pxAlert.Status`	Alert Status
Changing a contexual alert ID to a specific alert ID	`$pxAlert.AlertID = 123`	Alert
Changing the contexual sensor ID for an alert to a specific sensor ID	`$pxAlert.SensorID = 123`	Alert
Logging information into the trace log for Business Logic.	`$pxLogger.logInfo("This is a test message.")`	All
Obtaining the current version of PSOM Business Logic.	`$pxOEMInfo.ProductVersion`	All
Obtaining the current product name.	`$pxOEMInfo.ProductName`	All
Getting the company name.	`$pxOEMInfo.CompanyName`	All
Logging an event description based on the event issued by the 3rd party system.	`$pxLogger.logInfo($pxEvent.Description)`	Event
Obtaining the current GPS location for the source event.	`$currentGPS = $pxEvent.GPSLocation`	Event
Obtaining the current tracking object for the source event.	`$currentTrackingObj = $pxEvent.TrackingObject`	Event

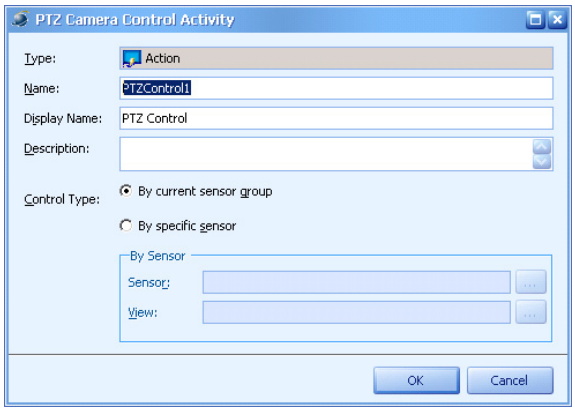
Configuring PTZ Control Properties

The PTZ Control component can send commands to PTZ cameras to control their movements. For example, you can swing a PTZ camera to a specific camera view, or swing all PTZ cameras in a sensor group to a camera view when an alert occurs.

To set properties for the PTZ Control component:

Step 1 Select the **PTZ Control** icon in the workspace and click **Properties**.

The PTZ Camera Control Activity window appears.



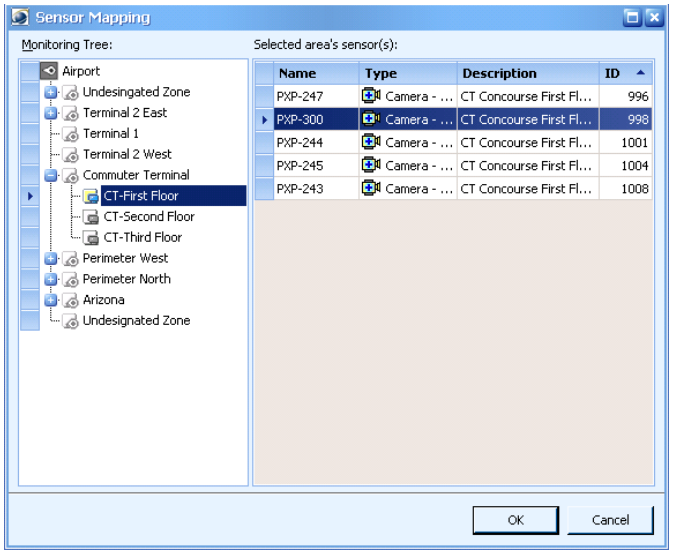
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

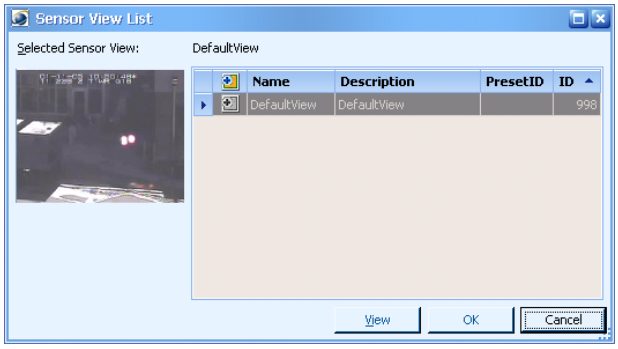
Step 5 Select the type of motion you want to perform:

- If you want to swing all cameras in a sensor group based on an alert occurring, select the **By current sensor group** option.
- If you want to swing a particular camera to a specified view, select the **By specific sensor** option. When this option is selected, the Sensor Mapping window appears.



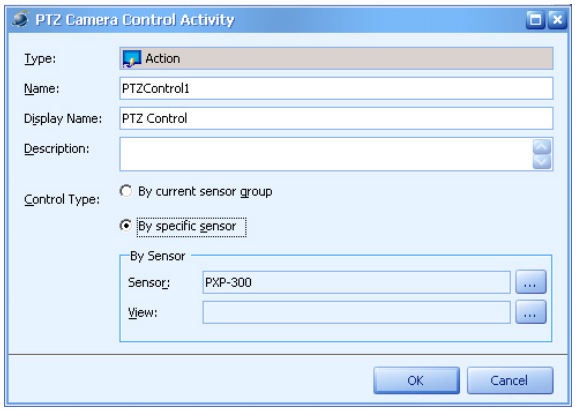
Navigate to select the PTZ camera and click **OK**.

The Sensor View List window appears.



Select the view to which you want to change the PTZ camera and click **OK**.

The PTZ Camera Control Activity window appears similar to the following.



Step 6 Click **OK**.

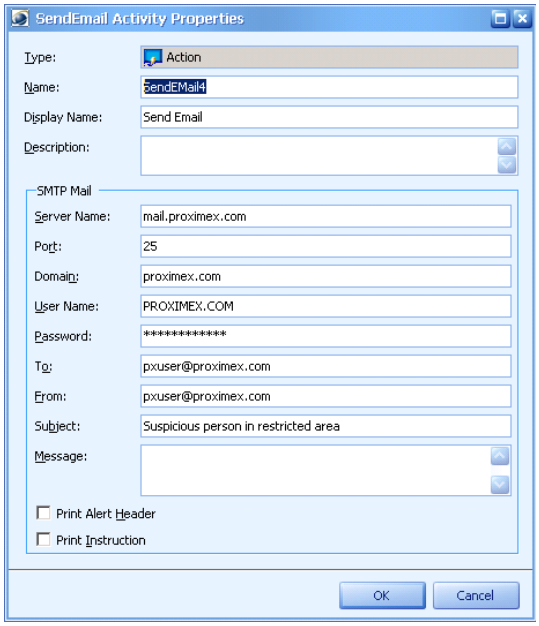
Configuring Send Email Properties

When you add a Send Email component to your business logic template, you can configure the email address, subject, body, SMTP server, login, password, and domain needed to send an email notification.

To set properties for the Send Email component:

Step 1 Select the **Send Email** icon in the workspace and click **Properties**.

The Send Email Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter the host name or IP address of your email server in the **Server Name** field.

Step 6 Enter the port number under which the email server is running in the **Port** field.

Step 7 Enter the name of the email server domain in the **Domain** field.

Step 8 Enter the email address for the user account that is used to send out email in the **User Name** field.

Step 9 Enter your email system password in the **Password** field.

Step 10 Enter the email address for the person who is sending the email notification in the **To** field.

Step 11 Enter the email addresses for all persons that should receive this email notification in the **From** field.

Step 12 Enter the subject of the email in the **Subject** field.

Step 13 Enter the message you want to send in the **Message** field.

Note In the **Subject** and **Message** fields, you can use system variables defined with '%VARIABLE%' where VARIABLE is the system variable in all capital letters. When these system variables are used, then PSOM will replace them with the right values and create the email. To use a combination of strings and variables, the string must precede the variable. For example:

```
net send MyMachineName hello %ALERTID%
```

See the "Using Global System Variables in Business Logic" section on page 14-51 for a list of system variables you can use to pass PSOM system information in the email.

Step 14 If you want to include the alert details in the email body, check the **Print Alert Header** option.

Step 15 If you want to include alert response instructions in the email body, check the **Print Instruction** option.

Step 16 Click **OK**.

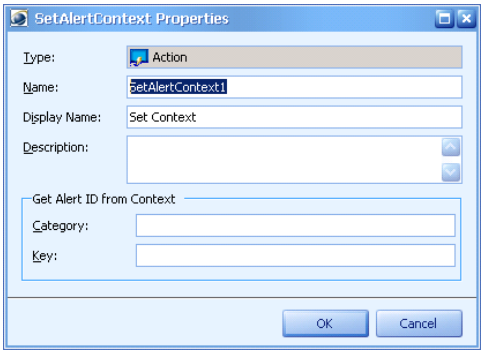
Configuring Set Alert Context Properties

The Set Alert Context activity allows you to dynamically switch the current alert context to a different alert by specifying a dynamic alert ID. This is useful in scenarios where you want to dynamically change the current alert context or invoke an alert-based business logic from other business logic types using a Call Child Logic activity, (for example, from a Scheduled business logic template).

To set properties for the Set Alert Context Activity component:

Step 1 Select the **Set Alert Context** icon in the workspace and click **Properties**.

The SetAlertContext Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

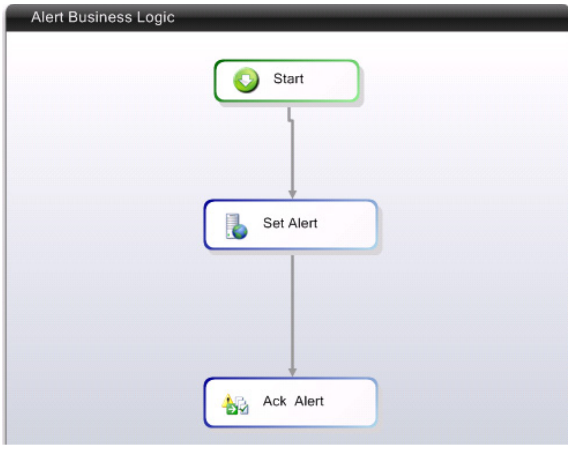
Step 5 Enter the category (defined in the dynamic business logic context) that contains the AlertID in the **Category** field.

Step 6 Enter the key (defined in the dynamic business logic context) that contains the AlertID in the **Key** field.

Step 7 Click **OK**.

- If the AlertID cannot be found in the specified category and key, no alert context will be set.
- If no alert can be found with the dynamically-loaded AlertID, the alert context will not be set.
- Once an alert context is set, you can run other alert-specified activities within the same business logic template. For example, you can use SetSeverity, SetStatus, or AlertCondition activities after the SetAlertContext activity.

  For example, you can acknowledge an alert using the dynamic alert context.



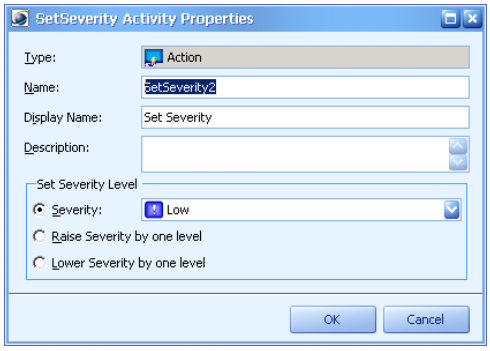
Configuring Set Alert Severity Properties

When you add a Set Alert Severity component to your business logic template, you can configure the severity of the alert that is being handled by the business logic.

To set properties for the Set Alert Severity component:

Step 1 Select the **Set Alert Severity** icon in the workspace and click **Properties**.

The Set Severity Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Set the severity level assigned to the alert using one of these methods:

- Choose a severity level from the **Severity** field if you want to set a specific severity level for the alert.
- Select the **Raise Severity by one level** option if you want to raise the severity level for the alert.
- Select the **Lower Severity by one level** option if you want to reduce the severity level for the alert.

Step 6 Click **OK**.

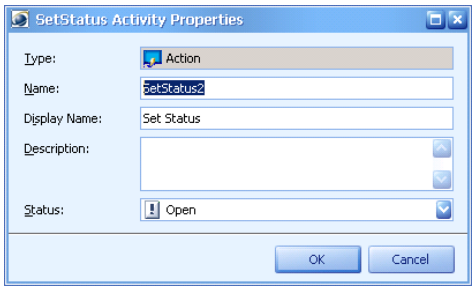
Configuring Set Alert Status Properties

When you add a Set Alert Status component to your business logic template, you can configure the status assigned to the alert that is being handled by the business logic.

To set properties for the Set Alert Status component:

Step 1 Select the **Set Alert Status** icon in the workspace and click **Properties**.

The SetStatus Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Set the status assigned to the alert from the **Status** field.

Note Once the status has been set to **Deleted**, the status cannot subsequently be reset to any other value during execution of this business logic template. In other words, once an alert has a status of **Deleted**, it cannot subsequently be assigned a status of **Open** or **Acknowledged**.

Step 6 Click **OK**.

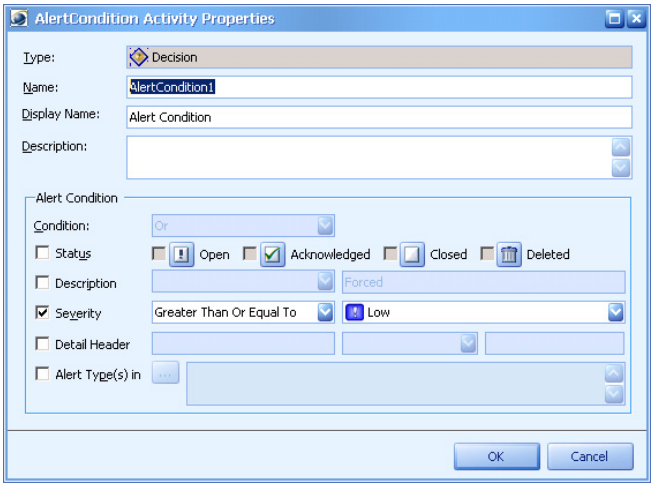
Configuring Alert Condition Properties

When you add an Alert Condition component to your business logic, you can configure the properties by which the component decides to direct alerts to different branches of the business logic. The decision is based on the severity and description of the alert.

To set properties for the Alert Condition component:

Step 1 Select the **Alert Condition** icon in the workspace and click the **Properties** button.

The AlertCondition Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

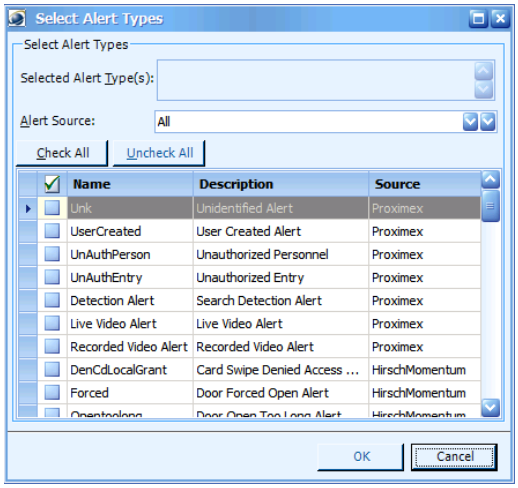
Step 4 Enter information about the component in the **Description** field.

Step 5 To make a decision based on an alert's status, check the **Status** option and select statuses to match (**Open**, **Acknowledged**, **Closed**, or **Deleted**). If the current status matches any of the checked statuses, the AlertCondition will be met.

Step 6 To make a decision based on an alert's description, check the **Description** option and enter the appropriate text in the field provided.

Step 7 To make a decision based on an alert's severity, check the **Severity** option and select the severity level. You can choose to match severity levels that are greater than or equal to, equal to, or less than or equal to the selected severity level.

Step 8 To make a decision based on specific alert types, select the **Alert Type(s) in** option, and click the button to view the Select Alert Types window. Check the boxes next to all the alert types you want to include, and then click **OK**.



Step 9 To make a decision based on a combination of factors, check all pertinent options and make a selection from the **Condition** field to indicate whether all conditions must be true (select **And**) or some can be true (select **Or**).

Step 10 Click **OK**.

Configuring Geo-Location Properties

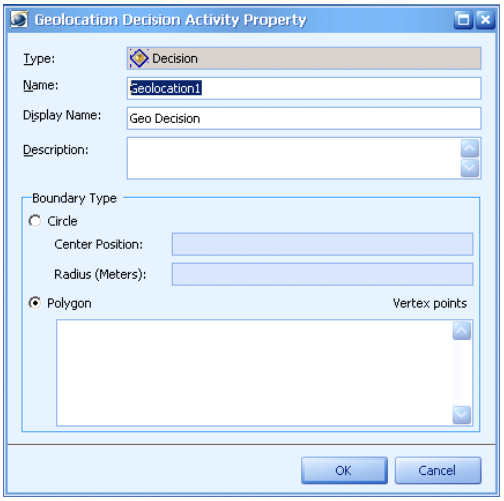
When you add a Geo-Location component to your business logic template, you can configure the properties by which the component decides to direct alerts to different branches of the business logic. The decision is based on whether an alert has occurred within the boundary of an area specified by GPS coordinates.

By default the Geo-Location component will try to retrieve the current geographical location from the alert context's alert header. If no alert is available (such as with an Event Monitoring Business Logic) it will look for the current geolocation from the event data. If it cannot find current geolocation from the alert header nor the event header, the activity will look for current geolocation from the parent activity's context registry. The current geolocation must use this format: *Longitude,Lattitude,Altitude*.

To set properties for the Geo-Location component:

Step 1 Select the **Geo-Location** icon in the workspace and click **Properties**.

The Geolocation Decision Activity Property window appears.



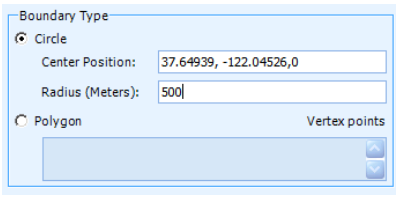
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

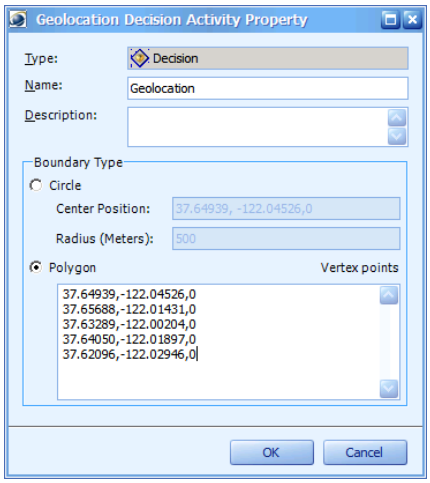
Step 4 Enter information about the component in the **Description** field.

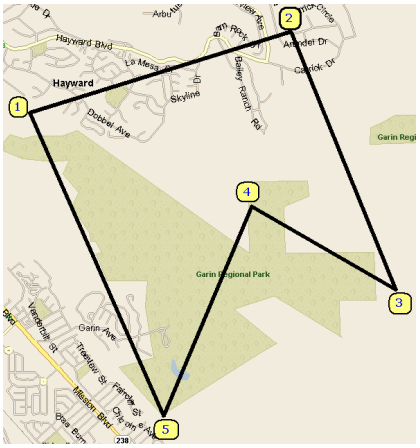
Step 5 Choose how you want to define the boundaries for the geographic area:

- Circle—To define the geographic area as a circle, select **Circle**, enter a GPS coordinate for the center of the circle and specify the number of meters radius.



- Polygon—To define the geographic area as a polygon, select **Polygon** and then enter the GPS coordinates for the points of the polygon area. Specify polygon vertex coordinates in a clockwise direction.





Step 6 Click **OK**.

Configuring Monitor Hierarchy Properties

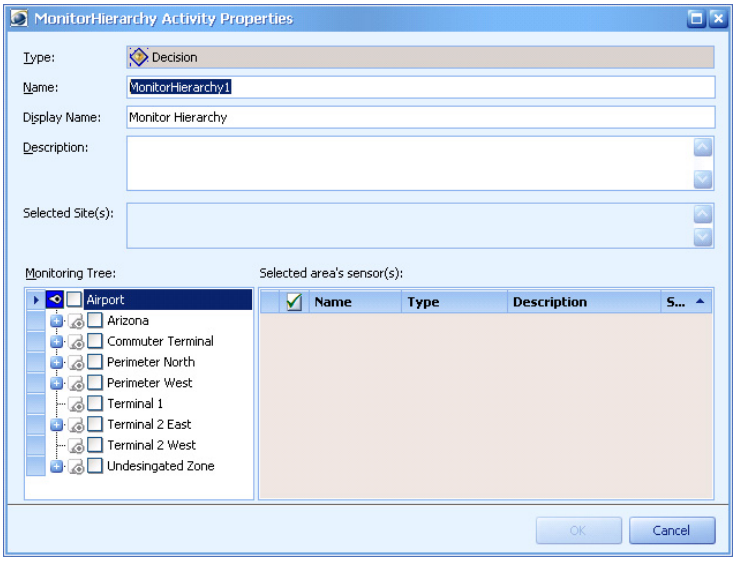
When you add a Monitor Hierarchy component to your business logic template, you can decide which branch of the business logic to execute based on the monitoring zones or areas that issued the alert that is passed to this component. You can also select specific sensors within a single monitoring area; specific sensors cannot be selected from more than one monitoring area.

The Monitor Hierarchy component can be used in Alert Business Logic, Alert Status Business Logic, and Event Business Logic templates. When used inside an Event Business Logic template, the Monitor Hierarchy component will make decisions based on the event's associated sensor location within the monitoring hierarchy.

To set properties for the Monitor Hierarchy component:

Step 1 Select the **Monitor Hierarchy** icon in the workspace and click **Properties**.

The Monitor Hierarchy Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Select the monitoring zone(s) or monitoring area(s) from the **Monitoring Tree** area that determines an alert should be sent to the next icon in the business logic rule. You can also select specific sensors from a single monitoring area, but not across multiple monitoring areas and zones.

Step 6 Click **OK**.

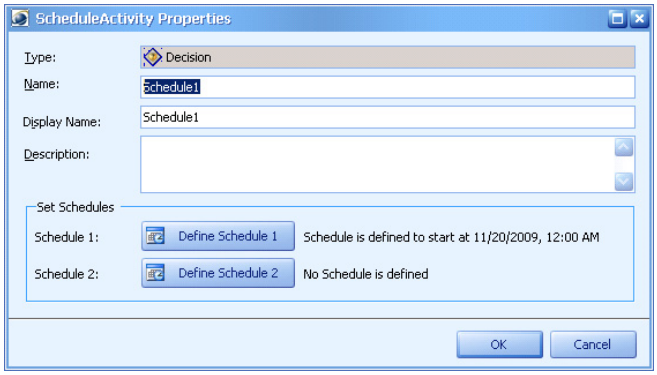
Configuring Schedule Condition Properties

When you add a Schedule Condition component to your business logic template, you can configure the properties by which the component decides to direct alerts to different branches of the business logic. The decision is based on the schedule specified within the component. You can define two different schedules for comparison; if the alert matches either schedule, then a "true" condition will exist. Otherwise, the "false" condition is executed.

To set properties for the Schedule Condition component:

Step 1 Select the **Schedule Condition** icon in the workspace and click **Properties**.

The Schedule Activity Properties window appears.



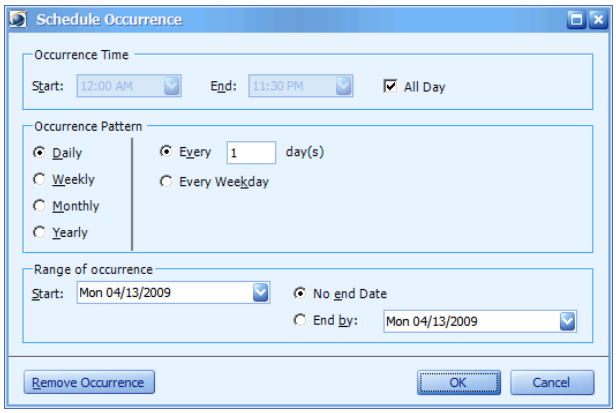
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 You can define two schedules that can be linked to different actions. To define a schedule, click its **Define Schedule** button.

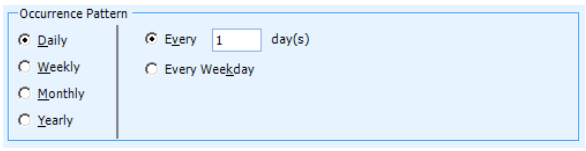
The Schedule Occurrence window appears.



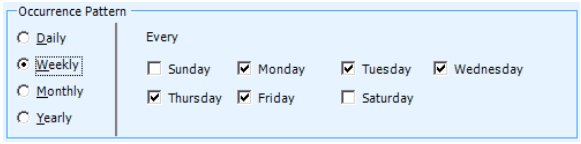
Step 6 Enter the daily starting and ending times for this schedule in the **Start** and **End** fields. If you want the schedule to run all the time, check the **All Day** option.

Step 7 Decide how often this schedule should be repeated in the **Occurrence Pattern** area: daily, weekly, monthly or yearly. And then enter the number of days/weeks/months/years that should pass before the schedule repeats in the **Every** field.

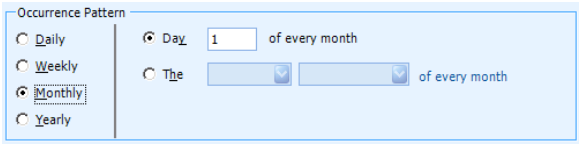
- For daily schedules, you can repeat the schedule on weekdays by selecting the **Every Weekday** option.



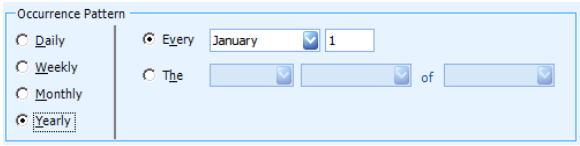
- For weekly schedules, you can select the days of the week that you want to repeat the schedule.



- For monthly schedules, you can select to repeat the schedule on a certain day of the month; or you can repeat the schedule every first/second/third... day of the month.



- For yearly schedules, you can repeat the schedule on a certain month/day every year, or you can select the first/second/third... occurrence of the specified day of the week in the selected month.



Step 8 Determine the start and end dates for this schedule in the **Range of occurrence** area. For the end date, you can:

- Choose not to end the schedule by selecting the **No end Date** option.
- End the schedule by a certain date by selecting that date from the **End by** field.

Step 9 If you want to remove this schedule, click the **Remove Occurrence** button.

Step 10 Click **OK** to save your schedule.

Step 11 When finished defining schedules, click **OK**.

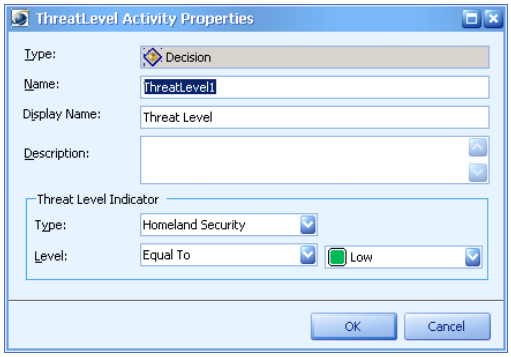
Configuring Threat Level Properties

When you add a Threat Level component to your business logic template, you can configure the properties by which the component decides to direct alerts to different branches of the business logic. The decision is based on the threat level of Homeland Security or MARSEC configured in PSOM.

To set properties for the Threat Level component:

Step 1 Select the **Threat Level** icon in the workspace and click **Properties**.

The Threat Level Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 If you want to make a decision based on Homeland Security, select **Homeland Security** from the **Type** field, and choose Low, Guarded, Elevated, High, or Severe from the **Level** field. You can select whether the level should be Equal To, Greater Than or Equal To, or Less Than or Equal To from the first drop-down menu next to the **Level** field.

Step 6 If you want to make a decision based on MARSEC, select **MARSEC** from the **Type** field, and choose MARSEC 1, MARSEC 2, or MARSEC 3 from the **Level** field. You can select whether the level should be Equal To, Greater Than or Equal To, or Less Than or Equal To from the first drop-down menu next to the **Level** field.

Step 7 Click **OK**.

Configuring Simulate Alert Properties

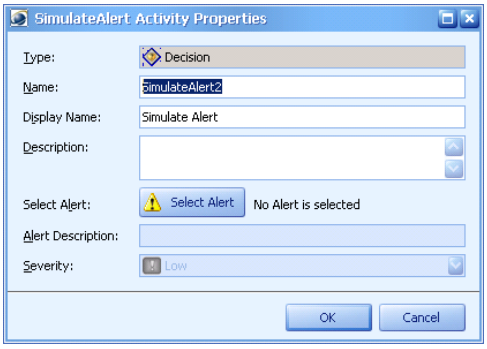
By adding a Simulate Alert component to your business logic template, you can test the business logic design by simulating the type of alert that you want to handle with the business logic template. The Simulate Alert component is only applicable inside Alert Business Logic or Alert Status Business Logic templates. You cannot use this component in other types of business logic templates.

Note When the business logic template runs and encounters a Simulate Alert component, it creates a new alert by copying an existing alert in PSOM. If, during Test Mode execution of the business logic, the original PSOM alert is deleted, it is possible that the simulated alert will not be created with full alert details (as presented in the Alert Details window). In this case, the simulated alert will not be an exact replica of the original PSOM alert, and may not show up in the Alert Manager or Operation Console.

To set properties for the Simulate Alert component:

Step 1 Select the **Simulate Alert** icon in the workspace and click **Properties**.

The Simulate Alert Activity Properties window appears.



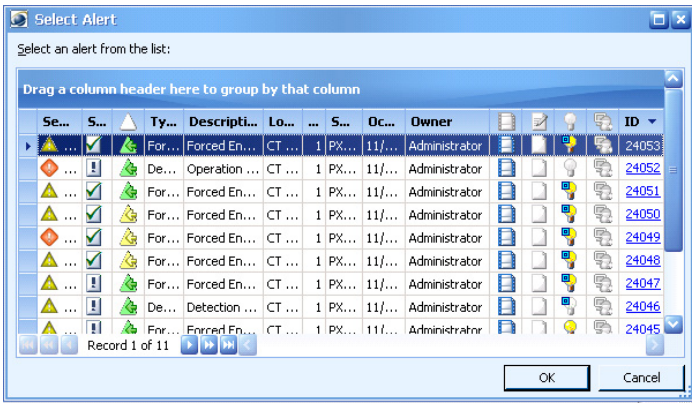
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 To select the alert that should be simulated, click the **Select Alert** button.

The Select Alert window appears.



Step 6 Select the alert you want to simulate and click **OK**. The alert's description and severity are automatically displayed in the SimulateAlert Activity Properties window.

Step 7 Click **OK**.

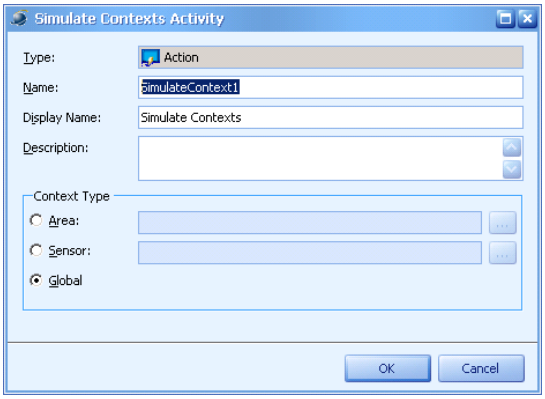
Configuring Simulate Contexts Properties

By adding a Simulate Contexts component to your business logic rule, you can simulate non-alert contexts for on-demand business logic.

To set properties for the Simulate Contexts component:

Step 1 Select the **Simulate Contexts** icon in the workspace and click **Properties**.

The Simulate Contexts Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

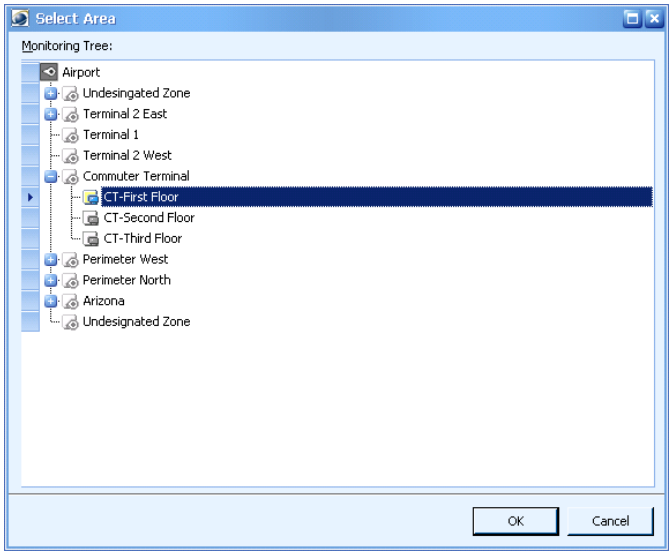
Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Choose how you want to simulate context for the business logic:

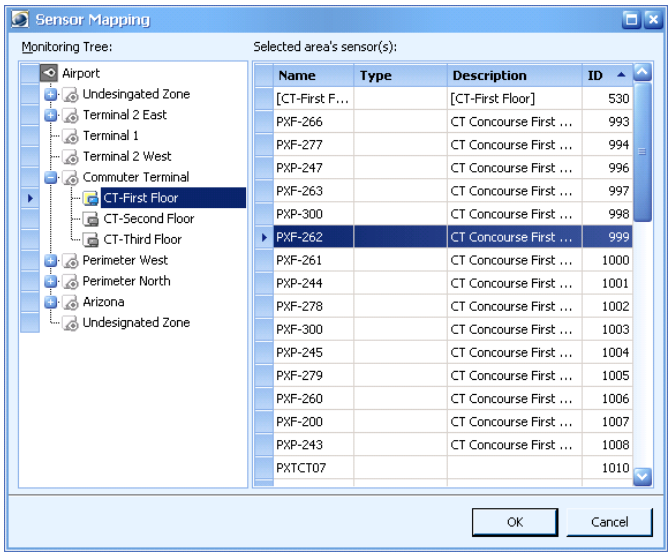
- To simulate context based on monitoring area, select **Area**.

  The Select Area window appears. Select a monitoring area and click **OK**.



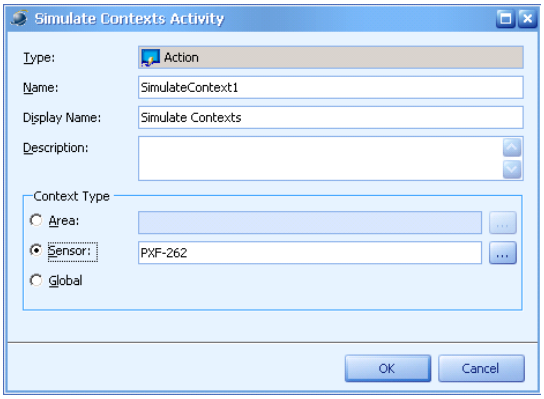
- To simulate context based on a sensor, select **Sensor**.

  The Sensor Mapping window appears. Select a sensor and click **OK**.



- To simulate context for the entire PSOM environment, select **Global**.

Depending on your selection, the Simulate Contexts Activity window appears similar to the following.



Step 6 Click **OK**.

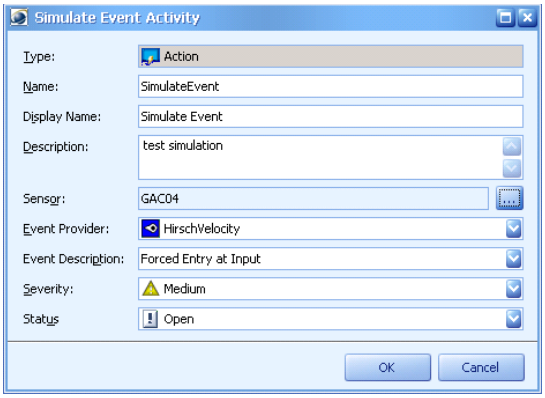
Configuring Simulate Event Properties

By adding a Simulate Event component to your business logic rule, you can test the business logic rule design by simulating the type of Integration Module event that you want to handle with the business logic rule.

To set properties for the Simulate Event component:

Step 1 Select the **Simulate Event** icon in the workspace and click **Properties**.

The Simulate Event Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Select the sensor from which the simulated event will be generated from the **Sensor** field. The sensor must be an actual access control sensor, not a virtual sensor or a camera sensor.

Step 6 Select the Integration Module from which the simulated event will be generated from the **Event Provider** field.

Step 7 Select the event that will be simulated from the **Event Description** field.

Step 8 Select the severity to be assigned to the simulated event from the **Severity** field.

Step 9 Select the status to be assigned to the simulated event from the **Status** field.

Note If you simulate an event status other than "OPEN", the event will be ignored by the EventMapFilter activity and the CreateAlert activity.

Step 10 Click **OK**.

Configuring Correlate Condition Properties

When you add a Correlate Condition component to your business logic, you can correlate multiple alerts across different systems to generate additional alerts, raise the severity level of alerts, or close or acknowledge existing alerts.

Reasons why you might use a Correlate Condition component include:

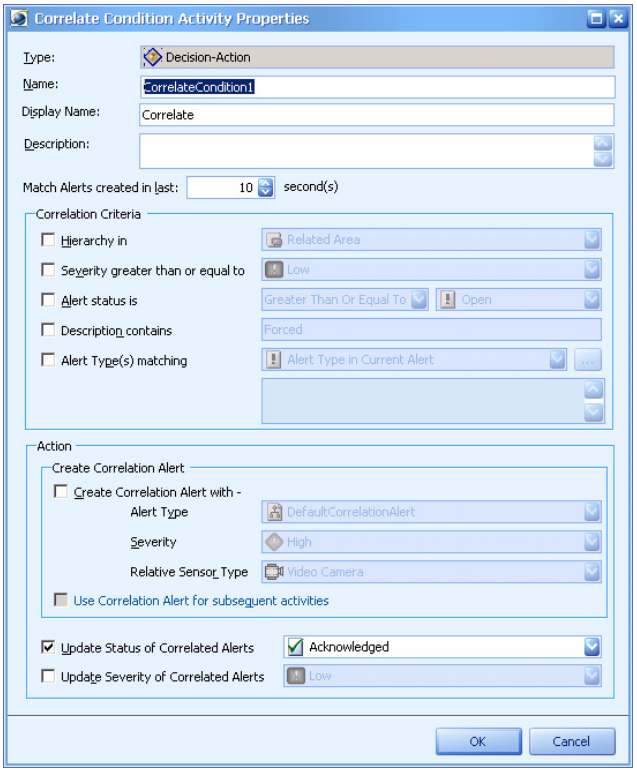
- To correlate alerts of a certain type across all sensors in an area or sensor group. This is specifically useful in areas of high importance. When the area has multiple sensors (doors, cameras, etc.) and alarms on these different sensors trigger at the same, or within a short span of time, it can be useful to analyze these alerts together.
- To determine when a specific type of alert occurs across the entire system at the same time; for example, correlating a Card Rejected alert across a building might help identify a suspect with a stolen card.
- To identify multiple false alerts from a sensor, or detect a malfunctioning sensor.

Alerts can be correlated by time range, proximity by monitoring area or sensor group, severity level, alert description, or alert type. Once correlation criteria are met, the Correlate Condition icon can generate a new alert, and update the status or severity of the existing correlated alerts.

To set properties for the Correlate Condition component:

Step 1 Select the **Correlate Condition** icon and click the **Properties** button.

The Correlate Condition Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter the number of seconds over which you want to correlate events that have occurred from the **Match Open Alerts created in last** field.

Step 6 Select the criteria that will be used to correlate alerts from the **Correlation Criteria** area:

a. To correlate alerts based on the originating monitoring area, sensor group, or sensor, select the **Hierarchy in** option. From the pull-down menu, choose **Related Area** to correlate alerts when they are issued in a common monitoring area, **Related Sensor within Sensor Group** to correlate alerts when they are issued by sensors in a common sensor group, or **Sensor in Current Alert** to correlate alerts when they are issued by the same sensor.

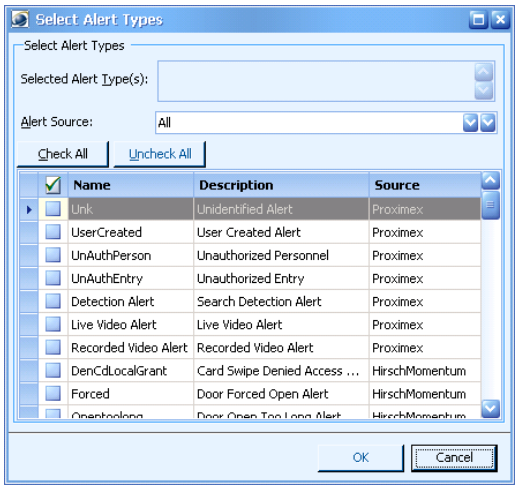
Note The **Related Sensor within Sensor Group** setting can be highly effective for correlating alerts raised by different sensor types. For example, a fence alert (against fence detection sensor) and an intelligent video alert (against a camera sensor) can be combined to create a real correlated alert, whereas each alert by itself would be highly prone to a false-positive error. To enable this alert correlation, create a sensor group that includes the different sensor types you want to combine for correlation purposes, and add the relevant sensors to it. When you create the CorrelationCondition activity, set the **Hierarchy in** field to **Related Sensor within Sensor Group**.

b. To correlate alerts based on their current severity levels, check the **Severity greater than or equal to** option and select a severity level from the pull-down menu (Low, Medium, High, or Critical).

c. To correlate alerts based on their current status, check the **Alert status is** option, select a relation (Equal To, Greater Than or Equal To, or Less Than or Equal To), and select an alert status (Open, Acknowledged or Closed).

d. To correlate alerts based on a common description, check the **Description contains** option and enter the descriptive words in the field provided.

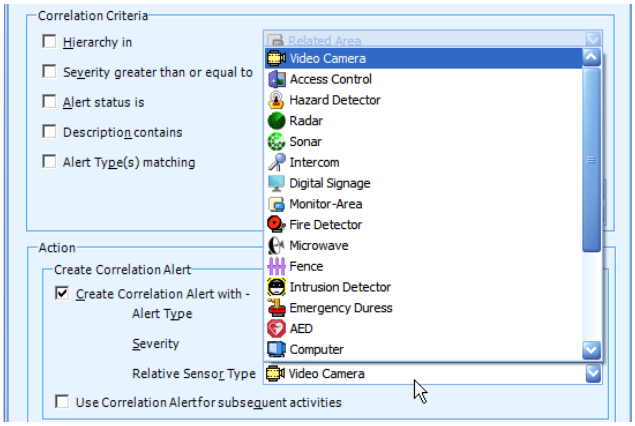
e. To correlate alerts based on alert type, check the **Alert Type(s) matching** option. You can either match alert type based on the current alert (select **Alert Type in Current Alert** from the pull-down menu), or based on selected alert types. To select specific alert types, choose **Select Alert Type(s)** from the pull-down menu and choose the types from the **Select Alert Types** dialog.



Note In most cases, you should set the **Alert Type(s) in** option as part of your correlation criteria to specific and limited alert types. If you do not use this option, or if you simply select all alert types for correlation, you may experience unwanted behavior including the creation of correlation alerts that trigger additional correlation activities.

Step 7 Choose the action to take when alerts are correlated from the **Action** area.

a. To generate a new alert, select the **Create Correlation Alert with** option. Select **DefaultCorrelationAlert** from the **Alert Type** field (or select a custom correlation alert), choose an alert severity to assign this alert from the **Severity** field (Low, Medium, High, or Critical), and select the sensor type for this alert from the **Relative Sensor Type** field (shown next).



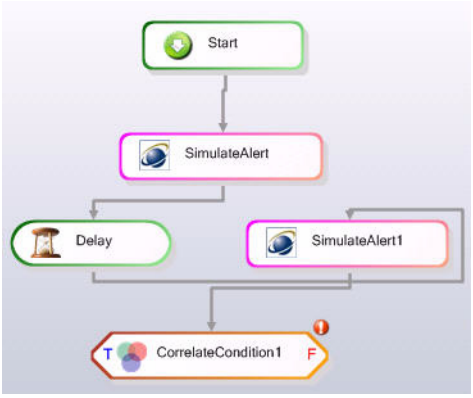
b. If you choose the **Create Correlation Alert with** option, PSOM will create a new alert that combines the multiple input alerts into one new correlated alert. To perform an action on this new correlated alert, you must check the **Use Correlation Alert for subsequent activities** option as well. Otherwise, actions may be performed on just one of the multiple input alerts.

c. To update the status of the correlated alerts, select the **Update Status of Correlated Alerts** option and choose the appropriate status from the pull-down menu (Acknowledged or Closed).

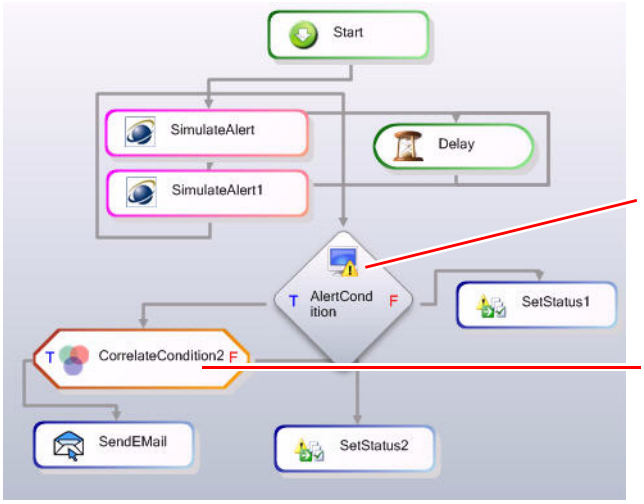
d. To update the severity of the correlated alerts, select the **Update Severity of Correlated Alerts** option and choose the severity to assign from the pull-down menu (Low, Medium, High, or Critical).

Step 8 Click **OK**.

The following business logic design uses SimulateAlert components connected with a Delay component. This flow simulates the alerts that this business logic rule is designed to correlate; the Delay component simulates a realistic timeframe during which the alerts are raised. Once both alerts have been raised, the CorrelateCondition component performs its work.



In the next example, an Alert Condition component verifies that the correct alerts, at or above the necessary severity level, have occurred before launching the Correlate Condition component.

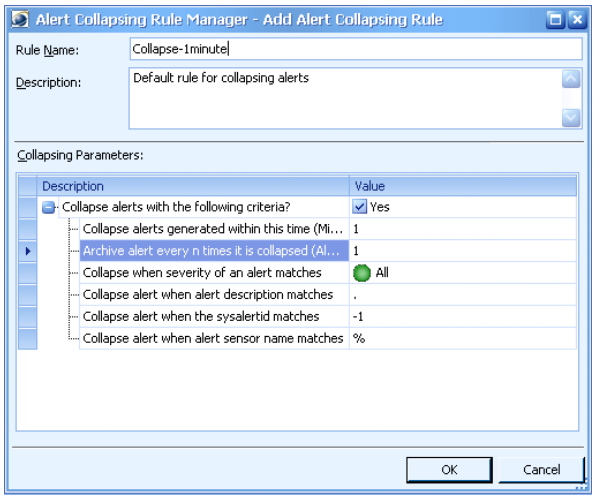


The Alert Condition component verifies that the specific alerts have occurred before passing control to the Correlate Condition component.

The Correlate Condition component takes different actions depending on whether its conditions have been met. For example, it sends a notification email if its conditions are true, and lowers the status of the alerts it investigated if conditions are false.

Note Additional guidelines for using Correlate Condition are provided next.

- Using Correlate Condition with other conditional activities—If you need to use other conditional activities (such as Alert Condition or Schedule), use them before you use Correlate Condition. For example, if you only want the Correlate Condition to run when a Forced Door or Door Open alert occurs, you can put an Alert Condition just before the Correlate Condition. The Alert Condition will check that the triggering alert matches its conditions before passing the alert to the Correlate Condition which will look for alerts that have already been created that match its criteria.
- Limiting Actions with Correlate Condition—Try to perform Action activities separately from performing CorrelateCondition activities as actions can interfere with the evaluation of correlation conditions.
- Avoiding multiple levels of Correlate Condition—It is acceptable to use several Correlate Condition activities at the same level in a business logic rule; for example, different Correlate Condition activities can be issued based on schedule. However, multi-level Correlate Condition activities (e.g., one Correlate Condition leading to another Correlate Condition) can become extremely difficult to navigate.
- Planning for different execution sequences—Your business logic rule may not execute in the same order during deployment as it does in trial or test mode. For example, if a business logic rule deletes an alert based on a Schedule activity, but you have a Correlate Condition activity that performs some action with that alert, you must make sure to account for various execution sequence scenarios since you cannot predict whether the delete will occur before the Correlate Condition executes.
- Reduce correlation processing with Alert Collapsing rules—When Correlate Condition is used, there is often a tendency for multiple duplicate false alerts to be raised, thereby generating Correlation alerts. To minimize the number of Correlation alerts, apply an Alert Collapsing rule so that multiple alerts of the same type are collapsed, generating fewer Correlation alerts.



- Designing coordinated Correlative Alerts—You can design a business logic template to handle processing for correlative alerts specifically. Use this technique in conjunction with general sensor groups. For example, you could create a “dummy” sensor to serve as a receptacle for Correlative Alerts, and then add this sensor to a sensor group; such as a sensor with type IntrusionDetection that is added to the sensor group for fence and camera alerts. Next, create a Correlate Condition that generates a “Single Correlated Intrusion” alert when both fence and camera-based alerts are triggered. Last, create another sensor group to contain all alerts of IntrusionDetection type sensors, and correlate this group to the “Single Correlated Intrusion” alert; when the Correlate Condition detects this situation, it generates a new alert called “Coordinated Intrusion Alert”. The end result is that this “Coordinated Intrusion Alert” tells the security staff that there is a coordinated attack on the facility as multiple correlative alerts (against fence and intelligent video) have risen at the same time in multiple places. Another business logic template can send an email to local police when a “Coordinated Intrusion Alert” is detected.

Configuring Event Map Filter Properties

When you add an Event Map Filter component to your business logic template, you can filter Integration Module events for an Event Business Logic template. Events that meet the criteria specified in the Event Map Filter component are created as alerts in PSOM with the defined severity against the selected sensor type. You can define as many filters in the Event Map Filter component as you need.

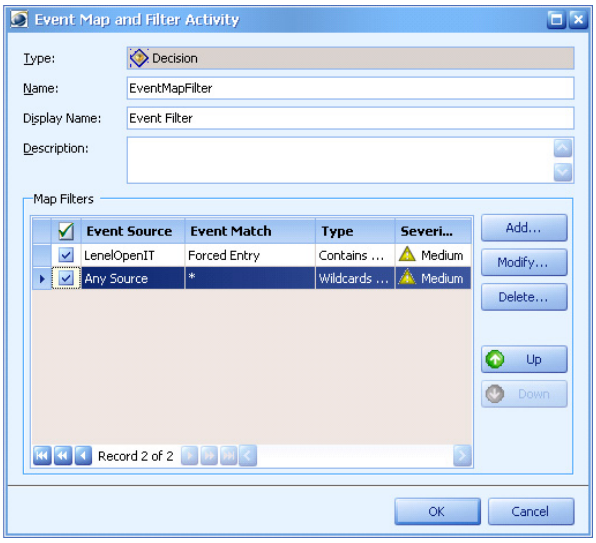
Note

- If you want to receive all Integration Module events into PSOM as alerts, you do not need to use this activity. However if you want to perform advanced filtering and specify the parameters for raised alerts, then you can use this activity.
- Because Event Business Logic raises an alert by default on the source sensor, customers of AgentVI or Nextiva may want to use an **Event Map Filter** activity to specify the target sensor type to be “Camera - Stationary”, “Camera - PTZ”, or “Camera - Others” so that the alert will be raised on the associated camera sensor instead.

To set properties for the Event Map Filter component:

Step 1 Select the **Event Map Filter** icon in the workspace and click **Properties**.

The Event Map and Filter Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

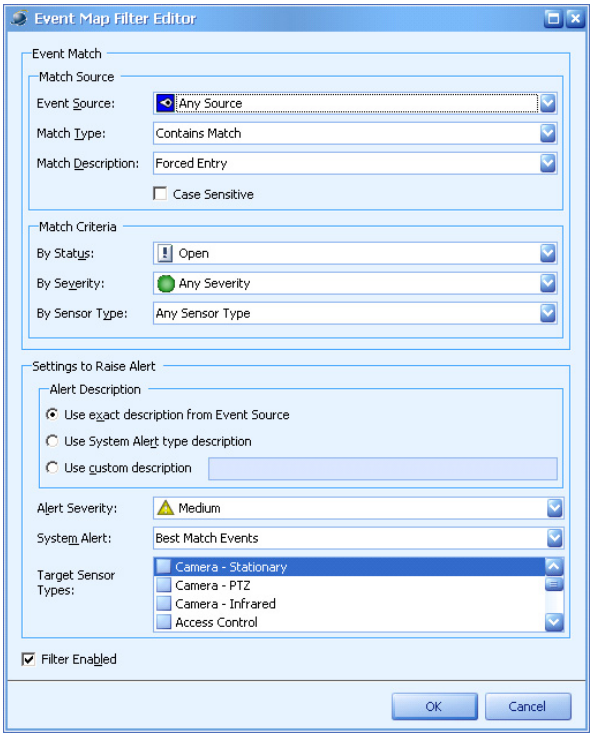
Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 To add a new filter:

a. Click **Add**.

The Event Map Filter Editor window appears.



b. In the **Match Source** area, select the Integration Module instance that will be generating the event from the **Event Source** field.

c. Select the type of match you want to use from the **Match Type** field. Choices include:

   - **Exact Match (Equal)**—The value provided in the **Match Description** field must be exactly the same as the event description in the external system for a match to be proved.
   - **Exact Match (Not Equal)**—The value provided in the **Match Description** field must not be the same as the event description in the external system for a match to be proved.
   - **Contains Match**—The value provided in the Match Description field must be included as part of the event description in the external system for a match to be proved.
   - **Wildcards Match**—The value provided in the Match Description field is matched to the event description using wildcard patterns. For example, pattern "*" will match against all descriptions. Pattern "*forced*" will match against all event descriptions that contains the word "forced".
   - **Regular Expression Match**—This is the most advanced matching in the Match Types. The value provided in the Match Description field is matched to the event description using regular expressions. For example, pattern "^.*forced$" will match against all event descriptions that contains the word "forced" at the end of the description.

d. Enter the event description you want to match in the **Match Description** field.

e. Check the **Case Sensitive** option if you want to require matches based on upper and lower case letters in the values. Uncheck this option if case does not matter.

f. Beyond matching the event description, if you want to match events using status, alert severity, or sensor type, make those selections in the **Match Criteria** area.

g. When a match is found, specify the alert description you want to use when raising an alert in PSOM in the **Raise Alert | Alert Description** area. You can use the event description from the external system, the description recorded in PSOM for the matching system alert, or a custom description.

h. For matching events, specify the severity that should be assigned to the PSOM alert in the **Alert Severity** field.

i. For matching events, specify how you want PSOM to match event to system alerts in the **System Alert** field.

j. Select the type of sensor that this alert should be associated with from the **Target Filter Types** field. If you do not make a selection, or a related sensor of the selected type cannot be found, the alert will be raised on the sensor that triggered the event.

k. If you want to enable this filter, check the **Filter Enabled** option.

l. Click **OK**.

Step 6 Repeat the last steps to specify as many filters as you need.

Step 7 Click **OK**.

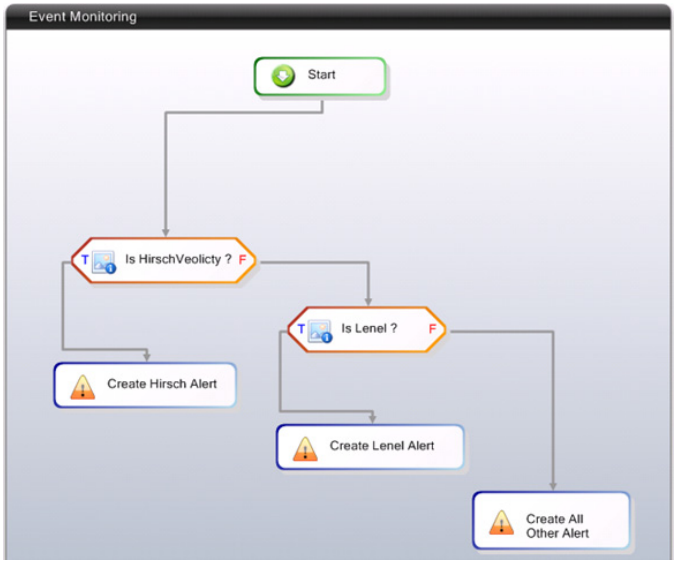
Note If multiple filters are used, an event will be matched against all of the filters in order until a first match is found.

If a match is found, the rest of the filters in the sequence will be skipped. For example, if you have 3 filters defined in the activity and an event matches the 2nd filter, the activity will exit. And the last filter will be skipped in this case.

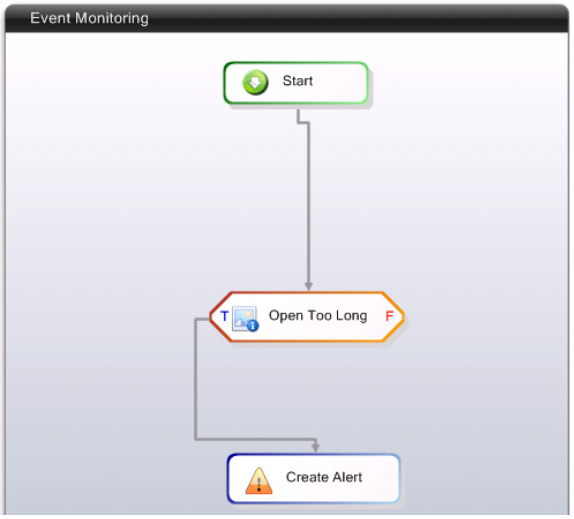
If a filter is disabled (the **Filter Enabled** option is unchecked), the filter will be skipped during execution.

Using Event Map Filter in Event Monitoring Business Logic

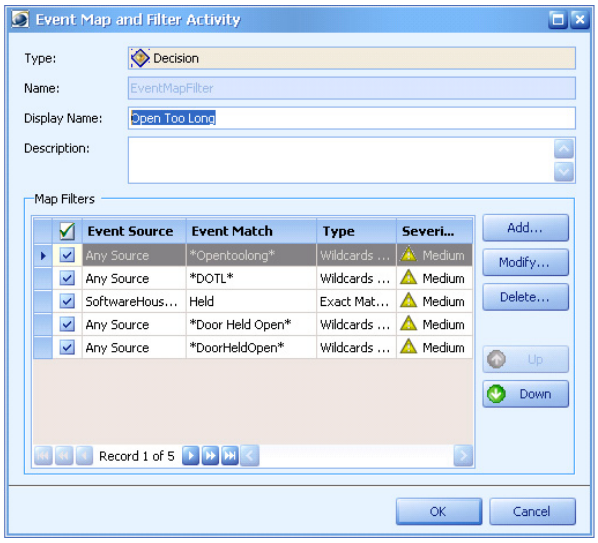
You can fine tune Event Monitoring business logic templates to include decisions based on a particular Integration Modules; for example, a decision specific to Hirsch Velocity and a different decision specific to Lenel. The following business logic template has two decisions based on two different Integration Module types.



You can also have decisions based on a particular type of event; for example, Door Forced Open or Door Opened Too Long. The following example shows a template with a test for the "Door Opened Too Long" event before an alert is generated.



The Event Map and Filter Activity window is configured as shown next.



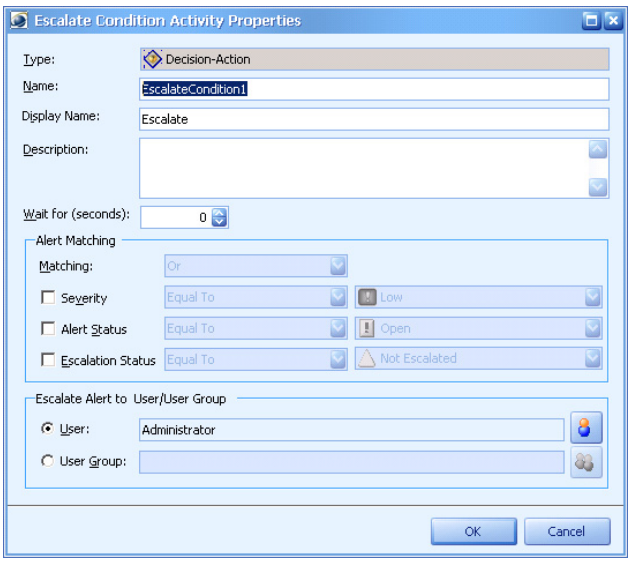
Configuring Escalate Condition Properties

When you add an Escalate Condition component to your business logic, you can configure the business logic template to escalate alerts to certain individuals or groups after a specified amount of time, or when certain conditions are met, based on the alert's status and severity.

To set properties for the Escalate Condition component:

Step 1 Select the **Escalate Condition** icon in the workspace and click **Properties**.

The Escalate Condition Activity Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Set the amount of time that should pass before the alert is escalated in the **Wait for (seconds)** field.

Step 6 Select the conditions upon which the alert will be escalated. You can choose any combination of the following:

a. To escalate alerts based on their current severity levels, check the **Severity** field and select a severity level from the pull-down menu at the far right (Low, Medium, High, or Critical). You can indicate a match is successful if the severity is equal to, greater than or equal to, or less than or equal to by selecting a choice from the first pull-down menu.

b. To escalate alerts based on their current alert status, check the **Alert Status** field and select a status from the pull-down menu at the far right (Open, Acknowledged, or Closed). You can indicate a match is successful if the alert status is equal to the selected status.

c. To escalate alerts based on their current escalation status, check the **Escalation Status** field and select a status from the pull-down menu at the far right (Not Escalated, Escalated, or Escalated-Viewed). You can indicate a match is successful if the alert status is equal to the selected status.

Step 7 Select the user or user group that should receive the escalated alert from the **Escalate Alert to User/User Group** area.

Step 8 Click **OK**.

Configuring ODBC Condition Properties

When you add an ODBC Condition component to your business logic template, you can run custom ODBC SQL scripts against a specified data source and return a true or false value to make a decision.

The decision will be “False” if the final result of the SQL query is zero. If the SQL query returns a positive integer, the decision will be “True.” In addition, the SQL query should return a scalar value (a single value) instead of rows of values.

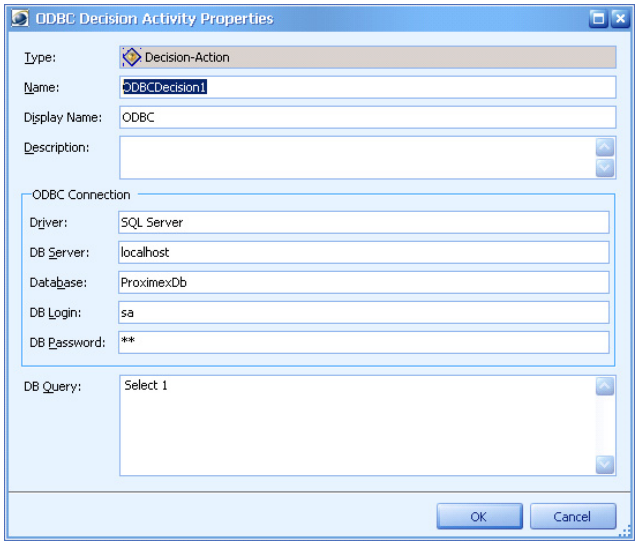
If the SQL query returns multiple rows or columns, only the first column of the first row will be evaluated. If the evaluated value is a positive integer, the decision will be “True”; otherwise if the value is negative or zero, the decision will be “False.” If the value cannot be evaluated to an integer, errors will be shown.

The result of the ODBC Condition query is stored in the alert context under the PxData category and ODBCResult key. You can use PowerShell to retrieve this context data.

To set properties for the ODBC Condition component:

Step 1 Select the **ODBC Condition** icon in the workspace and click **Properties**.

The **ODBC Decision Activity Properties** window appears.



Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Enter information for the ODBC data source in the **ODBC Connection** area:

a. In the **Driver** field, enter the ODBC driver used to access this data source.

b. In the **DB Server** field, enter the server where the ODBC database is running.

c. In the **Database** field, enter the name of the database you want to access.

d. In the **DB Login** field, enter the login name for accessing the database.

e. In the **DB Password** field, enter the corresponding password.

Step 6 Enter a custom SQL script to execute against the datasource in the **DB Query** area.

Step 7 Click **OK**.

Configuring PowerShell Decision Properties

You can write a PowerShell scriptblock to perform an analysis, or correlate data with existing systems like Microsoft SQL Server or Exchange Server, and then return TRUE or FALSE for a decision that affects the flow of the business logic template. The PowerShell Decision component supports logging, object passing, calls to a WF Web Service, and passing and creating contextual data between activities in a business logic design.

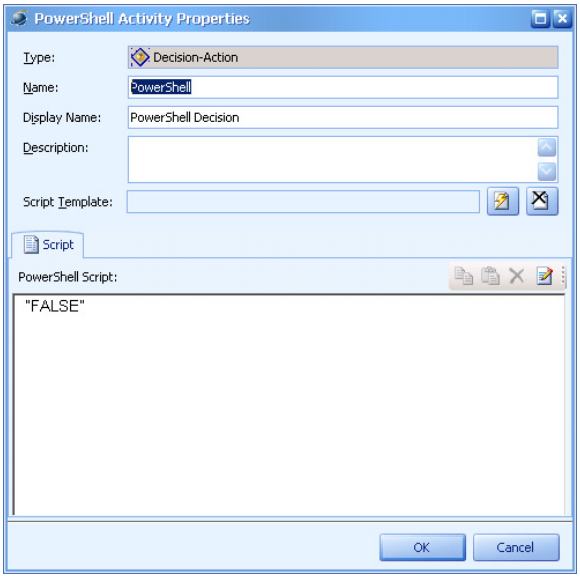
See the "Setting Up PowerShell Scripts" section on page 14-56, the "PowerShell Script Format" section on page 14-57, and the "PowerShell Action Examples" section on page 15-28 for details on defining basic PowerShell scripts. This section describes how to add PowerShell as decision components in business logic templates.

Note You must have PowerShell installed on your system to execute PowerShell Decision components. PowerShell requires Windows XP SP2 or later, and Windows Server 2003 SP1 or later. You can download PowerShell from the Microsoft website.

To set properties for the PowerShell Decision component:

Step 1 Select the **PowerShell Decision** icon and click **Properties**.

The PowerShell Activity Properties window appears.



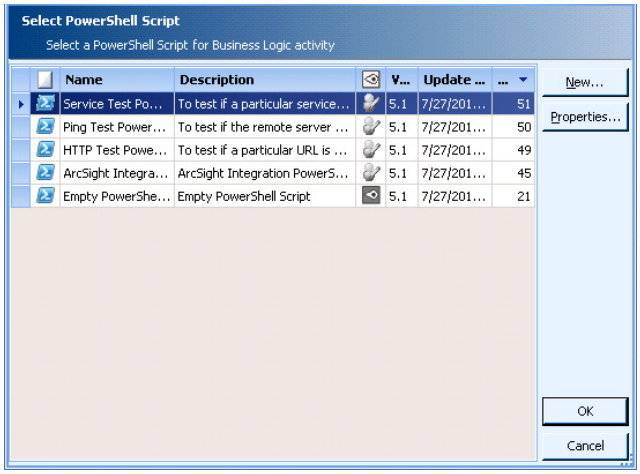
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

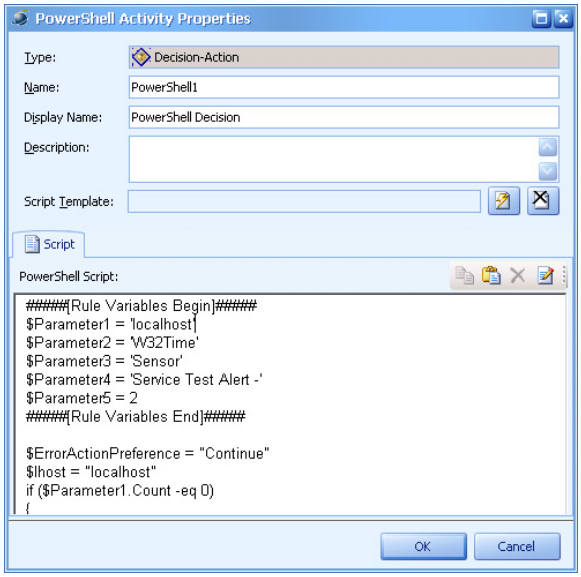
Step 5 To select a PowerShell script, click the button in the **Script Template** field.

The Select PowerShell Script window appears.



Select the PowerShell script you want to use and click **OK**. The PowerShell Activity Properties window is populated with the script and parameters that have been defined for the selected script.

Step 6 You can also enter the script directly into the **Script** area of the PowerShell Activity Properties window.



If you want to write the PowerShell script in a different script editor (such as Notepad or an open source tool like Power GUI Editor), click the button in the **Script** area, and navigate to select your script editor. Once you've finished writing and debugging your code, you can copy and paste it into **Script** area.

Step 7 Click **OK** when finished.

S

PowerShell Decision Examples

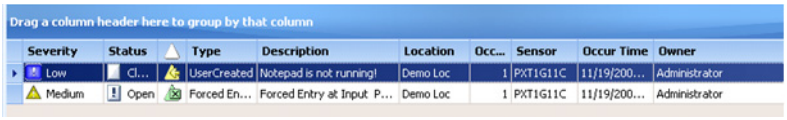
You can write script code to make decisions within business logic templates. For example, you could use a PowerShell Decision to determine if the number of processes for an application has exceeded a limit—for example, if three instances of "Notepad" are running return TRUE, otherwise return FALSE.

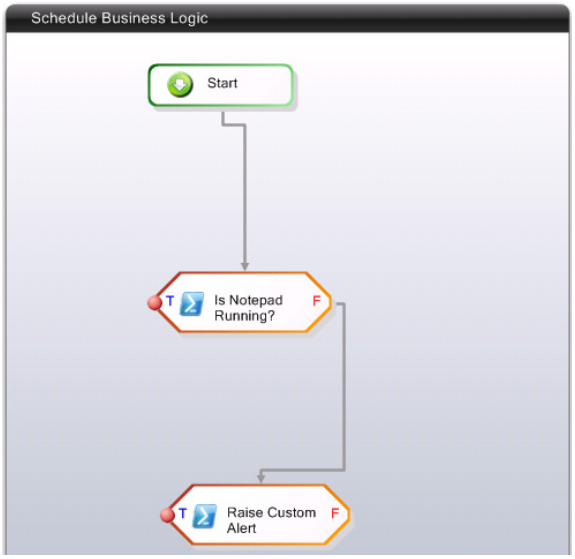
```
#####[Rule Variables Begin]#####
$Threshold = 2
$ProcName = 'notepad'
#####[Rule Variables End]#####

$colItems = Get-Process
$TotalCount = 0
for each ($objItem in $colItems)
{
    #write-host "Name: " $objItem.Name "ID: " $objItem.ID
    if($objItem.Name -eq $ProcName)
    {
        $TotalCount++
    }
}
if($TotalCount -gt $Threshold)
{
    "True"
}
else
{
    "False"
}
```

Example 1: Creating User Alerts when a Process is Not Running

In this example, the business logic uses two PowerShell scripts. The first checks whether a process (in this case, Notepad) is running. If the process is not running, the second PowerShell script creates a user alert. This script can be used in Scheduled Business Logic.

When the process is closed, alerts periodically appear in PSOM:





This PowerShell script checks whether the process is running:

```
$procCounter = @(Get-Process notepad*).Count
if ($procCounter -ge 1)
{
   "TRUE"
}
else
{
   "FALSE"
}
```

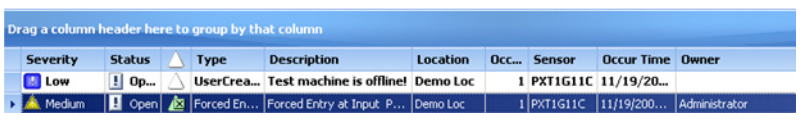
This Powershell script raises a user alert if the process is not running:

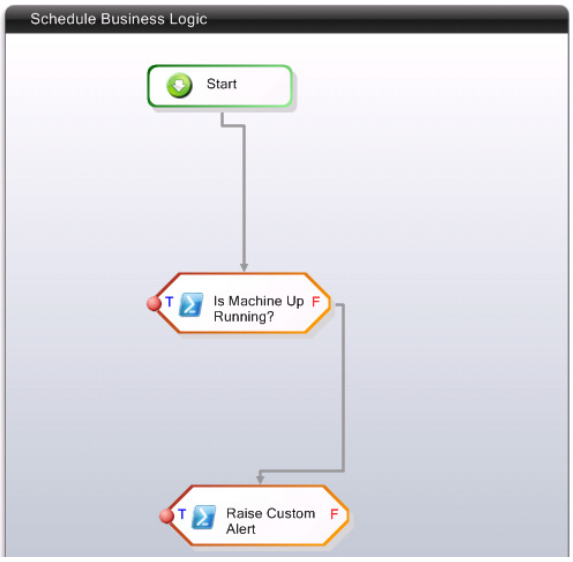
```
$sensorID = 1
$areaId=1
$ruleID = -1
$currentTime = get-date
$message= "Notepad is not running!"
$pxWFWS.CreateAlertSimple(1,$sensorID,"","",
$message,$areaID,$ruleID,$currentTime.ToString(),1,
"<DESCRIPTION></DESCRIPTION>", 0,0,0,0)
```

For this example, the alert is created on in the monitoring area with an ID=1 for the sensor with ID=1. The alert message is “Notepad is not running”.

Example 2: Creating User Alerts when a Machine Becomes Unreachable

In this example, the business logic uses two PowerShell scripts. The first pings a particular IP address to determine whether a machine is running. If the machine is not running, the second PowerShell script creates a user alert. This script can be used in Scheduled Business Logic. When the machine is unreachable, alerts appear:





This PowerShell script checks whether the machine is running. You can change the test IP address to any IP address that you want to check.

```
$testIPAddress= "192.168.1.188"
$ping = New-Object System.Net.NetworkInformation.Ping
$pReply = $ping.Send($testIPAddress)
$pStatus = $pReply.Status
if ($pStatus -eq "Success")
{
   "TRUE"
}
else
{
   "FALSE"
}
```

This Powershell script raises a user alert if the machine is not running:

```
$sensorID = 1
$areaId=1
$ruleID = -1
$currentTime = get-date
$message= "Test machine is offline!"
$pxWFWS.CreateAlertSimple(1,$sensorID,"","",$message,$areaID,$ruleID,$currentTime.ToString
(),1,"<DESCRIPTION></DESCRIPTION>", 0,0,0,0)
```

For this example, the alert is created on in the monitoring area with an ID=1 for the sensor with ID=1. The alert message is “Test machine is offline!”.

Configuring RSS Alerts Properties

When you add a RSSAlerts component to your Schedule Business Logic, you can configure the properties by which the component decides to aggregate RSS or ATOM feeds, filter through the feed items and then create corresponding alerts in PSOM. You can create multiple PSOM alerts in a single

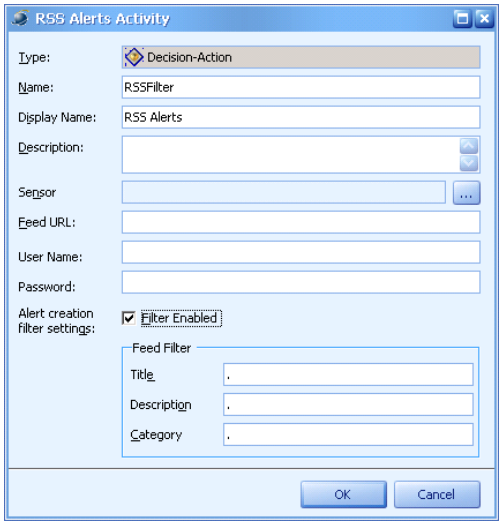
execution based on the number of filtered feed items you specify in the RSS Alerts component; only feed items that match all filter expressions will generate an alert. If the RSS Alerts component does not create any alerts the decision result will be “FALSE”.

If you add a Create Report component after the RSS Alerts component in your business logic, you can generate multiple Alert Detail reports. See the “Configuring Create Report Properties” section on page 15-18.

To set properties for the RSS Alerts component:

Step 1 Select the **RSS Alerts** icon in the workspace and click **Properties**.

The RSS Alerts Activity window appears.



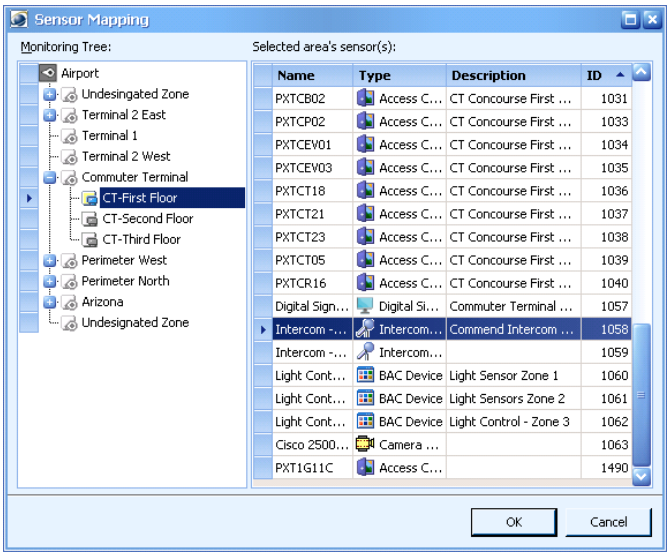
Step 2 Enter a new name for the component in the **Name** field.

Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

Step 5 Choose the sensor for which alerts should be generated when matching feed items occur by clicking the … button in the **Sensor** field.

The Sensor Mapping window appears. Select a sensor and click **OK**.



Step 6 Enter the URL for the RSS or ATOM feed that this component should poll during execution in the **Feed URL** field.

Step 7 Enter the access credentials for the feed in the **User Name** and **Password** fields.

Step 8 If you want to filter the alerts received from the feed URL to only create PSOM alerts under certain conditions:

a. Select the **Filter Enabled** option. Once enabled, only those feeds that match all filter criteria will create alerts in PSOM.

b. Enter text into the **Title** field that should appear in the title of a feed for it to result in a PSOM alert. Filter criteria is case-sensitive.

c. Enter text into the **Description** field that should appear in the description of a feed for it to result in a PSOM alert. Filter criteria is case-sensitive.

d. In the **Category** field, enter the category to which a feed must belong before a PSOM alert will be created. Filter criteria is case-sensitive.

Step 9 Click **OK**.

Note The filter uses a Regular Expression for matches. A feed must meet all filter criteria before an alert is created in PSOM. If you do not want to specify a filtering criteria, leave it as "." as it will match against all characters in that field.

The RSS Alerts activity can only be used inside Schedule Business Logic templates.

Some feeds are not supported in this release (such as Google news).

Test feeds in the Business Logic Designer before deploying the business logic template. All RSS alerts created inside the Business Logic Designer will appear as "Simulated" in the Operation Console.

Configuring Lock Door Properties

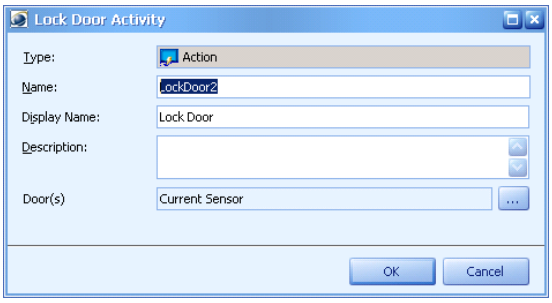
The Lock Door activity allows you to issue a "Lock Door" command to Integration Module door sensors. This activity is part of the Sensor Commands activity list.

Note PSOM Bus Service must be running for this component to complete successfully in a runtime environment.

To set properties for the Lock Door component:

Step 1 Select the **Lock Door** icon in the workspace and click **Properties**.

The Lock Door Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

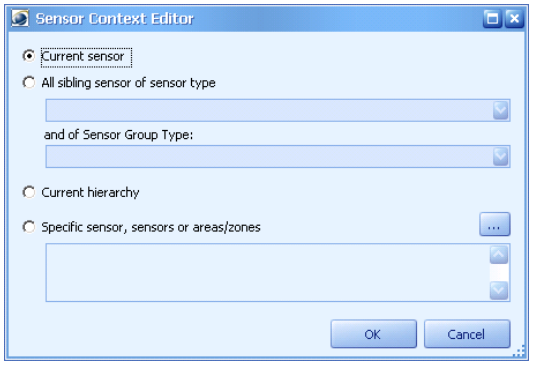
Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

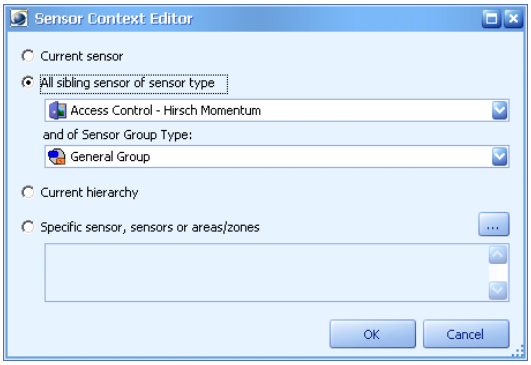
Step 5 In the **Door(s)** field, make a choice:

- Leave **Current sensor** selected to apply the command to whichever access control is being handled by the business logic when Lock Door is called. For Event Business Logic, the current sensor is the sensor associated with the source event. For Alert Business Logic or Alert Status Business Logic, the current sensor is the sensor associated with the PSOM alert.
- Apply the command to a sibling or specific sensor. Click the ... button.

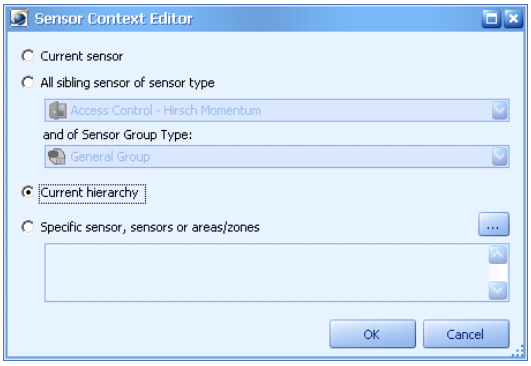
  The Sensor Context Editor window appears.



Select the **All sibling sensor of sensor type** option to apply the command to a sibling sensor, and choose the sensor type and sensor group from the fields.

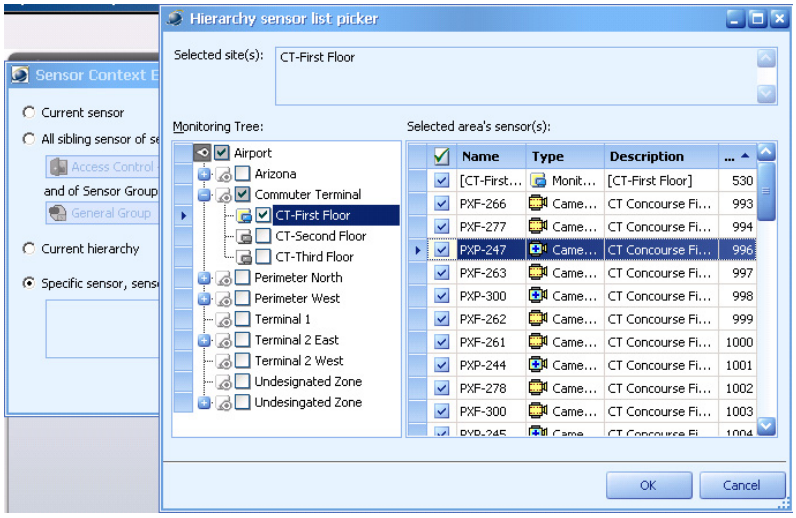


Select the **Current hierarchy** option to apply the command to all access control sensors in the current monitoring area or zone.



When **Current hierarchy** is selected, the Lock Door component will first try to obtain the ZoneID from the activity context registry (category PxSensor, key ZoneID); then the AreaID (category PxSensor, key AreaID). Finally, it will try to obtain the AreaID from the associated PxAlert or PxEvent directly.

Select the **Specific sensor, sensors, or area/zone** option to apply the command to a specific sensor and click the ... button. The Hierarchy sensor list picker window appears where you can navigate the monitoring hierarchy and select the sensor to which this command should be applied. Click **OK** when finished.



Step 6 Click **OK** in the Sensor Context Editor window.

Step 7 Click **OK** in the Lock Door Activity window.

Configuring Open Door Properties

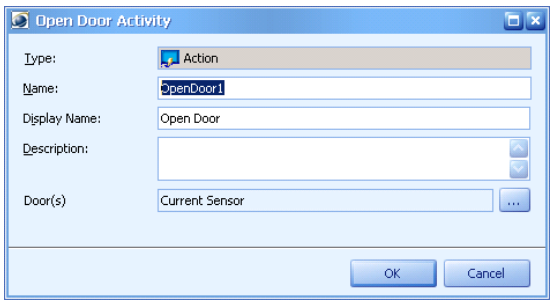
The Open Door activity allows you to issue an "Open Door" command to Integration Module door sensors. This activity is part of the Sensor Commands activity list.

Note PSOM Bus Service must be running for this component to complete successfully in a runtime environment.

To set properties for the Open Door component:

Step 1 Select the **Open Door** icon in the workspace and click **Properties**.

The Open Door Properties window appears.



Step 2 Enter a new name for the component in the **Name** field.

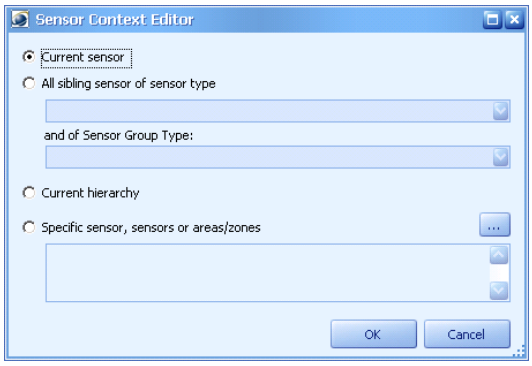
Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

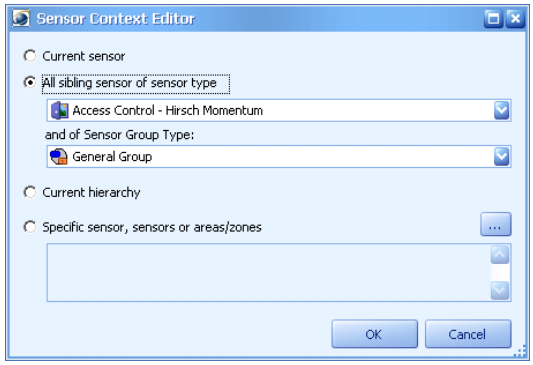
Step 5 In the **Door(s)** field, make a choice:

- Leave **Current sensor** selected to apply the command to whichever access control is being handled by the business logic when Open Door is called. For Event Business Logic, the current sensor is the sensor associated with the source event. For Alert Business Logic or Alert Status Business Logic, the current sensor is the sensor associated with the PSOM alert.
- Apply the command to a sibling or specific sensor. Click the ... button.

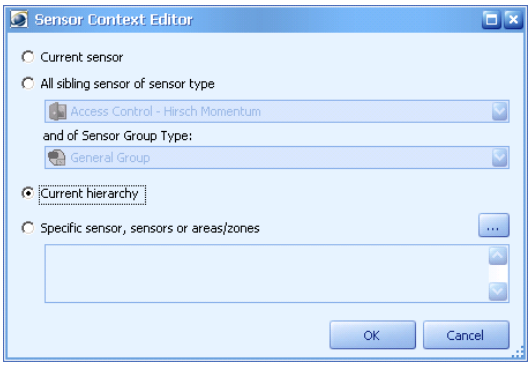
  The **Sensor Context Editor** window appears.



Select the **All sibling sensor of sensor type** option to apply the command to a sibling sensor, and choose the sensor type and sensor group from the fields.

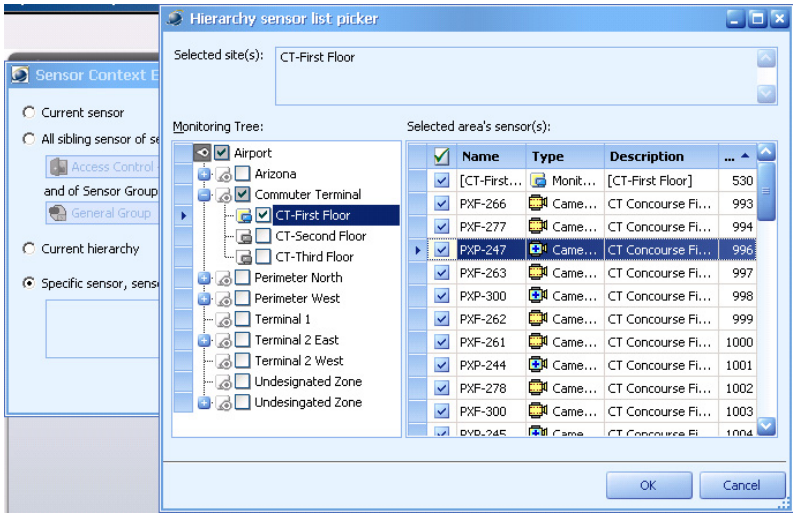


Select the **Current hierarchy** option to apply the command to all access control sensors in the current monitoring area or zone.



When **Current hierarchy** is selected, the Open Door component will first try to obtain the ZoneID from the activity context registry (category PxSensor, key ZoneID); then the AreaID (category PxSensor, key AreaID). Finally, it will try to obtain the AreaID from the associated PxAlert or PxEvent directly.

Select the **Specific sensor, sensors, or areas/zones** option to apply the command to a specific sensor and click the ... button. The Hierarchy sensor list picker window appears where you can navigate the monitoring hierarchy and select the sensor to which this command should be applied. Click **OK** when finished.



Step 6 Click **OK** in the Sensor Context Editor window.

Step 7 Click **OK** in the Open Door Activity window.

Configuring Open Door Momentarily Properties

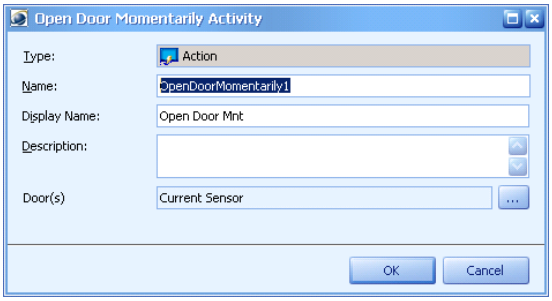
The Open Door Momentarily activity allows you to issue an “Open Door Momentarily” command to Integration Module door sensors. This activity is part of the Sensor Commands activity list.

Note PSOM Bus Service must be running for this component to complete successfully in a runtime environment.

To set properties for the Open Door Momentarily component:

Step 1 Select the **Open Door Momentarily** icon in the workspace and click **Properties**.

The Open Door Momentarily Activity window appears.



Step 2 Enter a new name for the component in the **Name** field.

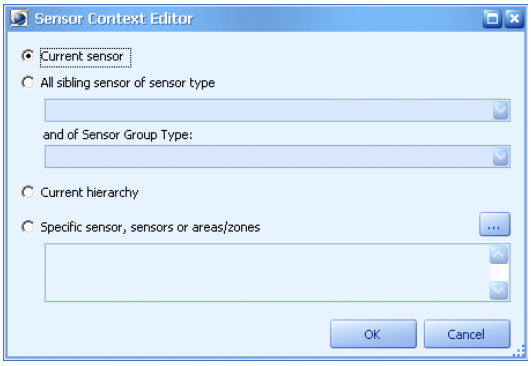
Step 3 Enter a name to display on the icon in the workspace in the **Display Name** field.

Step 4 Enter information about the component in the **Description** field.

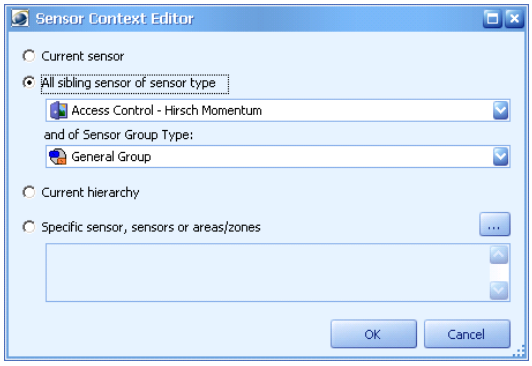
Step 5 In the **Door(s)** field, make a choice:

- Leave **Current sensor** selected to apply the command to whichever access control is being handled by the business logic when Open Door Momentarily is called. For Event Business Logic, the current sensor is the sensor associated with the source event. For Alert Business Logic or Alert Status Business Logic, the current sensor is the sensor associated with the PSOM alert.
- Apply the command to a sibling or specific sensor. Click the ... button.

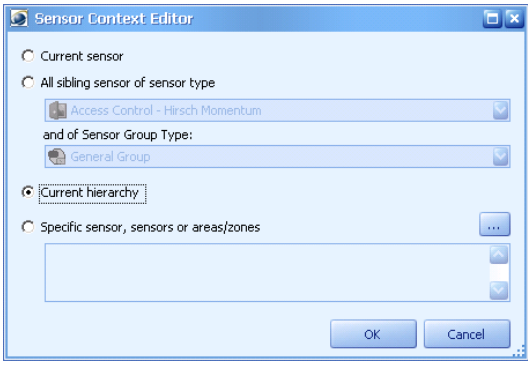
  The Sensor Context Editor window appears.



Select the **All sibling sensor of sensor type** option to apply the command to a sibling sensor, and choose the sensor type and sensor group from the fields.

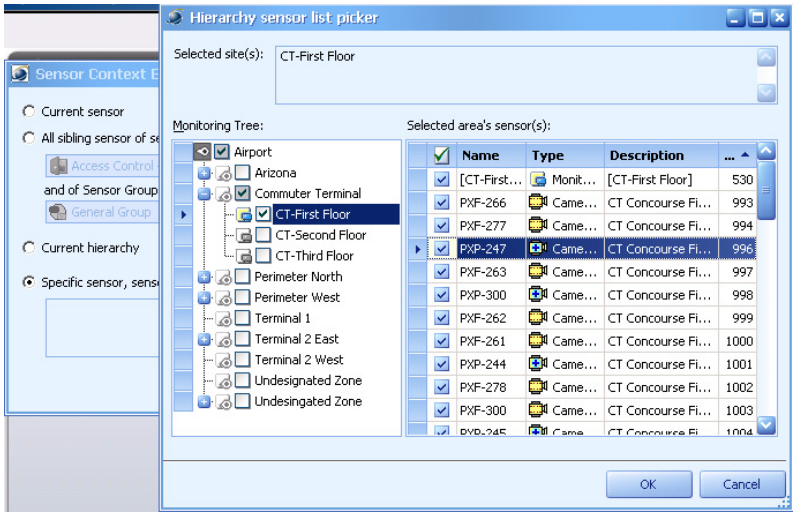


Select the **Current hierarchy** option to apply the command to all access control sensors in the current monitoring area or zone.



When **Current hierarchy** is selected, the Open Door component will first try to obtain the ZoneID from the activity context registry (category PxSensor, key ZoneID); then the AreaID (category PxSensor, key AreaID). Finally, it will try to obtain the AreaID from the associated PxAlert or PxEvent directly.

Select the **Specific sensor, sensors, or areas/zones** option to apply the command to a specific sensor and click the ... button. The Hierarchy sensor list picker window appears where you can navigate the monitoring hierarchy and select the sensor to which this command should be applied. Click **OK** when finished.



Step 6 Click **OK** in the Sensor Context Editor window.

Step 7 Click **OK** in the Open Door Momentarily Activity window.

CHAPTER 16

Diagnosing System Tasks and Alerts

PSOM logs information about alerts raised by sensor devices—this information can be viewed in both the Operation Console and Administration Console. See the *Using Cisco Physical Security Manager* guide for instructions to access alert details.

For the Administration Console only, PSOM also logs information about system-related alerts that have been raised to notify the administrator about such things as services restarting. You can also generate an audit trail of all activity that has occurred in PSOM.

This chapter includes these topics:

- Diagnosing Administrative Alerts, page 16-1
- Diagnosing Monitoring Alerts, page 16-3
- Producing an Audit Trail of all Activity in PSOM, page 16-6

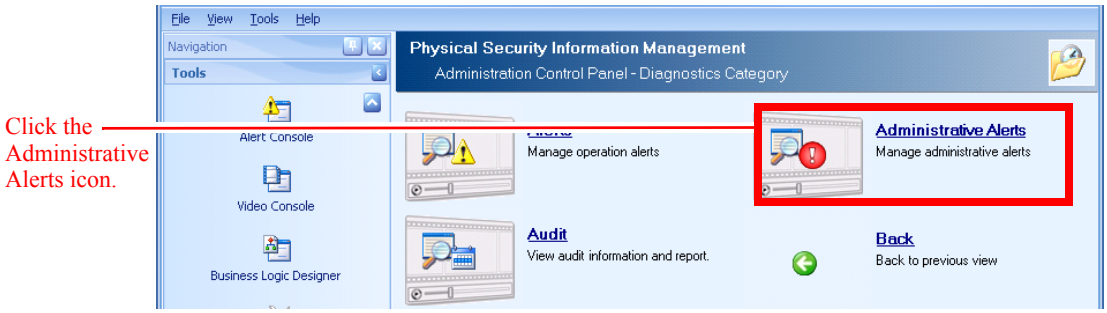
Diagnosing Administrative Alerts

PSOM raises alerts when services are terminated or restarted, as well as under other conditions. You can acknowledge, close and delete these alerts.

To diagnose administrative alerts:

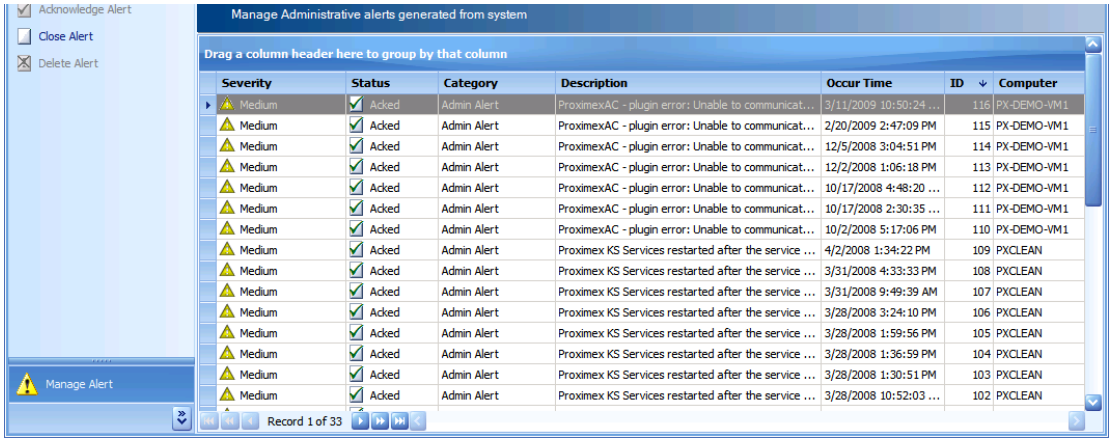
Step 1 Click the **Diagnostics** icon in the Administration Console.

The Diagnostics window appears.



Step 2 Click the **Administrative Alerts** icon.

The Administrative Alert Management window appears.



For each administrative alert, you can view its severity, status, type, description, and timestamp.

Step 3 To sort the list by a different column, drag the column to the area just above the table. The table will resort according to the data in the selected column.

To change the status of an alert:

a. Select the alert from the list.

b. Check the box for the status you want to apply to the alert under **Manage Alert** (left side of window). For example, check the box for the **Acknowledge Alert** option to change the alert's status to acknowledged.

Alerts can be acknowledged, closed and deleted. Only alerts that are closed can be deleted.

You can manage multiple administrative alerts at the same time using the SHIFT or CTRL keys to select multiple rows.

Note When PSOM detects that the ObjectVideo Daemon Service is down, it issues a single administrative alert. However, if the ObjectVideo Server is down, the administrative alert will not be issued. To correct this issue, you must restart the ObjectVideo Daemon Service for the PSOM ObjectVideo Integration Module.

Diagnosing Monitoring Alerts

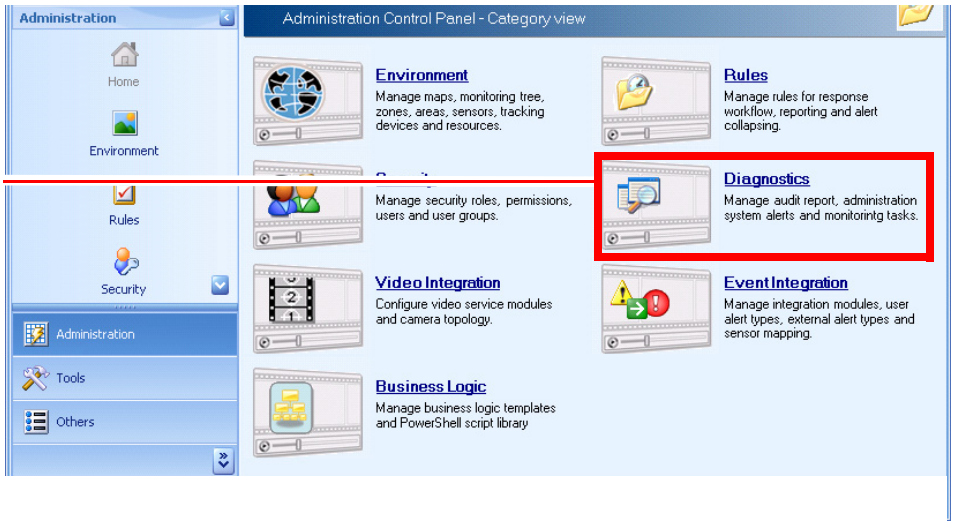
PSOM raises alerts when sensors within the security environment trigger events. You can view all the monitoring alerts that have occurred using the same method that operators use from the Operation Console—the Alert Manager.

To diagnose monitoring alerts:

Step 1 You can launch the Alert Management Console from **Start > All Programs > Cisco Physical Security Operations Manager 5.1 > Alert Management Console**.

You can also click the **Diagnostics** icon in the Administration Console.

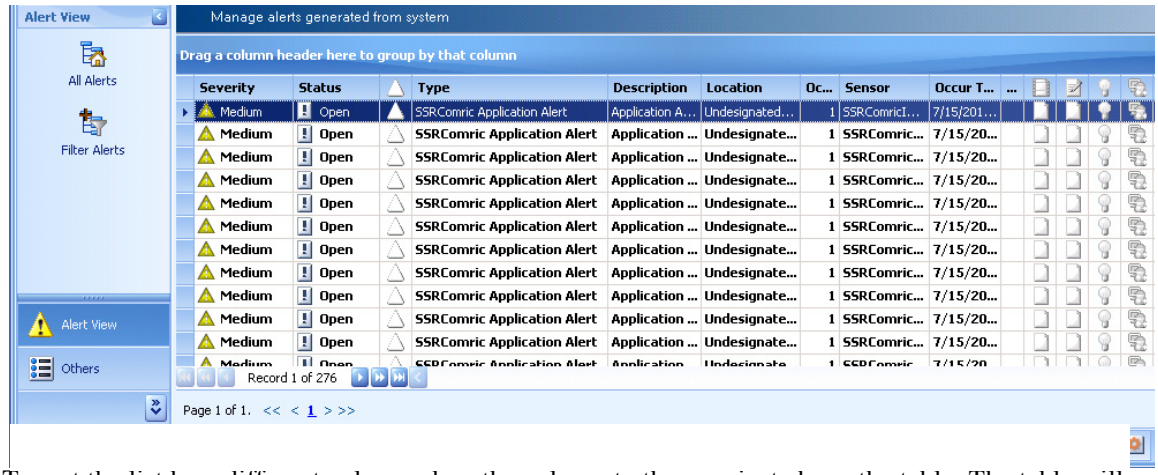
Click the Diagnostics icon.



The Diagnostics window appears.

Step 2 Click the **Alerts** icon.

The Alert Management window appears.

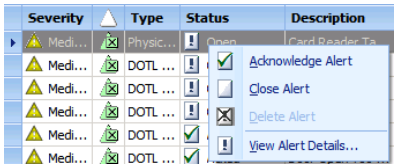


Step 3 To sort the list by a different column, drag the column to the area just above the table. The table will resort according to the data in the selected column.

Step 4 To change the status of an alert:

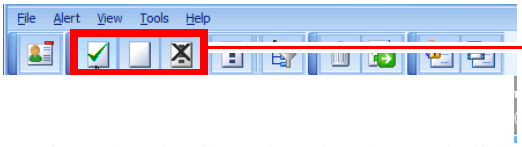
a. Right-click the value in the Status column for the alert you want to change.

b. Select the new status you want to apply to the alert.



Alerts can be acknowledged, closed and deleted. Only alerts that are acknowledged can be closed. Only alerts that are closed can be deleted.

Note You can also select the alert and click the buttons at the top of the window.

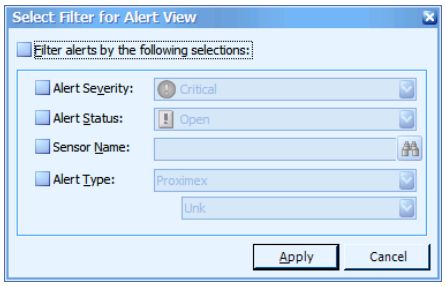


Step 5 To view alert details, select the alert and click the **View Details** button.

Step 6 To pause the refreshing of alerts temporarily, click the Pause Refresh button. To resume, click **Resume Refresh**.

Step 7 To filter the alerts that are displayed in the Alert Manager, click **Filter Alerts** in the left pane or at the top of the window.

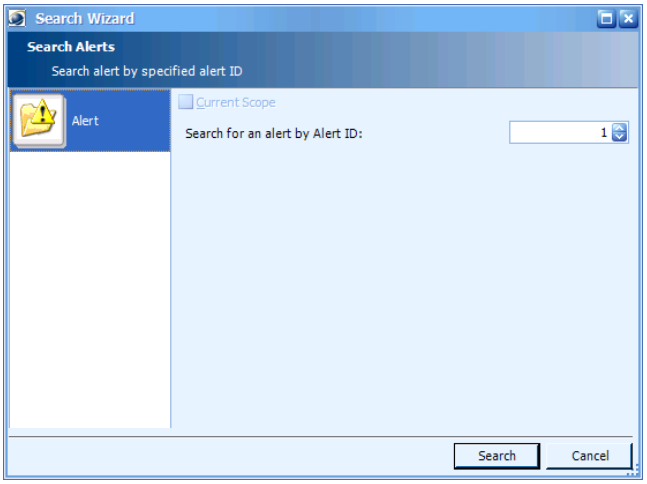
The Select Filter for Alert View window appears where you can click the **Filter alerts by the following selections** option. Then click each option by which you want to filter results. The following example shows results filtered to show only Critical alerts.



Step 8 You can manage multiple administrative alerts at the same time using the SHIFT or CTRL keys to select multiple rows.

Step 9 You can view deleted alerts by clicking **Show Deleted Alerts** at the top of the window.

Step 10 To search for a certain alert, click the **Search** icon in the toolbar. The **Search Wizard** appears.



Enter the ID for the alert you want to find and click **Search**.

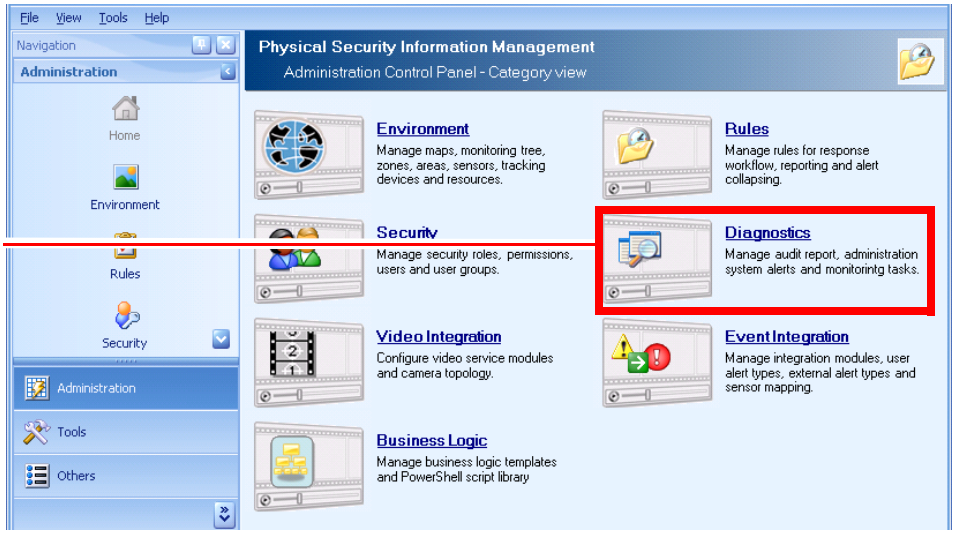
Producing an Audit Trail of all Activity in PSOM

PSOM logs all operational actions taken in the Operation Console and Administration Console, and you can view an audit report of this activity.

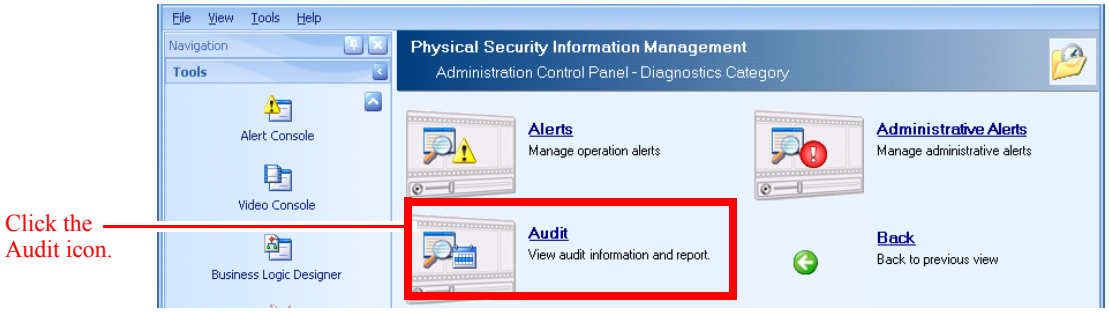
To produce an audit trail of activity in PSOM:

Step 1 Click the **Diagnostics** icon in the Administration Console.

Click the Diagnostics icon.

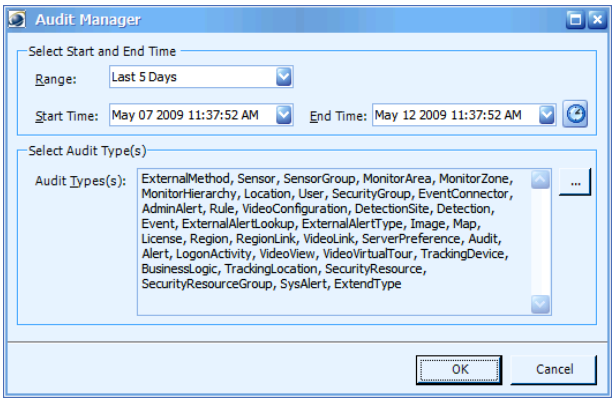


The Diagnostics window appears.



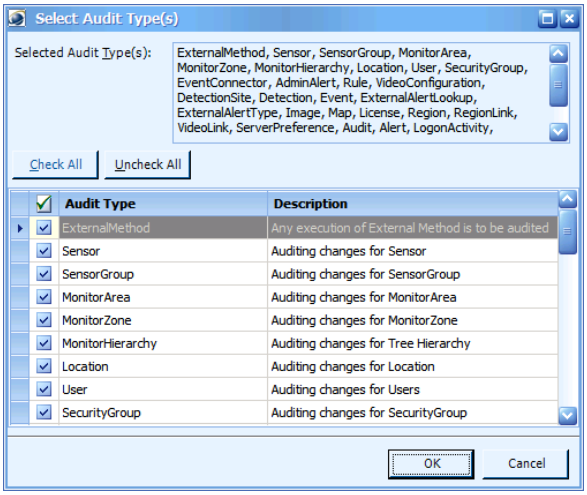
Step 2 Click the **Audit** icon.

The Audit Manager window appears.



Step 3 Click the **More** icon ... in the **Select Audit Types** area to choose the types of activity you want included in this audit report.

The Select Audit Type(s) window appears.



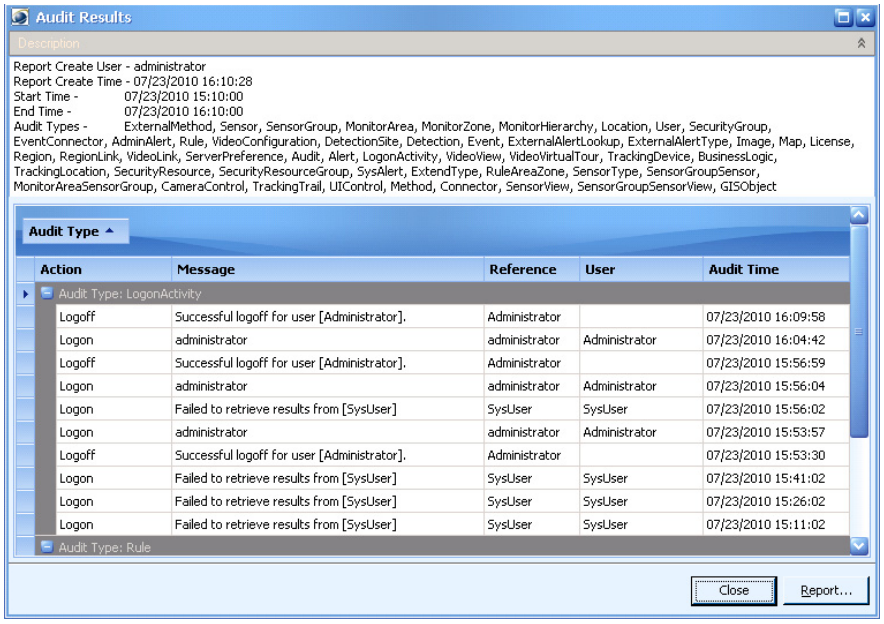
Step 4 Check the items for which you want to view an audit history.

Step 5 Uncheck the items for which you do not want to view an audit history.

Step 6 Click **OK**.

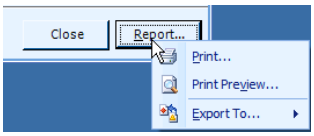
Step 7 Click **OK** in the Audit Manager window to generate the report.

The Audit Results window appears.

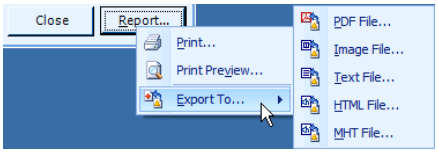


By default the results are grouped by audit type and sorted by audit name. You can expand and collapse groupings using the + or - icons in the top left of each group.

Step 8 Click **Report > Print** to generate a printed version of this audit report.



Step 9 Click **Report > Export To...** to export the report to Adobe PDF (.pdf), JPG (.jpg), text (.txt), HTML (.html) or MHT (.mht) formats.



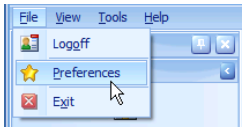
Step 10 Click **Close** to close the Audit Results window.

Setting How Long Audit Records are Stored by PSOM

By default, PSOM stores audit trail information for seven (7) days. You can change this setting to keep audit trail information for more or less time.

To determine how long audit records are kept:

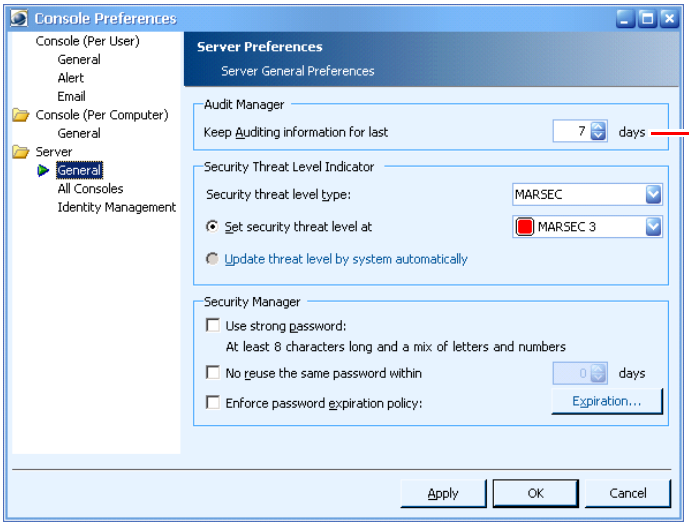
Step 1 Select **File > Preferences** from the menu bar in the Administration Console.



The **Console Preferences** window appears.

Step 2 Click **General** under **Server** in the left navigation bar.

The **General** tab appears.



Step 3 Select the number of days you want to store audit records in the **Keep Auditing information for last** field.

Step 4 Click OK to save your changes.

APPENDIX A

Planning Worksheets

This appendix includes worksheets you can use for planning your PSOM environment. Feel free to make copies of these worksheets.

This appendix includes these sections:

- Access Control System Integration Planning, page A-2
- User Deployment Planning, page A-3
- Locations Planning, page A-4
- Video Camera Planning, page A-5
- Monitoring Zone Planning, page A-6
- Monitoring Areas Planning, page A-7
- Task Items Planning, page A-8
- Response Workflow Planning, page A-9
- EZ-Track Planning, page A-10

Access Control System Integration Planning

Table A-1 Access Control System Integration Planning

Access Control #	IP Address	Server Login Name	Server Login Password

User Deployment Planning

Table A-2 User Deployment Planning

Employee	User Name	Password	User Role	User Group	Description

Locations Planning

Table A-3 Locations Planning

Location Name	Description

Video Camera Planning

Table A-4 Video Camera Planning

Device ID	Location	View Range (in degrees)	View Distance (in feet)	View Direction (in degrees

Monitoring Zone Planning

Table A-5 Monitoring Zone Planning

Monitoring Zone	Description	Areas that should be included

Monitoring Areas Planning

Table A-6 Monitoring Areas Planning

Monitoring Area	Description	Sensor Groups to include

Task Items Planning

Table A-7 Task Items Planning

Task Item	Required to Acknowledge Alerts?	Required to Close Alerts?

Response Workflow Planning

Table A-8 Response Workflow Planning

Response Task	Types of Alerts	Task Items to Perform	Task Items to Complete for Acknowledging Alerts	Task Items to Complete for Closing Alerts

EZ-Track Planning

Table A-9 EZ-Track Planning

Source Video Camera	UP Sensor #	Seconds Walk to UP	DOWN Sensor #	Seconds Walk to DOWN	LEFT Sensor #	Seconds Walk to LEFT	RIGHT Sensor #	Seconds Walk to RIGHT

APPENDIX **B**

Backup and Restore PSOM Database

This appendix explains how to backup and restore the PSOM database. This appendix includes these topics:

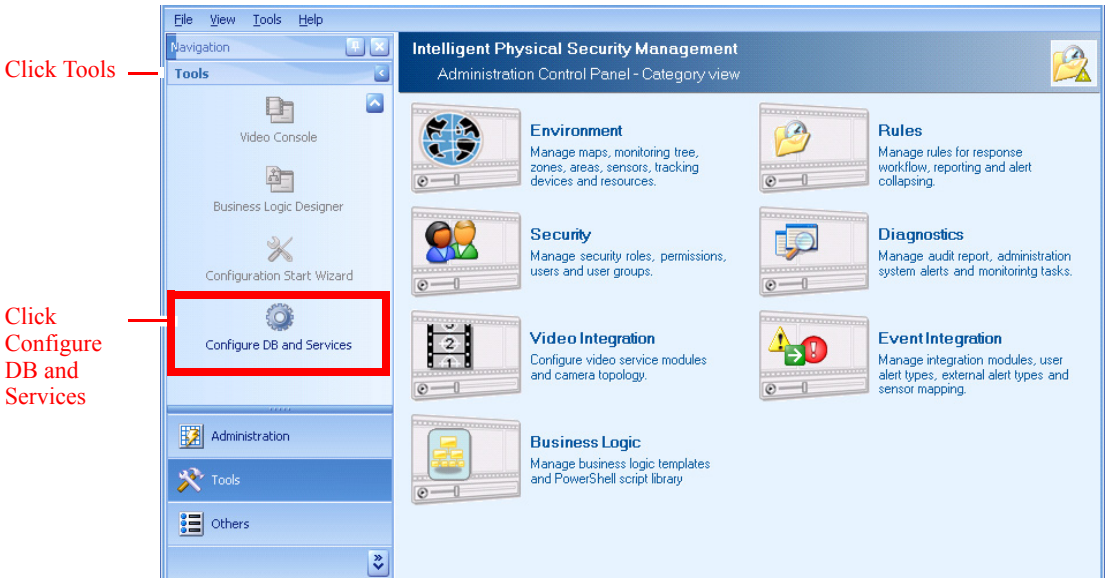
- Scheduled Back-up of the PSOM Database, page B-1
- Manually Backing up the PSOM Database, page B-3
- Restoring the PSOM Database, page B-5
- Grooming the PSOM Database, page B-7

Scheduled Back-up of the PSOM Database

You can configure when the PSOM database is scheduled for backup.

To configure the backup schedule for the PSOM database:

Step 1 Click Tools in the Navigation bar, and then click **Configure DB and Services**.

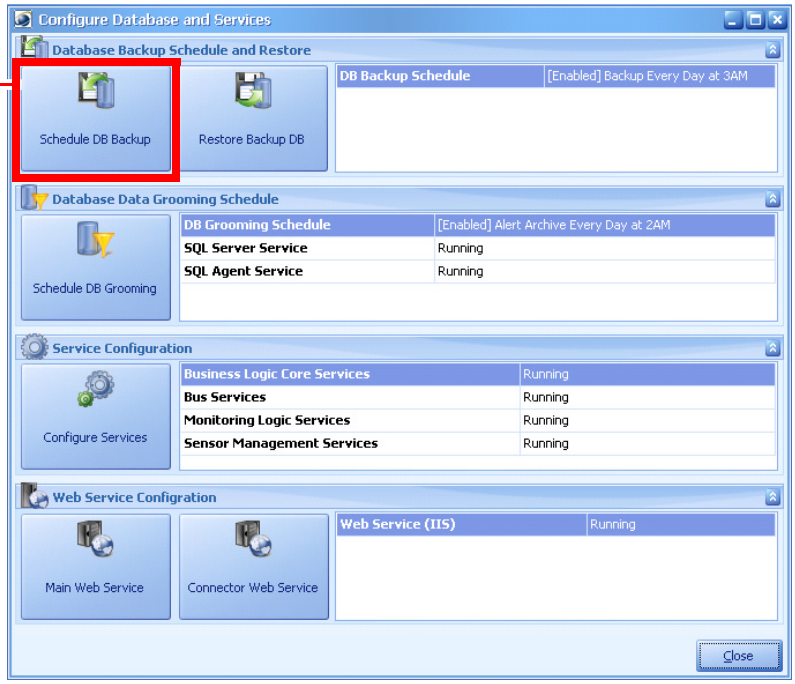


A window appears asking you to logoff PSOM.

Step 2 Click **Yes**.

The Configure Database and Services window appears.

Click Schedule DB Backup



Step 3 Click **Schedule DB Backup**.

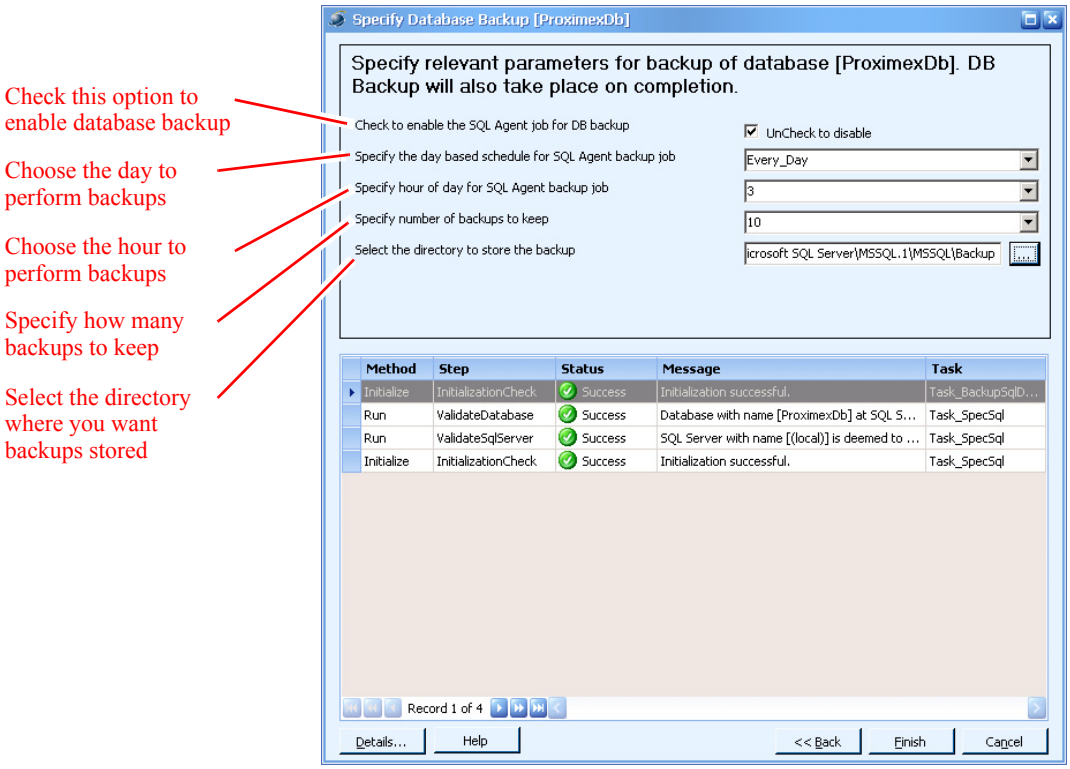
The Server and Database for Repository window appears.

Step 4 In the **Provide the SQL Server hosting the target database** field, enter (local) unless the PSOM Repository is not located on the current machine. In this case, enter the name of the server hosting the Repository.

Step 5 Enter **ProximexDb** in the **Select or type in Database name** field, unless the PSOM Repository has been given a different name.

Step 6 Click **Next**.

The Specify Database Backup window appears.



Step 7 Periodic backups of the PSOM Repository will be triggered by a SQL Agent process if the **Check to enable the SQL Agent job** option is selected. If this option is not checked, then the database backup will not take place.

Step 8 Select the day of the week to perform database backups from the **Specify the day based schedule for SQL Agent job** field, or select **Every_Day** to backup the database every day.

Step 9 Select the time that database backups should start from the **Specify the hour of day for SQL Agent job** field.

Step 10 Select the number of backups you want to keep from the **Specify number of backups to keep** field.

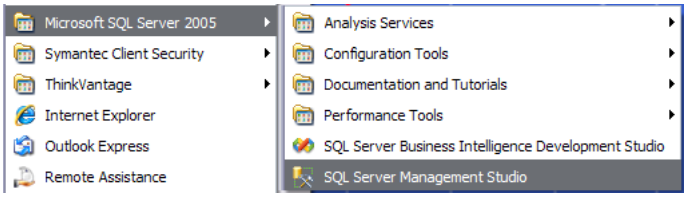
Step 11 Choose the directory where you want to store database backups from the **Select the directory to store the backup** field.

Step 12 Click **Finish** to save your changes.

Manually Backing up the PSOM Database

To manually backup the PSOM database:

Step 1 Launch **SQL Server Management Studio**.

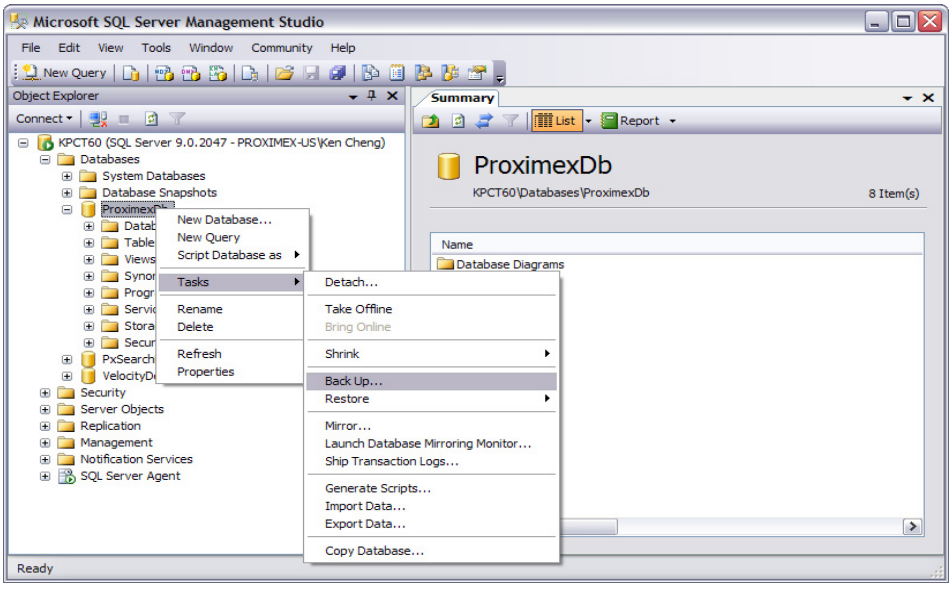


Step 2 Connect to the appropriate instance of the Microsoft SQL Server Database Engine.

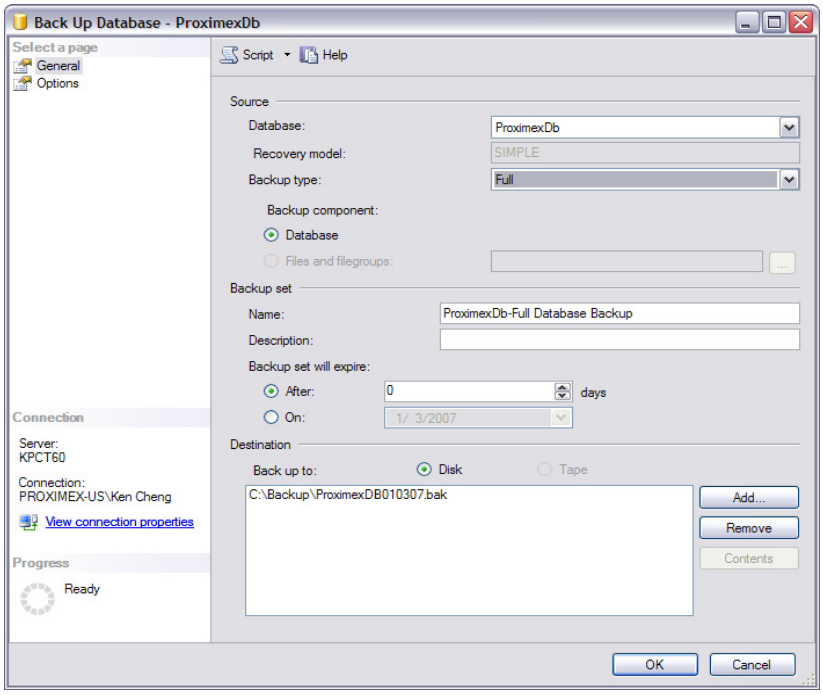
Step 3 In Object Explorer, click the server name to expand the server tree.

Step 4 Expand **Databases**, and select the **ProximexDb** database.

Step 5 Right-click the database and select **Tasks > Back Up** from the right-click menu.



The **Back Up Database** window appears.



Step 6 In the **Database** field, verify the database name (**ProximexDb**).

Step 7 In the **Backup type** field, select the kind of database backup you want to perform. In this case, select **Full**.

Note You can perform a database backup for any recovery model: **FULL, BULK_LOGGED**, or **SIMPLE**. After you create a full database backup, you can create a differential database backup.

Step 8 Click **Database** under **Backup component**.

Step 9 In the **Name** field under **Backup set**, either accept the default name, or enter a different name for the backup set.

Step 10 In the **Description** field, enter a description of the backup set.

Step 11 Choose the type of backup destination by clicking **Disk**. To select the path of the backup file click **Add**. The selected paths are displayed in the **Backup to** field.

Step 12 Click **OK**.

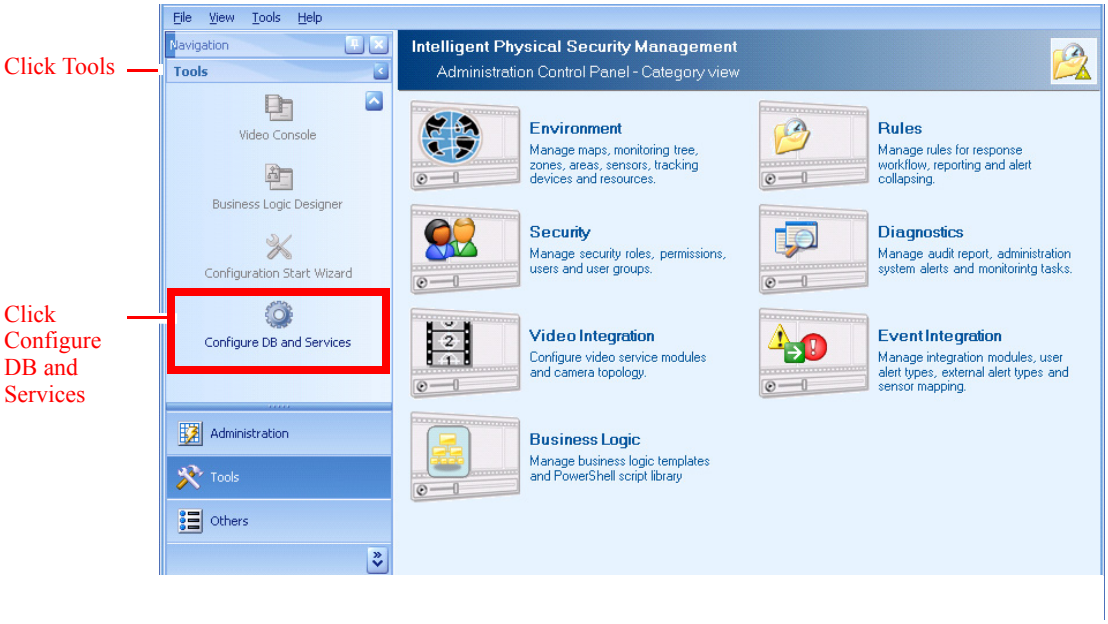
A confirmation dialog box appears.

Restoring the PSOM Database

To restore the PSOM database:

Step 1 Make sure that there are no other administrators or operators who are using the PSOM database.

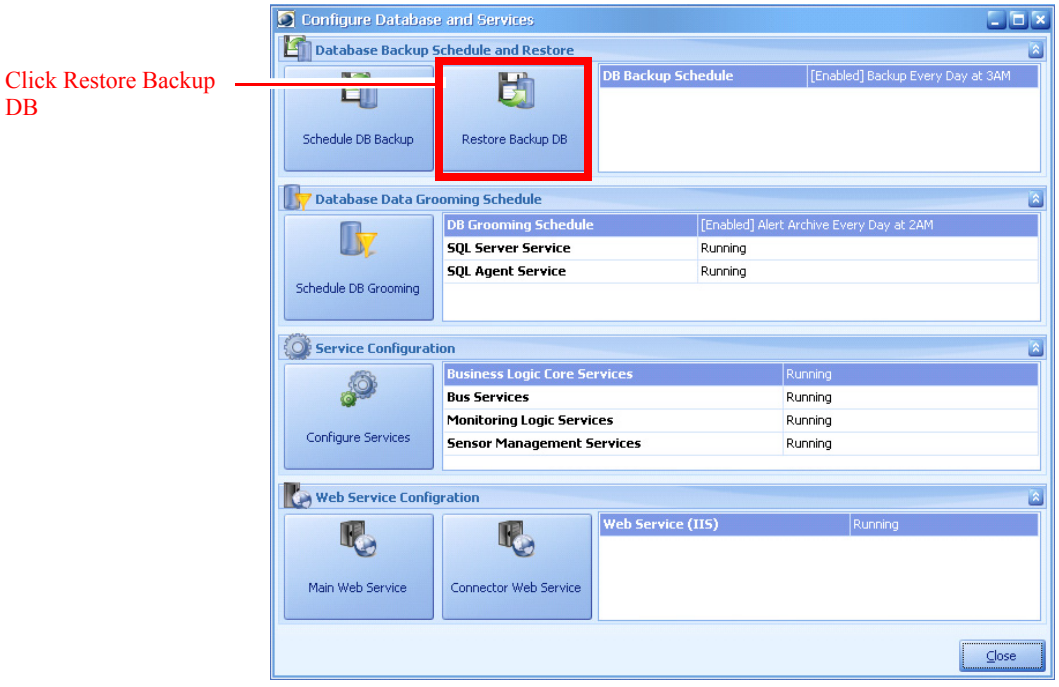
Step 2 Click **Tools** in the Navigation bar, and then click **Configure DB and Services**.



A window appears asking you to logoff PSOM.

Step 3 Click **Yes**.

The **Configure Database and Services** window appears.



The **Server and Database for Repository** window appears

Step 4 Provide the name of the SQL Server host in the field provided.

Step 5 Select **ProximexDb** from the next field.

Step 6 Click **Next**.

The Restore Database window appears.

Step 7 Choose the backup file to restore from the **Select backup file for database restore** field.

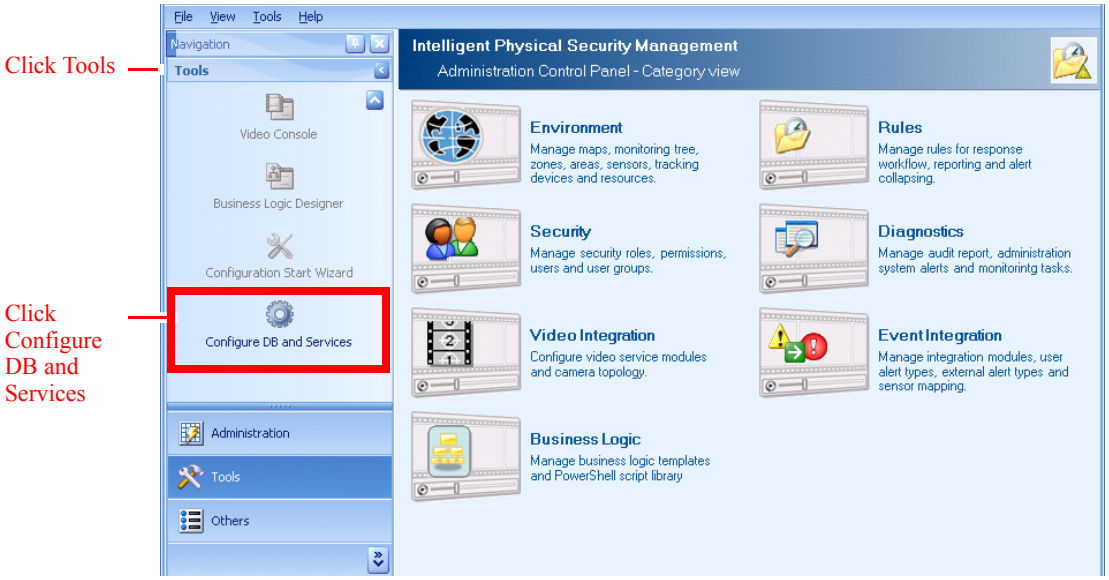
Step 8 Select the instance of the backup to restore (by timestamp) from the **Select the backup set to database restore** field.

Step 9 Click **Finish**.

Grooming the PSOM Database

To set the grooming schedule for the PSOM database:

Step 1 Click Tools in the Navigation bar, and then click **Configure DB and Services**.

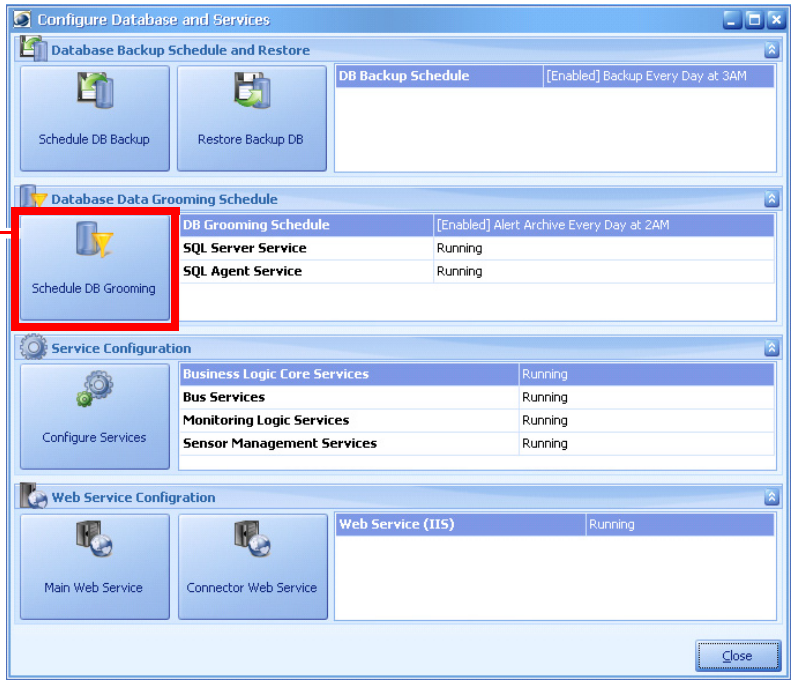


A window appears asking you to logoff PSOM.

Step 2 Click **Yes**.

The Configure Database and Services window appears.

Step 3 Click **Schedule DB Grooming**.



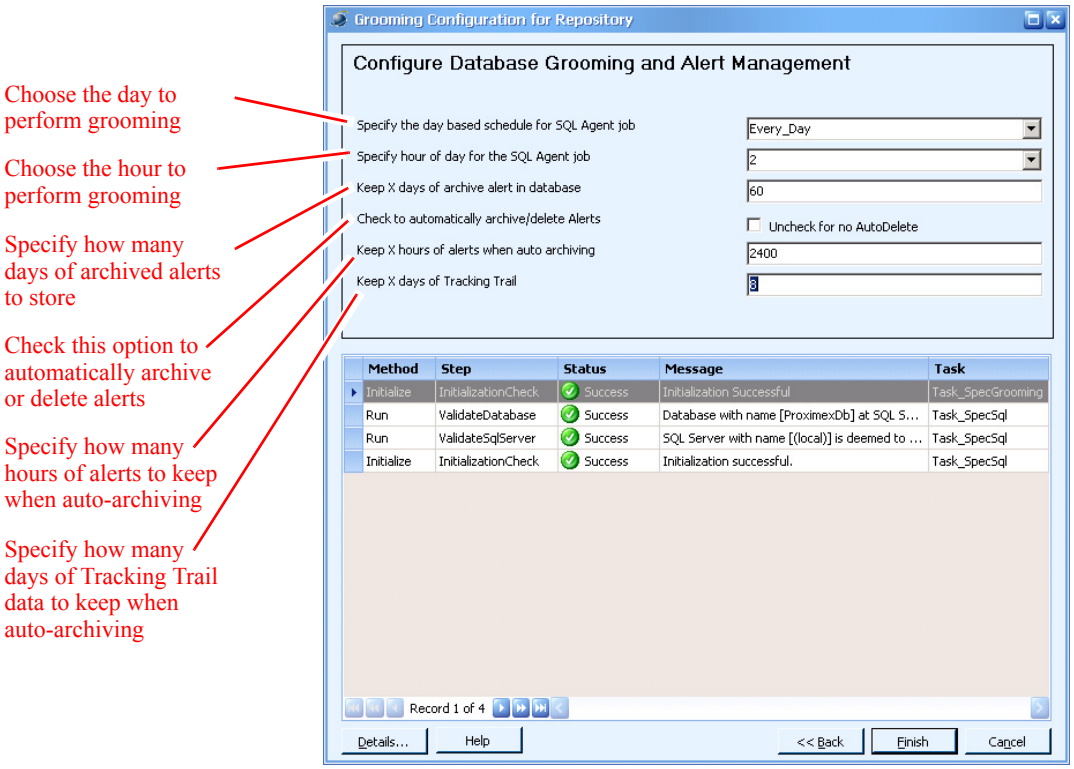
The Server and Database for Repository window appears.

Step 4 Provide the name of the SQL Server host in the field provided.

Step 5 Select **ProximexDb** from the next field.

Step 6 Click **Next**.

The Grooming Configuration for Repository window appears.



Step 7 Choose the day to perform database grooming from the **Specify the day based schedule for SQL Agent job** field, or select **Every_Day** to perform database grooming every day.

Step 8 Choose the hour to perform database grooming from the **Specify the hour of day for the SQL Agent job** field.

Step 9 Specify how many days of archived alerts to store in the **Keep X days of archive alert in database** field.

Step 10 To automatically archive or delete alerts, check the **Check to automatically archive/delete Alerts** option.

Step 11 Specify how many hours of alerts to keep when auto-archiving from the **Keep X hours of alerts when auto archiving** field.

Step 12 Specify how many days of Tracking Trail data to keep when auto-archiving from the **Keep X days of Tracking Trail** field.

Step 13 Click **Finish**.

APPENDIX C

Reconfiguring PSOM Services

This appendix explains how to reconfigure PSOM Services, PSOM Web Service, and PSOM Connector Web Service after the initial deployment.

This appendix includes these topics:

- Reconfiguring Settings for PSOM Services, page C-1
- Specifying Custom Parsing, page C-13
- Changing the Configuration of the PSOM Web Service, page C-16
- Changing the Configuration of the Connector Web Service, page C-19
- Reconfiguring Settings for PSOM User Services, page C-22

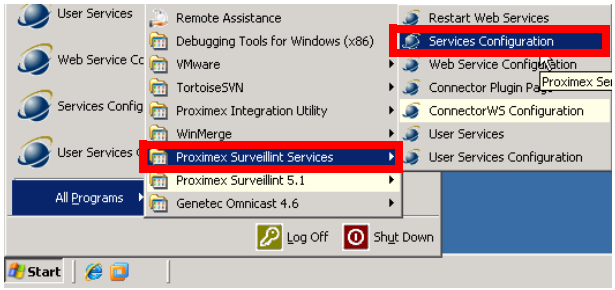
Reconfiguring Settings for PSOM Services

You can change the configuration of PSOM Services after the initial deployment of PSOM.

Note You must be a member of the local *Administrators* group to launch **Services Configuration**.

To reconfigure PSOM Services:

Step 1 From the **Start** menu, select **All Programs > Cisco Physical Security Operations Manager > Services Configuration**.



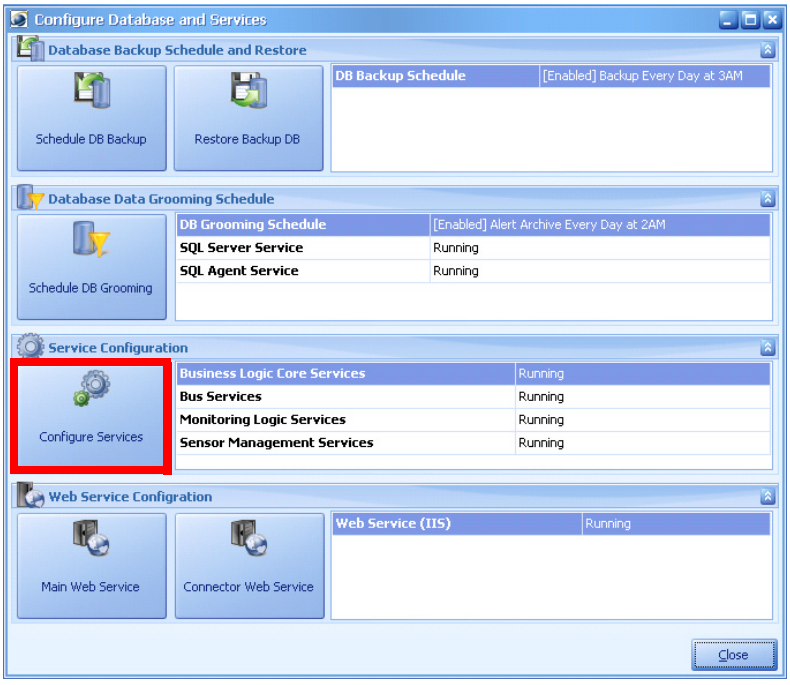
Or from the PSOM Administration Console:

a. Select **Tools** in the **Navigation** pane

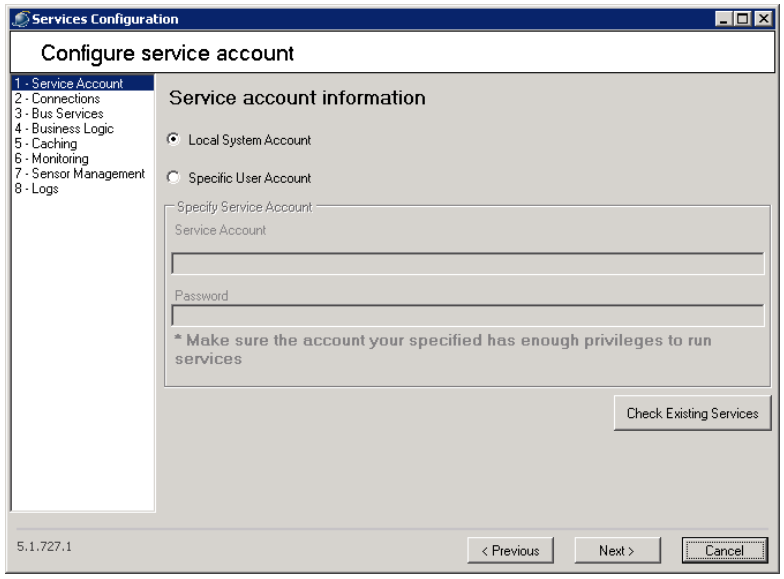
b. Click **Configure DB and Services**.

c. Click **Yes** to log off PSOM temporarily while you configure the services.

d. Click **Configure Services**.



The **Services Configuration** dialog box appears.

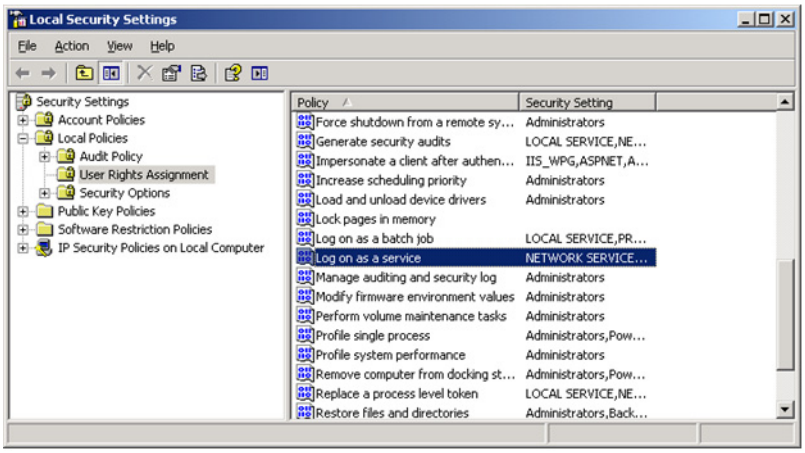


On the Service account information window, select **Local System Account** to use the default account to run PSOM Services.

If you want to specify a different user account, make sure the account meets the following criteria:

- Belongs to the local Administrators group
- Has permission to SQL Server database through Integrated Windows Security
- Has the *Log on as a service* permission

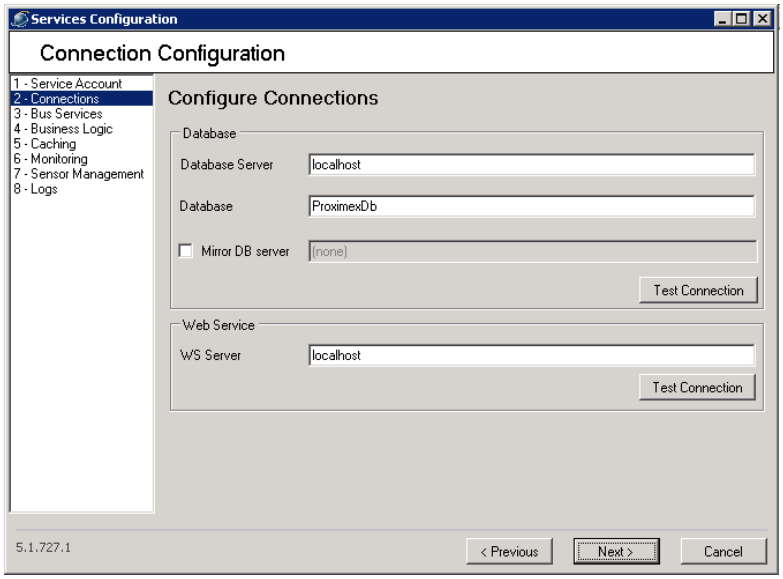
To ensure the account has the *Log on as a service* permission, you need to launch the Local Security Settings window, select **Local Policies > User Rights Assignment**, and double-click **Log on as a service**.



When specifying a user account, select **Specific User Account** and enter:

- The name of the user account on the Windows Server that PSOM Services will use to perform administrative functions in the **Service Account** field.
- The password for that service account in the **Password** field.

Step 2 Click **Next** or **2 – Connections** to configure connections to the PSOM Repository and PSOM Web Service.



On the Configure Connections window:

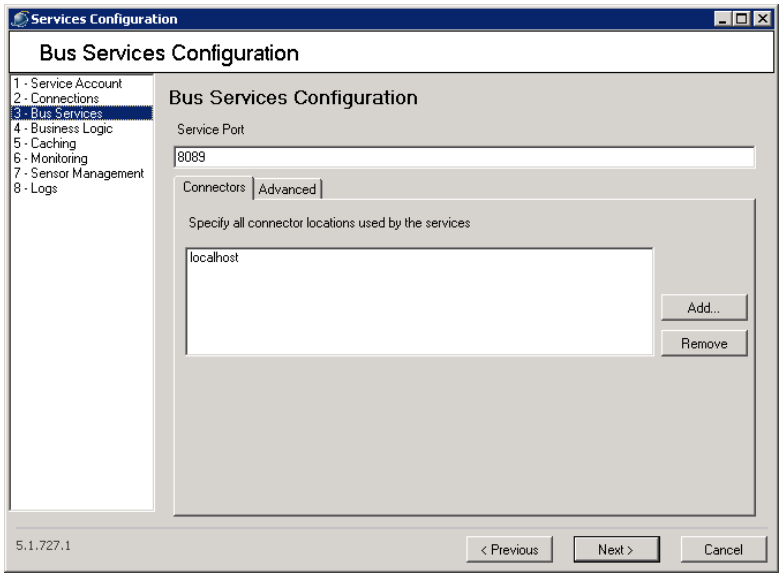
- The **Database Server** field contains **localhost** unless you installed PSOM Repository on a different machine in the network. In this case, enter the IP address or server name of the machine where PSOM Repository is installed.
- The **Database** field contains **ProximexDb**, unless there is a reason to change the name of the PSOM Repository.
- If you are using a mirrored database, click **Mirror DB server** and enter the IP address or server name of the machine where the mirrored database resides.
- The **WS Server** field contains **localhost** unless you installed PSOM Web Service on a different machine in the network. In this case, enter the IP address or server name of the machine where you installed PSOM Web Service.

Note PSOM Services use the Integrated Security mode for connections. Ensure that SQL Server allows this connection mode.

Click **Test Connection** in the **Database** or **Web Service** areas to verify settings.

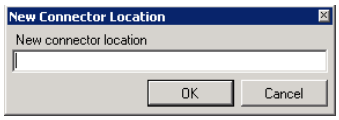
Note When you click **Test Connection for Database**, your current Windows account is used to authenticate the specified SQL Server and SQL database.

Step 3 Click **Next** or select **3 - Bus Services** on the left side of the window.



On the Bus Services Configuration window:

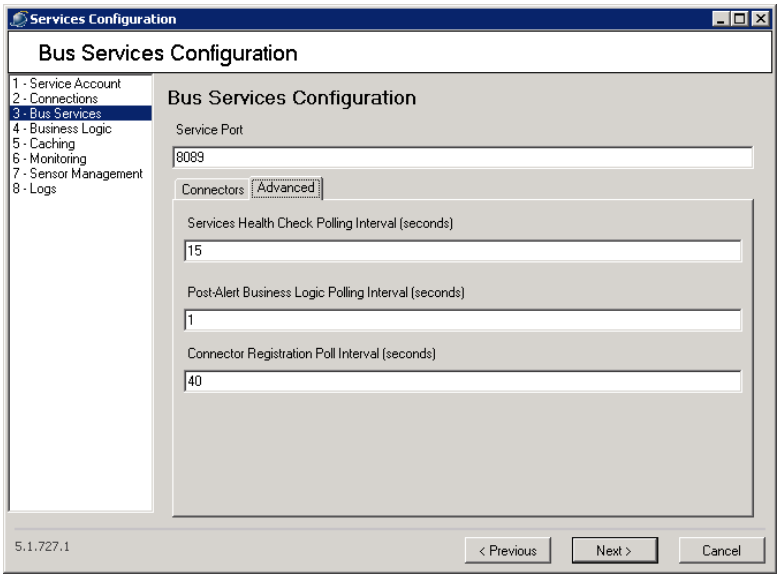
- The **Service Port** field contains the port number under which PSOM Services run.
- The **Connectors** tab shows all the machines where PSOM Integration Modules are installed. Click **Add** to define a new location, enter the IP address or server name in the dialog box and click **OK**.



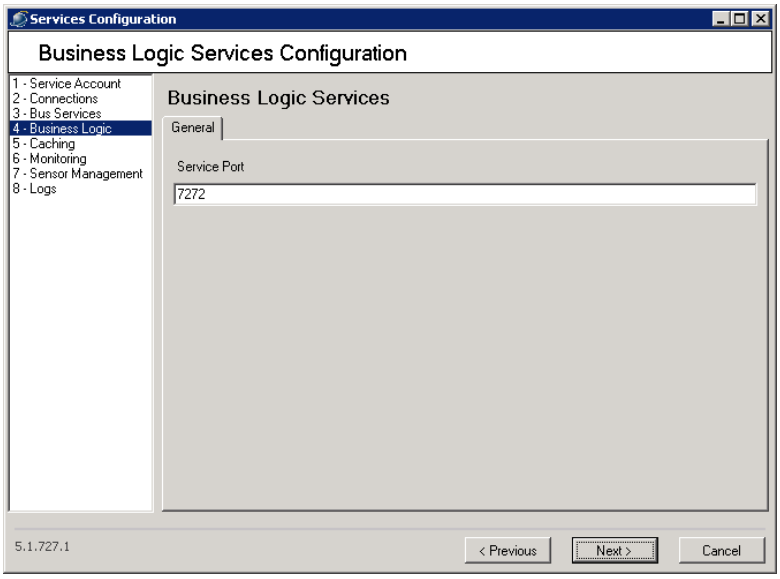
- The **Advanced** tab shows various polling interval settings at which PSOM Services are polled for general health (the **Services Health Check Polling Interval** field) as well as the interval at which PSOM polls for business logic after an alert has occurred (the **Post-Alert Business Logic Polling Interval**).

Note A shorter polling interval for the **Post-Alert Business Logic Polling Interval** can improve the response time for Alert Business Logic, but it will negatively impact CPU performance and database response on the host machine.

The **Connector Registration Poll Interval** shows the interval at which the Bus Services updates commands and sensor type registration for connectors. A shorter polling interval will generally improve the response time for the system to discover and import new or updated sensor types and commands, but it will negatively impact the CPU performance and connector performance on the host machine.



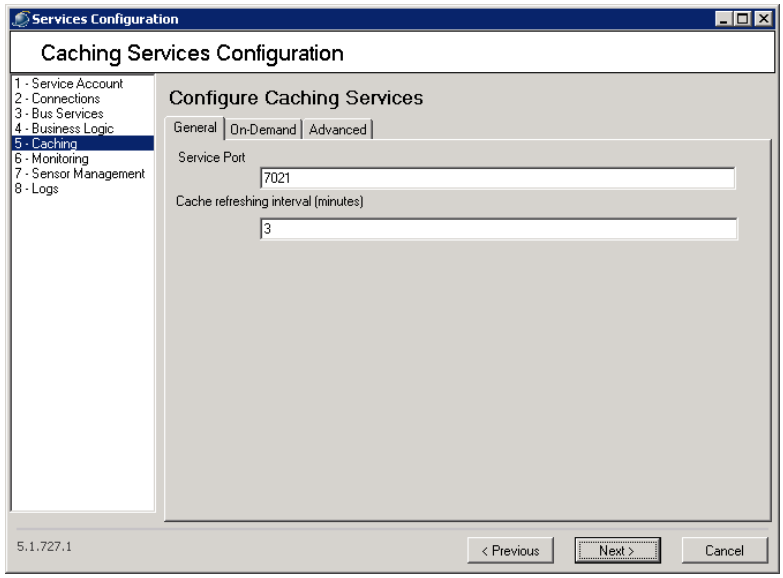
Step 4 Click **Next** or select **4 - Business Logic** on the left side of the window.



On the Business Logic Services window:

- The **Service Port** field contains the port number under which PSOM Business Logic Services run.

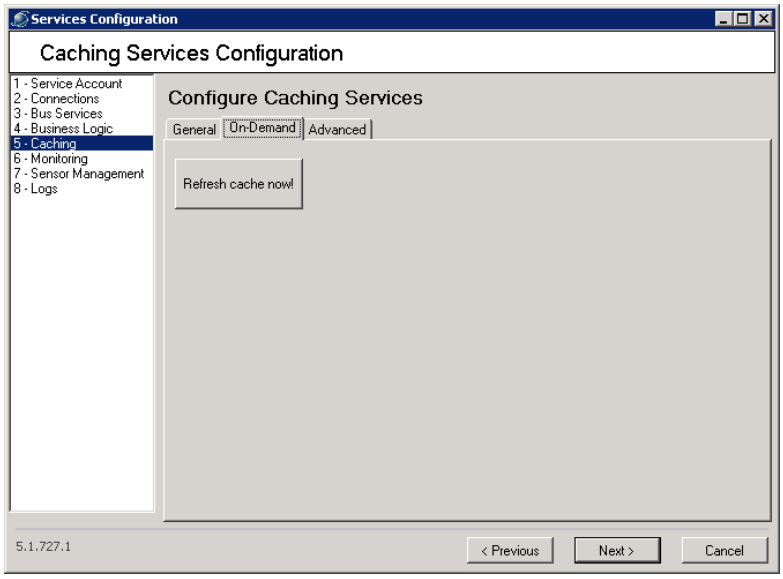
Step 5 Click **Next** or select **5 - Caching** on the left side of the window.



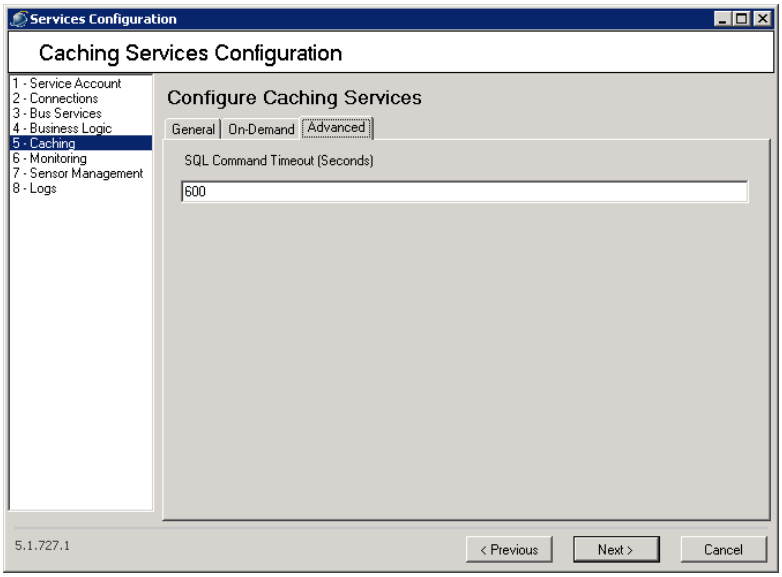
The PSOM Caching Service speeds up business logic execution by caching monitoring hierarchy and sensor map information.

On the Configure Caching Services window:

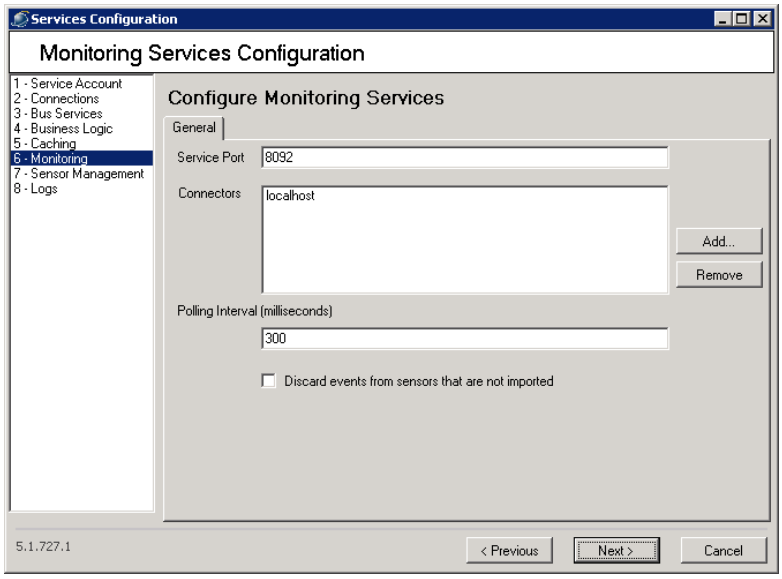
- The **General** tab allows you to specify the port number under which the PSOM Caching Service runs in the **Service Port** field, as well as the number of minutes that should pass before the Caching Service refreshes the cache in the **Cache refreshing interval** field.
- The **On-Demand** tab allows you to instantly refresh the cache by clicking the **Refresh cache now** button. You can refresh the cache once installation is complete by relaunching the Services Configuration window.



- The **Advanced** tab enables you to resolve poor SQL Server query performance by increasing the timeout that the Caching Service uses for SQL commands in the **SQL Command Timeout** field.

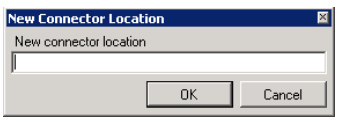


Step 6 Click **Next** or select **6 - Monitoring** on the left side of the window.



On the Configure Monitoring Services window:

- The **Service Port** field contains the port number under which PSOM Monitoring Services run.
- The **Connectors** field shows all the machines where PSOM Integration Modules are installed that the PSOM Monitoring Services need to track for ongoing event integration. Click **Add** to define a new location, enter the IP address or server name in the dialog box and click **OK**.

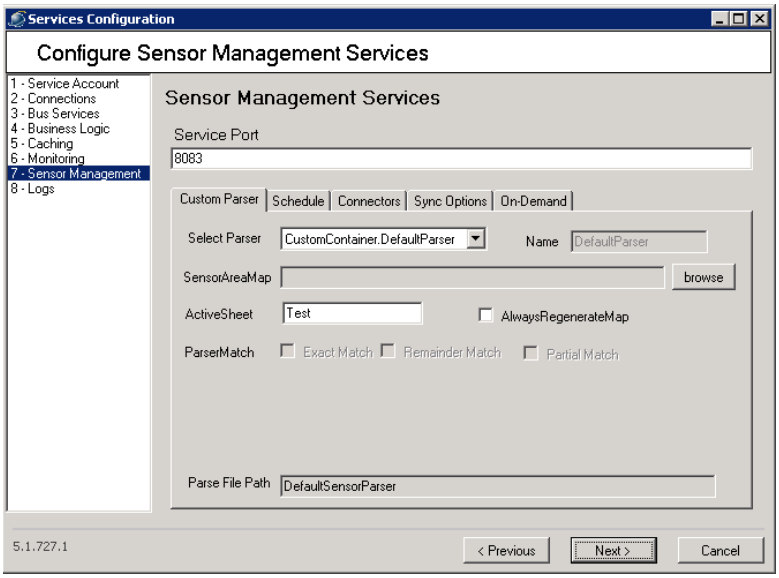


- The **Polling Interval** field shows the interval (in milliseconds) at which the PSOM Monitoring Service will seek new events. Check the **Discard events from sensor that are not imported** if you do not want the Monitoring Service to report on events issued by entities that are not sensors.

Note If you check the **Discard events from sensors that are not imported** option, the events from these sensors will not become alerts in PSOM.

The minimum polling interval for monitoring services is 100 milliseconds. However the recommended interval is 250 milliseconds or higher to avoid CPU contention within the host environment. If you have a dual core or quad core host environment, setting the polling interval to 100 milliseconds may be sufficient.

Step 7 Click **Next** or select 7 **- Sensor Management** on the left side of the window.

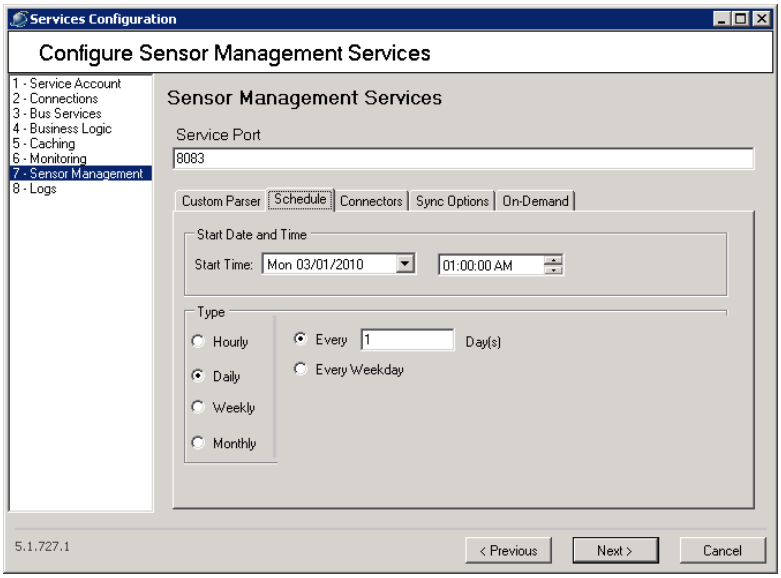


On the Sensor Management Services window:

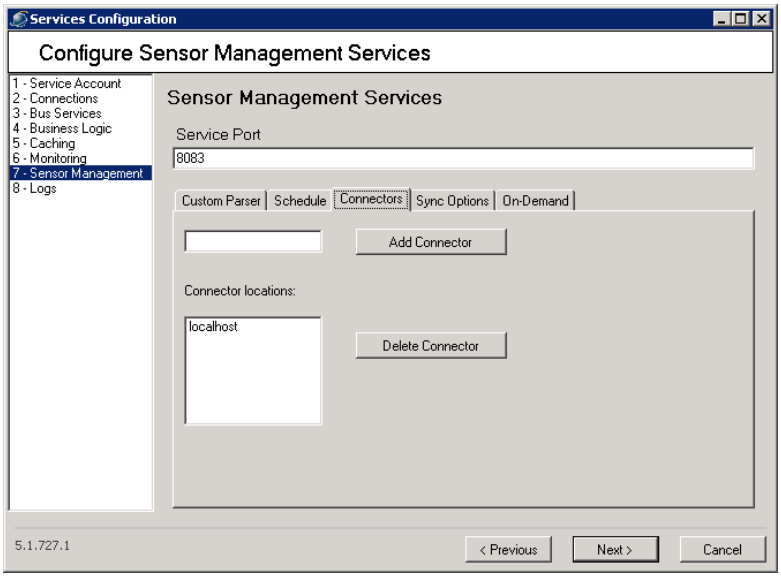
- The **Service Port** field contains the port number under which PSOM Sensor Management Service runs.
- On the **Custom Parser** tab, the default parser groups all newly discovered sensors into one category: undesignated zone, undesignated area and undesignated location. You can specify how each sensor should be grouped by passing the enhanced parser an Excel spreadsheet that maps sensor names to areas and locations.

  If you select **Default Parser** from the **Select Parser** field, the values in the other fields either are greyed out or ignored. The default parser groups all newly discovered sensors into one category: undesignated zone, undesignated area and undesignated location.

  If you want to perform custom parsing, see <Link>**Specifying Custom Parsing** on page 13 for details.
- On the **Schedule** tab, select the date and time that the PSOM Sensor Management Service will begin running, and then choose how frequently it will run (hourly, daily, weekly, monthly) in the **Type** area. Specify the interval at which the service will execute as well.

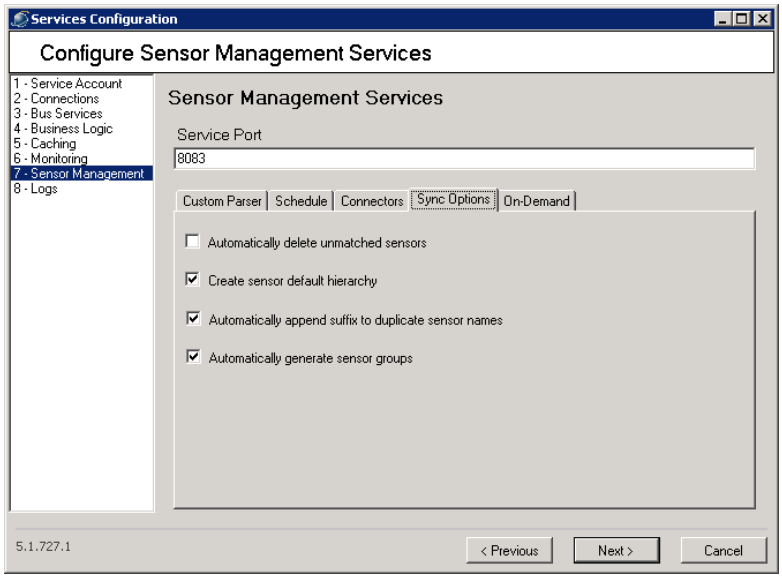


- On the **Connectors** tab, enter the default location where the Sensor Management Service should seek PSOM Integration Modules.



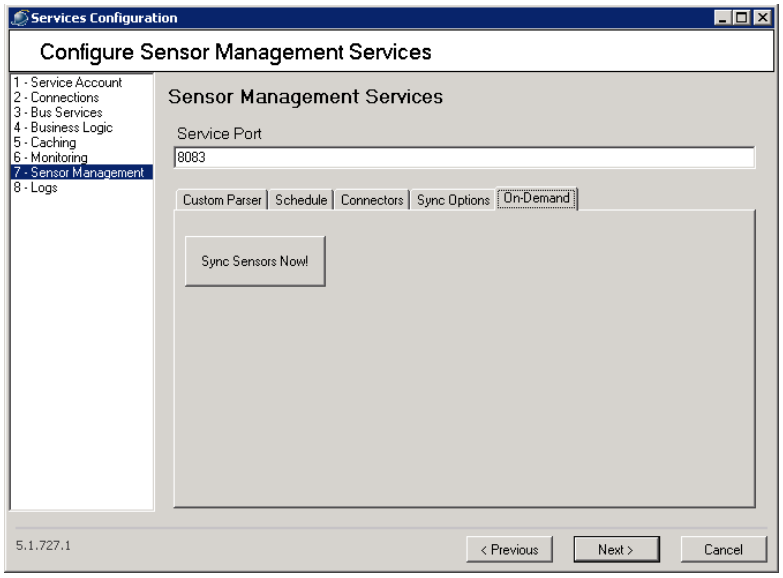
- On the **Sync Options** tab:
  - Check the **Automatically delete unmatched sensors** option if you want to remove any sensors from PSOM that could not be identified in the external system by the Sensor Management Service.
  - Check the **Create sensor default hierarchy** option if you want the Sensor Management Service to create a sensor hierarchy by default as sensors are added to PSOM. Sensors will be grouped as specified in the custom parsing (defined on the **Custom Parser** tab) or by default.
  - Check the **Automatically append suffix to duplicate sensor names** option to append a number to the sensor name if it already exists in the database.

– Check the **Automatically generate sensor groups** option to create sensor groups with a prefix of “SG” in the name.

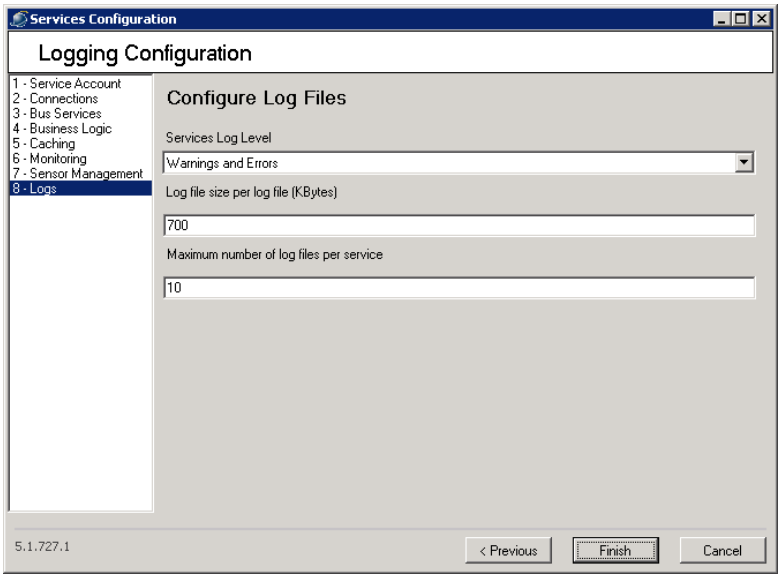


– On the **On-Demand** tab, you can run the sensor synchronization process on demand by clicking the **Sync Sensors Now** button.

Note If sensor synchronization is already in progress, then the on-demand sync request will be ignored.



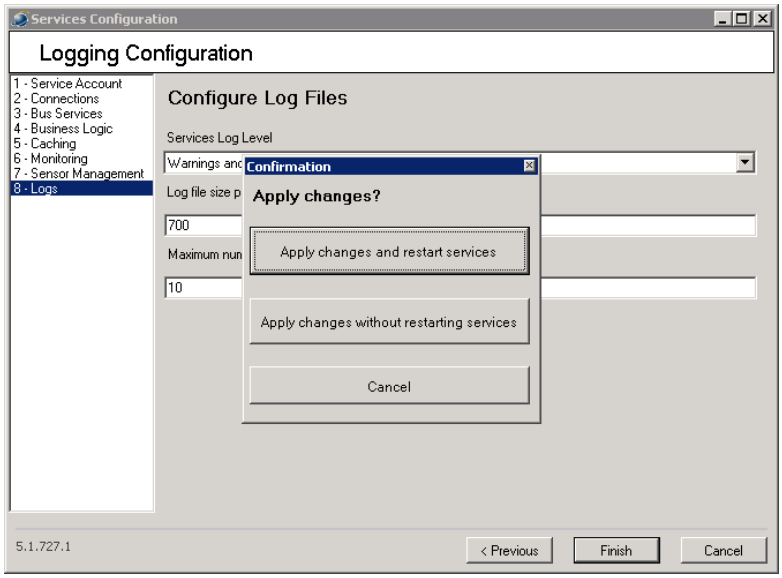
Step 8 Click **Next** or select **8 - Logs** in the left side of the window.



On the Configure Log Files window, select the level of events that should be maintained in the PSOM log files.

Note By default all services log file are located in the **\Program Files\Cisco PSOM\Managed Services\Log** directory.

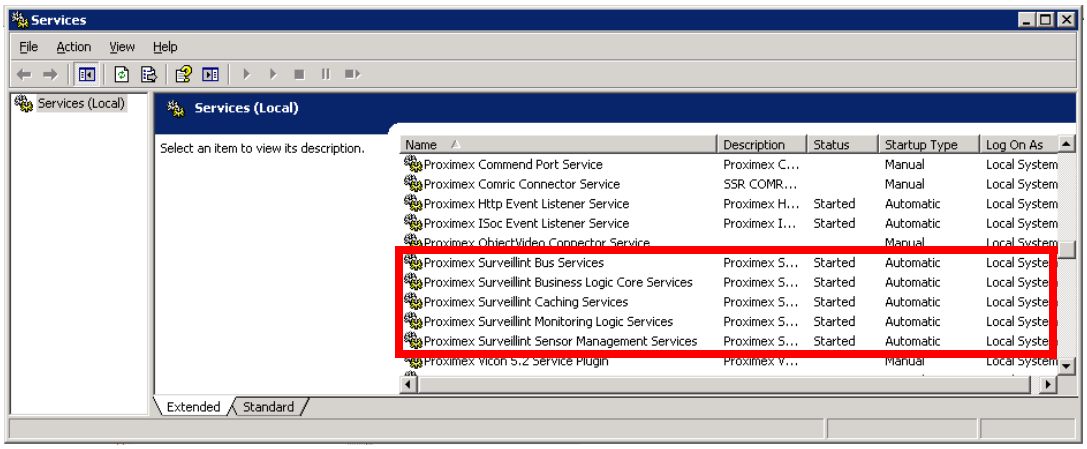
Click **Finish**. The following prompt appears.



Step 9 Click **Apply changes and restart services**. The PSOM Services restart and a confirmation window appears.

Step 10 Click **Finish**.

Step 11 If you want to verify installation, open the **Service Manager** by clicking **Start > Administrative Tools > Services**, and verify that the following services are running: PSOM Bus Services, PSOM Business Logic Core Services, PSOM Caching Services, PSOM Monitoring Logic Services, and PSOM Sensor Management Services.

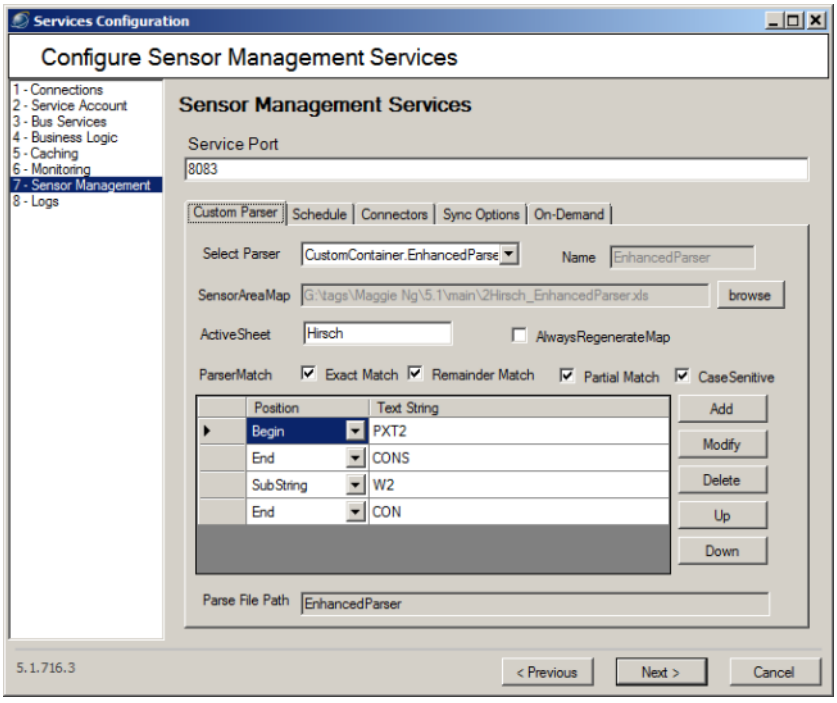


Specifying Custom Parsing

You can perform custom parsing to specify how each sensor should be grouped in PSOM. To do so, you will need to supply an Excel spreadsheet that has the name of each sensor matched with its associated monitoring zone, monitoring area, and location.

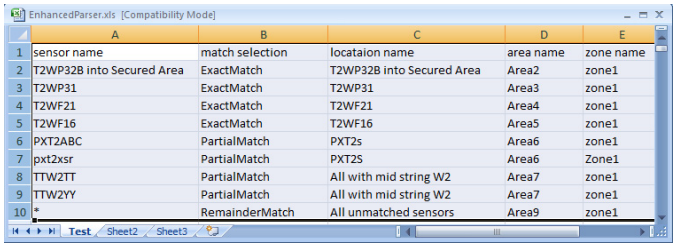
To specify custom parsing:

Step 1 Navigate to the **Custom Parser** tab under **7–Sensor Management** of the Services Configuration window.



Step 2 Select **CustomContainer.EnhancedParser** from the **Select Parser** field.

Step 3 Click the **Browse** button next to the **SensorAreaMap** field and select the location of the Excel spreadsheet that maps sensor names retrieved from third-party sensor lists with the monitoring zones, monitoring areas, and locations where the sensors should be associated in PSOM. The spreadsheet also needs to specify what type of match should be used when mapping each sensor name pattern with sensor names retrieved from the third-party sensor list; for example, ExactMatch.



Step 4 In the **ActiveSheet** field, enter the name of the sheet within the Excel spreadsheet that contains the sensor mapping. The default is **Test**.

Step 5 If you want to force the enhanced parser to update the sensor map and its group association when changes are applied to the sensor's group association, check the **AlwaysRegenerateMap** option. This enables operators to dynamically add or change sensor groupings from PSOM Administration Console.

Note If the changes are made to existing sensors, existing associations must be removed from the Administration Console; otherwise, changes will not be made for existing sensors.

If you do not check the **AlwaysRegenerateMap** option, the enhanced parser will generate the sensor map the first time the enhanced parser is executed, and then continue to use this sensor map association until a new version of PSOM is installed.

Step 6 Select the pattern match scheme(s) you want to use from the **ParserMatch** area. When more than one type of scheme is selected, the parser will first perform an exact match, then a partial match, then a remainder match. If no match scheme(s) are selected, then all sensors will be grouped to undesignated area, location and zone as if the default parser was applied.

- **Exact Match**—The entire sensor name or description, as provided in the Excel spreadsheet, must be matched to the sensor pattern. Case is ignored unless the **Case Sensitive** option is checked. Matching the sensor patterns listed below has these results when compared to the Excel spreadsheet sample shown earlier in this appendix.

Sensor Pattern	match selection	location name	area name	zone name
T2WP32B into Secured Area	ExactMatch	Secured Area	Area2	zone1
T2WP31	ExactMatch	Cafeteria	Area3	zone1
T2WF21	ExactMatch	Door1	Area4	zone1

- **Partial Match**—A portion of the sensor name must be identified for a match. You can use a wildcard search to match a string to the beginning, end, or substring of the sensor name. Case is ignored unless the **Case Sensitive** option is checked.
  - **Begin**—Matches a sensor name that begins with the pattern string which includes the wildcard "*" at the end; for example, "PXT2*".
  - **Substring**—Matches a sensor name that includes the pattern string surrounded by the wildcard "*"; for example, "*W2*".
  - **End**—Matches a sensor name that ends with the pattern string which includes the wildcard "*" at the beginning; for example, "*abc".

  Matching the sensor patterns listed below has the following results when compared to the Excel spreadsheet sample shown earlier in this appendix.

Sensor Pattern	match selection	location name	area name	zone name
PXT2*	PartialMatch	PXT2s	Area6	zone1
W2	PartialMatch	All with mid string W2	Area7	zone1
*abc	PartialMatch	All with mid string W2	Area7	zone1

Note Empty rows and empty fields are not allowed with Partial Match.

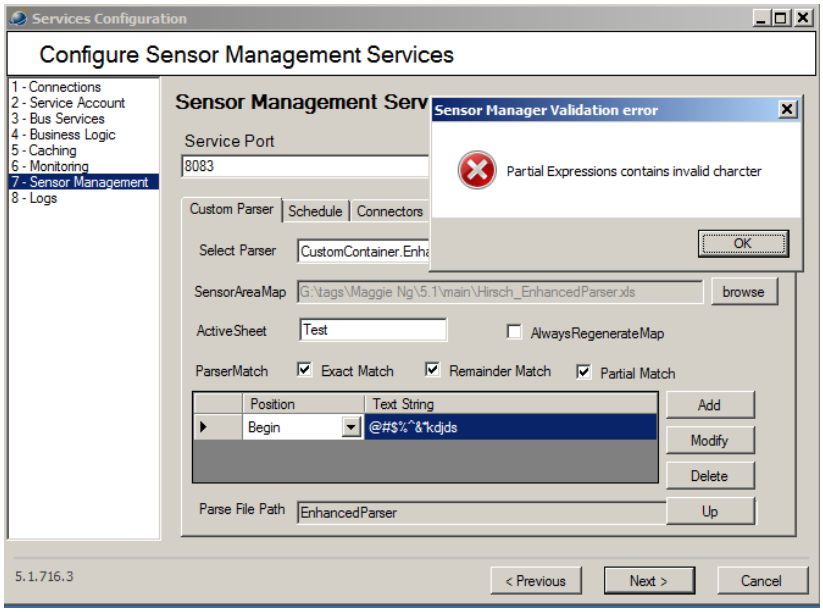
Case will be ignored when matching pattern strings unless the **Case Sensitive** option is checked.

- **Remainder Match**—All the unmatched sensors are associated with a designated group by using a sensor pattern of "*" which indicates that any remaining pattern is a match. Matching the sensor patterns listed below has the following results when compared to the Excel spreadsheet shown earlier in this appendix.

Sensor Pattern to be matched	match selection	location name	area name	zone name
*	RemainderMatch	undecided	Area9	zone1

Note The following characters are treated as illegal characters in the sensor name, and are not allowed for pattern matching:

"\", "/", ":", "*", "?", "<", ">", "|", "!", "@", "#", "$", "%", "^", "&", "(", ")", "~", "[", "]", "{", "}", ";", "`", """



Step 7 If you want matching to consider the case used in pattern matching strings, check the **Case Sensitive** option. If unchecked, the case in the pattern to be matched is ignored.

Changing the Configuration of the PSOM Web Service

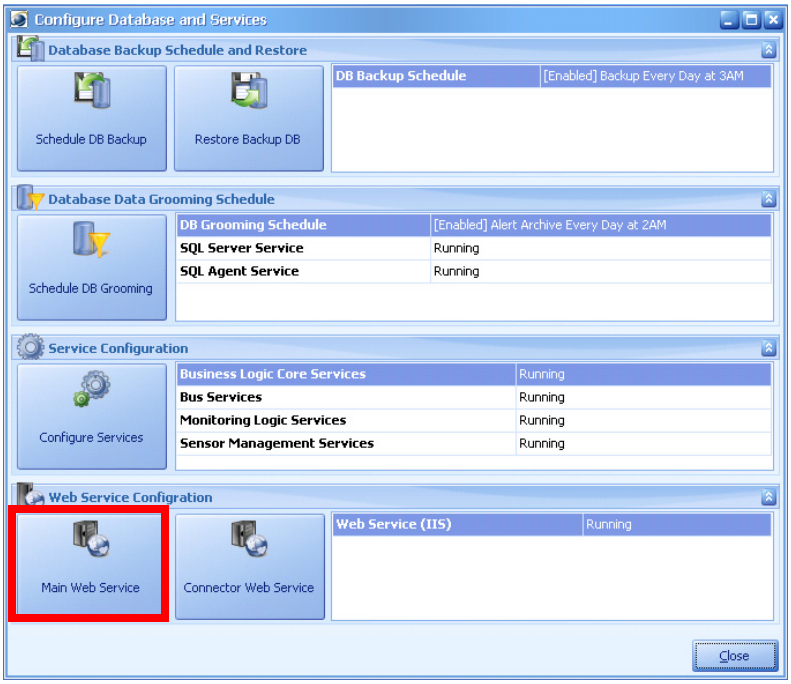
To change the configuration for PSOM Web Service:

Step 1 From the PSOM Administration Console, select **Tools** in the **Navigation** pane

Step 2 Click **Configure DB and Services**.

Step 3 Click **Yes** to log off PSOM temporarily while you configure the services.

Step 4 Click **Main Web Service**.



The Database Connection window appears.

Step 5 Enter the name of the SQL Server that is hosting the PSOM Repository in the **Enter name of the SQL Server for Web Service** field. Normally this is the local machine name unless the PSOM Repository is located on a different server.

Step 6 If you are using a mirrored database, enter the name of the mirrored SQL Server in the **Mirror SQL Server name** field. Otherwise, leave this field blank.

Step 7 Leave the value of the **Enter database name for Web Service** field set to ProximexDb unless you have customized the name of the PSOM Repository.

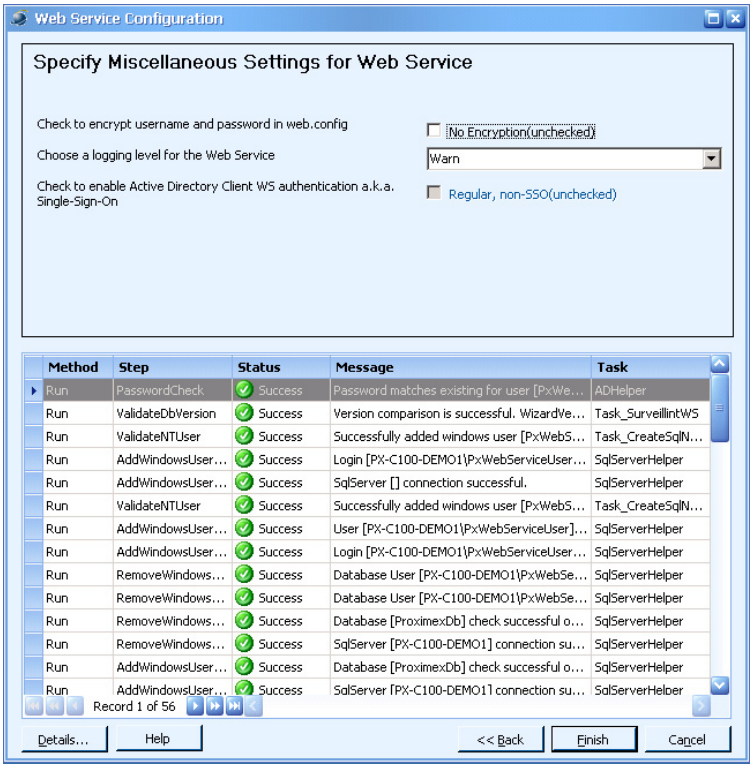
Step 8 If you are using a domain Windows user for the connection to PSOM Repository, select the **Check to create Domain User** option. Otherwise, leave this option unchecked to use a local Windows user for access to the Repository.

Note If you do not have permission to create a local or domain Windows user, this step will fail. You must then create the user account manually and re-run this wizard.

Step 9 Enter the name of the local or domain Windows user to be used for accessing PSOM Repository in the **Name of windows user for database connection** field. Do not include the domain name or machine name. The default value is PxWebServiceUser.

Step 10 In the **Enter the password for the user specified for update** field, enter the corresponding password.

Step 11 Click **Next**. The following window appears.



Step 12 Normally, the username and password for the PSOM Repository is stored in the web.config file located in the root directory of PSOM Web Service. To store the encrypted password for PSOM Repository in the Registry, select the **Check to encrypt username and password in web.config** option.

Note Decryption is not possible; therefore, if this option is checked, you will need to update the username and password if you re-run Web Service configuration.

Step 13 Select the desired level of logging for the PSOM Web Service from the **Choose a logging level for the Web Service** field. Choices include: **Debug**, **Info**, **Warn**, **Error**, or **Fatal**.

Step 14 If you want to use Active Directory for user authentication, select the **Check to enable Active Directory Client WS authentication** option. By default, Active Directory is not used for user authentication by PSOM or the Web Service. See <Link>**Single Sign On and User Management** on page 47 for information on enabling single sign on and Active Director user authentication in PSOM.

Step 15 Click **Finish**, click **OK** when prompted, and click **Close** at the final screen.

Changing the Configuration of the Connector Web Service

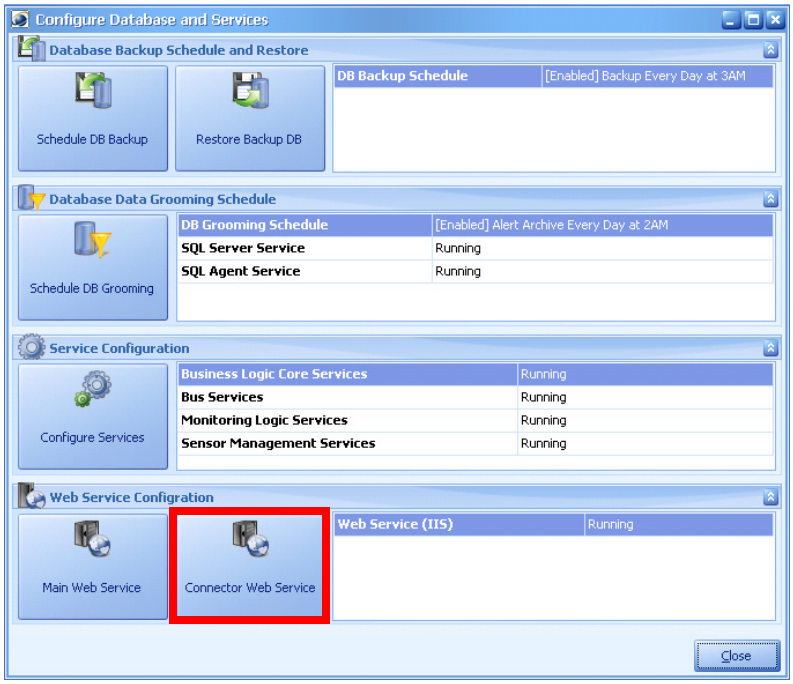
To change the configuration for the Connector Web Service:

Step 1 From the PSOM Administration Console, select **Tools** in the **Navigation** pane

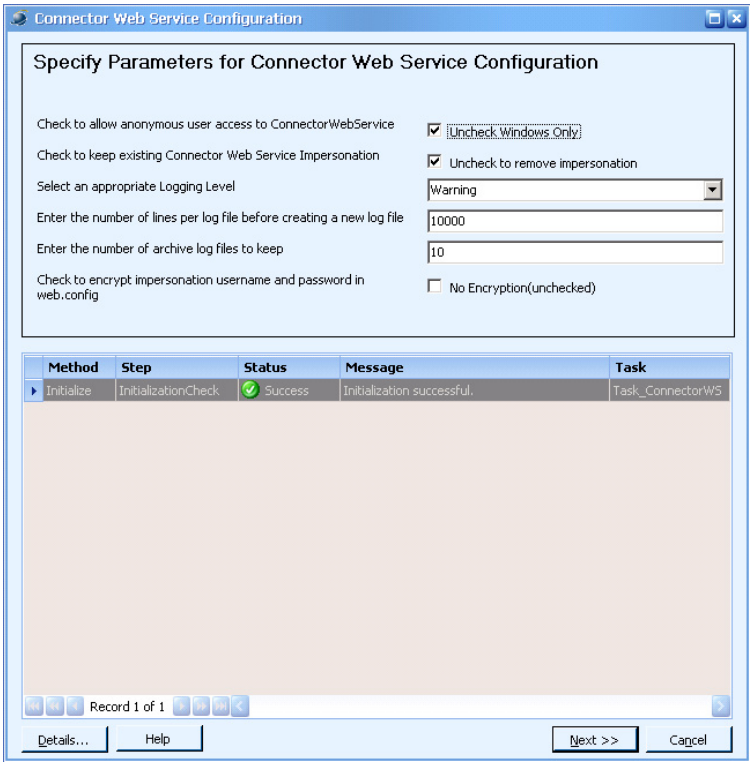
Step 2 Click **Configure DB and Services**.

Step 3 Click **Yes** to log off PSOM temporarily while you configure the services.

Step 4 Click **Connector Web Service**.



The Connector Web Service Configuration window appears.



Step 5 Leave the **Check to allow anonymous user access to ConnectorWebService** option selected unless PSOM Managed Services are running under a Windows context.

Step 6 Leave the **Check to keep existing Web Service Impersonation setting** selected unless you want to remove impersonation. If impersonation is removed, some PSOM Integration Modules will need to be reinitialized.

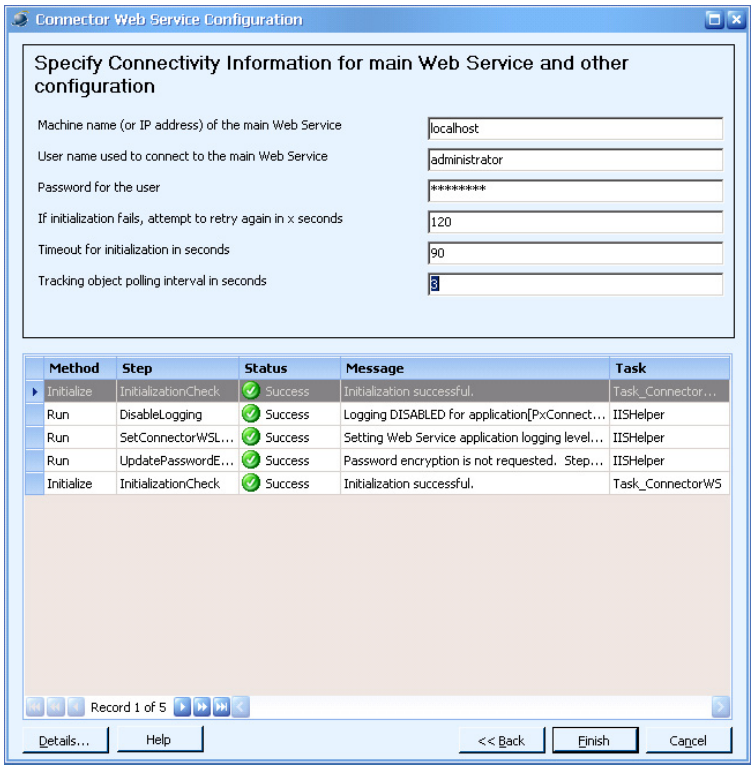
Step 7 Select the types of messages that should be logged by the Connector Web Service from the **Select an appropriate Logging Level** field.

Step 8 In the **Enter the number of lines per log file before creating a new log file** field, enter the maximum number of lines that can be written to a log file before a new log file is created.

Step 9 In the **Enter the number of archive log files to keep** field, enter the maximum number of log files that can be saved before the oldest log file is removed.

Step 10 If a PSOM Integration Module uses impersonation, the impersonation information is stored in the **web.config** file in plain text. You can encrypt the password and store it in the Registry by selecting the **Check to encrypt impersonation username and password in web.config** option.

Step 11 Click **Next**. The following screen appears.



Step 12 Enter the server name or IP address of the machine where PSOM Web Service is installed in the **Machine name (or IP address) of the main Web Service** field.

Note PSOM Web Service must be installed before the Connector Web Service installation is performed.

Step 13 Enter the username for connecting to PSOM Web Service in the **User name used to connect to the main Web Service** field. Administrator is the default.

Step 14 Enter the password for connecting to PSOM Web Service in the **Password for the user** field. The default password is provided.

Step 15 Enter the number of seconds the Connector Web Service should wait before reattempting to initialize an Integration Module in the **If initialization fails, attempt to retry again in x seconds** field. If initialization fails, PSOM creates an alert against the application sensor for the failed instance.

Step 16 Enter the number of seconds the Connector Web Service should wait for an Integration Module to complete initialization in the **Timeout for initialization in seconds** field.

Step 17 Enter the number of seconds that Integration Modules should wait between requests for tracking trail information in the **Tracking object polling interval in seconds** field. This field only pertains to Integration Modules that convey tracking trail information to external 3rd party systems.

Step 18 Click **Finish**. Click **OK** when prompted, then **Close** to complete configuration.

Reconfiguring Settings for PSOM User Services

You can change the configuration of PSOM User Services after the initial deployment of PSOM.

Note You must be a member of the local *Administrators* group to launch **Services Configuration**.

To reconfigure PSOM User Services:

Step 1 From the **Start** menu, select **All Programs > Cisco Physical Security Operations Manager > User Services Configuration**.

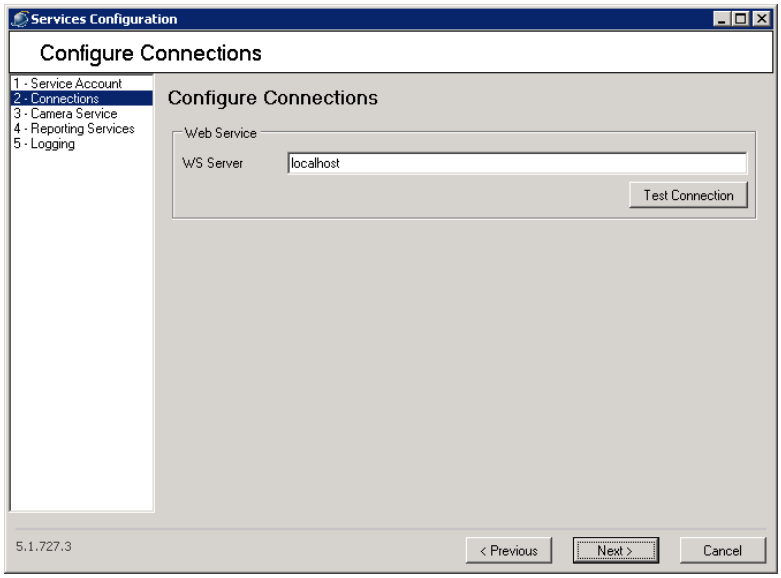
The **Services Configuration** window appears with **Configure Service Account** selected.

Step 2 If you decide to use a dedicated Windows account to automatically launch PSOM User Services when the system starts, check the **Use the following local service account for user services and auto logon upon system reboots** option. Enter a valid user name and password in the fields provided. When the system reboots, PSOM User Services will automatically login to the specified service account and lock the system to prevent unauthorized access.

Note By default the user account is PXUSERSERVICEUSER and the password is Pa$$w0rd123.

If the user account you provide does not exist, a new local account will automatically be created.

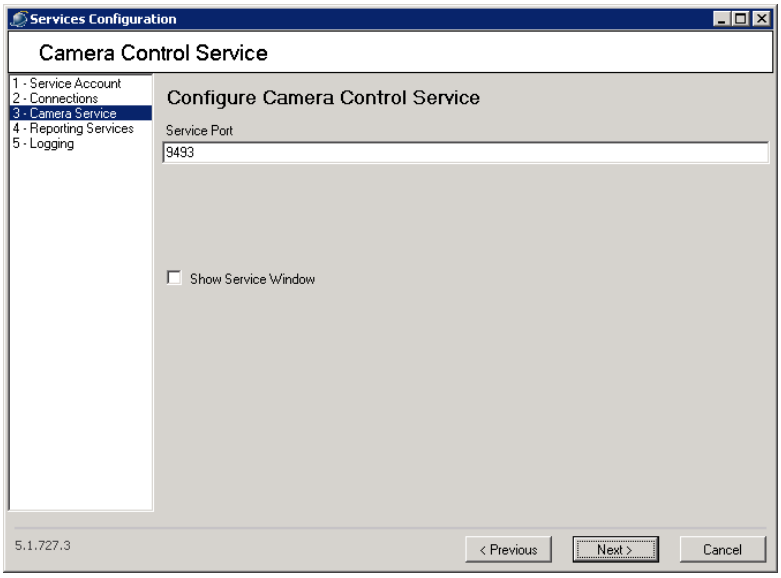
Step 3 Click **Next** or **2 – Connections**.



Step 4 The **WS Server** field contains **localhost** unless you installed PSOM Web Service on a different machine in the network. In this case, enter the IP address or server name of the machine where you installed PSOM Web Service.

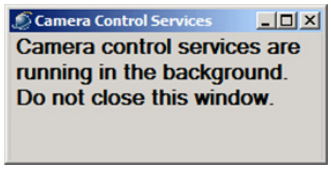
Click **Test Connection** to verify settings.

Step 5 Click **Next** or select **3 - Camera Service** on the left side of the window.



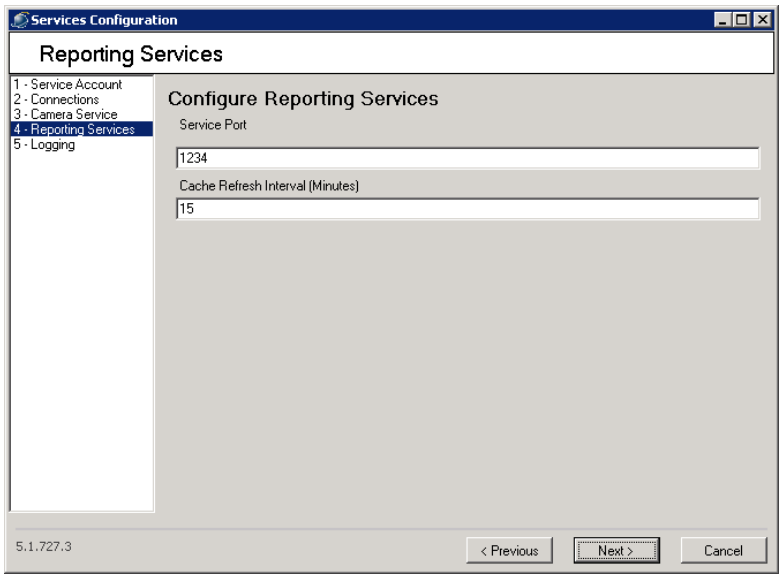
Step 6 The **Service Port** shows the port number under which the Camera Control Service will run by default. Only change this value if you need this service to run under a different port number.

Step 7 Uncheck the **Show Service window** option if you do not want the Camera Control Service to display the following window while it is running.



Note Do not close the Camera Control Services window while the service is running.

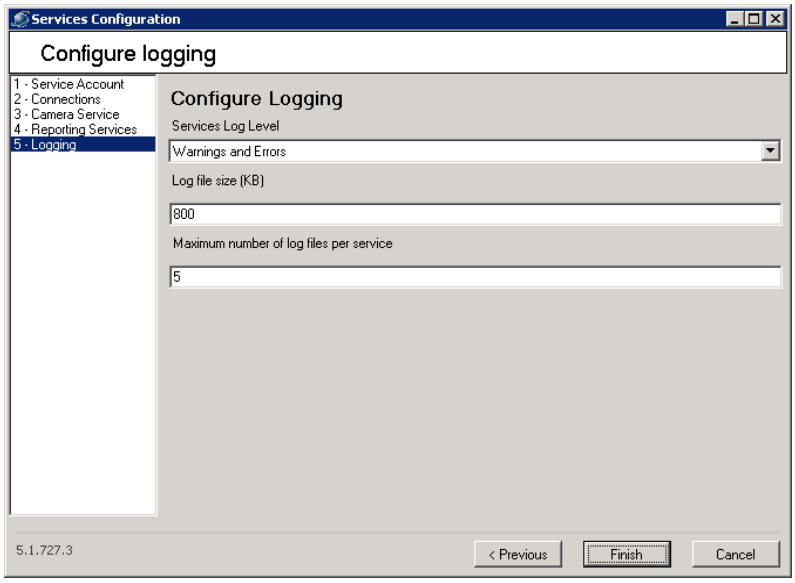
Step 8 Click **Next** or select **4 - Reporting Services** on the left side of the window.



Step 9 The **Service Port** shows the port number under which the Reporting Services will run by default. Only change this value if you need this service to run under a different port number.

Step 10 In the **Cache Refresh Interval (Minutes)** field, enter how often the Reporting Services will refresh its cache of sensor and monitoring hierarchy information. Caching is done to improve performance with regards to reporting.

Step 11 Click **Next** or select **5 - Logging** on the left side of the window.



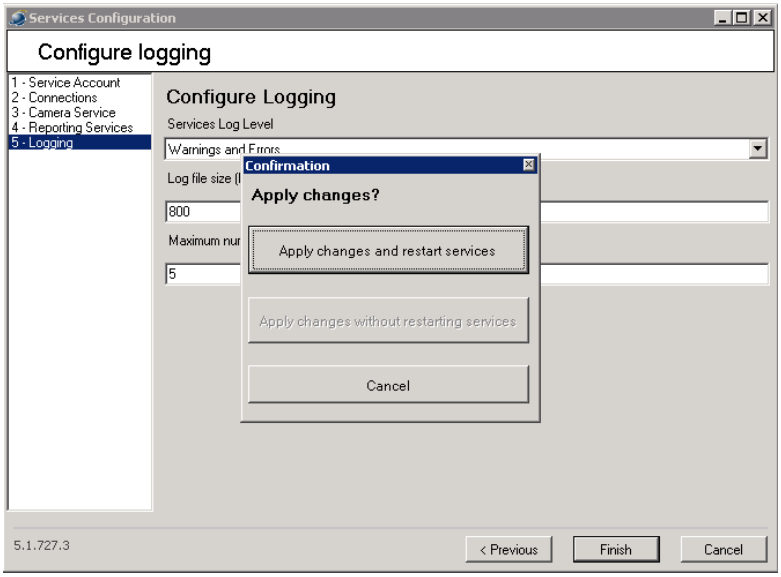
Step 12 From the **Services Log Level** field select the level of messages that should be retained in the log. Choices include: **Everything**, **Informational**, **Warnings and Errors**, and **Errors Only**.

Step 13 In the **Log file size** field, enter the maximum size (in kilobytes) that you want to allow for each log file generated by PSOM Services.

Note By default all log files generated by Surveillint Services are located in **\Program Files\Cisco PSOM\Managed Services\Log**.

Step 14 In the **Max number of log files per service** field, enter the maximum number of log files that can be generated by each PSOM Service. The default is 5.

Step 15 Click **Finish**.



Step 16 At the prompt that appears, click **Apply changes and restart services**.

Step 17 Click **Finish**.

GLOSSARY

A

Access control device — A door that is secured with a card reader as part of an access control system.

Access control system — An intrusion detection system such as Hirsch Velocity that monitors sensors at access control devices (such as doors or elevators)

Alarm — The event raised by an intrusion detection system such as Hirsch Velocity which indicates an inappropriate behavior has occurred at a sensor device.

Alert — The event raised within PSOM when a coordinating intrusion detection system raises an alarm at a sensor.

Attach — To include an image as part of an alert description such that people viewing the alert will be able to see the image.

AVI file — Audio Video Interleave. An audio-video standard designed by Microsoft

C

Client — The PSOM client application is the part of PSOM that runs locally, on the computer that you have on your desk. It interacts with several PSOM servers, which run on other computers linked to yours over a network.

Compression — When a file is stored differently such that it has a smaller file size, and potentially transmits across the Internet more quickly.

D

Database — The database holds all the information on which PSOM operates, including alert details, recorded video, snapshots and notes.

Database server — The server-side application responsible for interactions between the PSOM client and the set of data from which it draws.

Docked window — A window that is integrated within the overall PSOM software windows.

Dossier The set of information stored about an alert including its description, notes, recorded video, and snapshots.

DVR Digital Video Recorder. Electronic equipment that captures video from video cameras and stores it to a database.

E

Export To take information and transform it so it can be viewed in other ways. For example, to change a Word document so it can be viewed within Adobe Acrobat Reader by *exporting* the document to PDF format.

F

Footage A stream of video captured by a video camera.

I

Intrusion detection system Computer software such as Hirsch Velocity that monitors sensors at access control devices (such as doors or elevators).

L

live video Video footage that is happening in real time; it has not been recorded at an earlier time.

M

Monitoring area A physical location in which a collection of sensors are used in tandem to observe activity.

P

Pan To move the angle of a video camera so that it displays a different view of a physical location.

Pane A part of a window.

PTZ Pan-tilt-zoom. A video camera for which users can remotely control the view using pan, tilt, and zoom operations.

R

Recorded video Video footage that has been saved to a DVR database.

S

Security zone A logical group of monitoring areas within your total security boundary.

Sensor An electronic device that responds to certain stimulus (as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse. PSOM works with video camera sensors and access control sensors.

Snapshot A still frame captured from a video. A photograph.

Standalone window A window that is not integrated within the overall PSOM window.

T

Thumbnail A very small visual representation of a larger image.

U

Undocked window A window that has been removed from the overall PSOM window to become a standalone window.

V

Video feed The stream of visual images transmitted by a video camera.

Z

Zoom To make part of an image larger (zoom in) or smaller (zoom out).

INDEX

A

access control devices
- adding sensor for 6-2 to 6-6
- connecting to 6-2, 6-5
- icon 7-22
- integration planning A-2
- location, associating with 6-5
- placing on map 7-21 to 7-24

Access Control Service
- starting 1-25

action rule
- command-line arguments for 14-51, 14-57, 14-59

adding
- locations 4-2 to 4-3
- monitoring areas 5-2, 5-6
- monitoring zones 5-6 to 5-10
- response task items 8-3 to 8-7
- response workflow rules 8-9 to 8-13
- sensors
  - access control devices 6-2 to 6-6
  - video cameras 6-7 to 6-12
- user accounts 2-2 to 2-4
- user groups 2-12 to 2-15
- video cameras to PSOM 3-1 to 3-2

Administration Console, overview 1-10 to 1-13

administration tasks
- overview 1-6
- user accounts 2-1

administrative alerts, diagnosing 16-1 to 16-3

administrative reports
- Alert Count Daily Report 10-1
- Alert Count Hourly Report 10-1
- Alert Detail Report 10-1
- Alert Response Time by Alert Type Report 10-1
- customizing default 10-2 to 10-8, 13-1
- Operator Alert Count Report 10-2
- Operator Alert Response Time Report 10-2
- Top X Alert Response Time Report 10-2
- Top X Alerts by Alert Type Report 10-2
- Top X Alerts by Area Report 10-2
- Top X Alerts by Sensor Report 10-2
- types of 10-1 to 10-2, 13-5

administrators, defined 2-1

alarms, third-party integration 11-6 to 11-10
- deleting alert types 11-10 to 11-11
- modifying alert types 11-10 to 11-11

Alert Count Daily Report 10-1

Alert Count Hourly Report 10-1

Alert Detail Report 10-1

Alert List Pane, what is 1-4

Alert Response Time by Alert Type Report 10-1

architecture of PSOM 1-2

attachment, defined 1-1

B

background image for map, adding 7-5 to 7-6

backup PSOM database
- manually performing B-3 to B-5
- scheduled B-1, C-1, C-22

C

client, defined 1-1

customizing default reports 10-2 to 10-8, 13-1

alert types to include 10-5
chart type to use 10-7
deleting 10-9
modifying 10-8
monitoring areas to include 10-6
monitoring zones to include 10-6
sensors to include 10-6
severity levels to include 10-5
time period for reporting 10-6

D

database, defined 1-1
database for PSOM
backup manually B-3 to B-5
restoring B-5 to B-7
scheduled backups B-1, C-1, C-22
database server, defined 1-1
deleting
custom reports 10-9
locations 4-5 to 4-6
monitoring areas 5-23
monitoring zones 5-26
registered alert types 11-10 to 11-11
response task items 8-8
response workflow rules 8-15
sensor groups 6-29, 6-35
sensor mappings 11-5
user groups 2-19 to 2-20
users 2-7 to 2-8
deploying PSOM
architecture 1-2
locations, planning 4-1
monitoring areas and zones, planning 5-2
monitoring services 1-2
planning 1-6 to 1-10
sensor integration, planning 6-2
user accounts, planning 2-2
diagnosing problems
administrative alerts 16-1 to 16-3
monitoring alerts 16-3 to 16-5
display options for maps, setting 7-14 to 7-15
dock window 1-13

E

editing
custom reports 10-8 to 10-9
locations 4-3
monitoring areas 5-20 to 5-23
monitoring zones 5-23 to 5-24
passwords for users 2-6
registered alert types 11-10 to 11-11
response task items 8-7 to 8-8
response workflow rules 8-14
sensor groups 6-27, 6-33
sensor mappings 11-5 to 11-6
user groups 2-15 to 2-17
user names 2-6
external alarms, registering with PSOM 11-6, 11-6 to 11-10
deleting alert types 11-10 to 11-11
modifying alert types 11-10 to 11-11
external application, launching upon alert
command-line arguments 14-51, 14-57, 14-59
external intrusion detection system, integrating with 11-1
EZ-Track
Add Link icon 12-16
base camera view, changing 12-18
batch configuration 12-20 to 12-22
exporting from PSOM 12-22 to 12-23
uploading XML file 12-21 to 12-22
XML syntax 12-20 to 12-21
Browse Back icon 12-16
Browse To icon 12-16
camera topology, configuring 12-11 to 12-16
configuring 12-3 to 12-18
Delete Link icon 12-16
Edit Link icon 12-16

how used by operators 12-1
link
adding 12-12, 12-16
deleting 12-17
editing 12-17
region links, viewing 12-18
live video for sensor, viewing 12-16
Live Video icon 12-16
map
sensor names, showing 12-16
sensors, showing 12-16
planning worksheets A-10
PTZ cameras with 12-3
sensor
name, displaying 12-7 to 12-10
range, displaying 12-7 to 12-10
Show Links icon 12-16
snapshot 'field of view' images 12-3 to 12-5
stationary cameras with 12-3
testing a configuration 12-18 to 12-19
video cameras
view direction configuring 12-6 to 12-7
view distance, configuring 12-6 to 12-7
view range, configuring 12-6 to 12-7
what it does 12-1
XML configuration 12-20 to 12-22
exporting from PSOM 12-22 to 12-23
syntax 12-20 to 12-21
uploading 12-21 to 12-22

F

field of view for camera, adding 6-11
FOV for camera, adding 6-11

G

group, user
creating 2-12 to 2-15
deleting 2-19 to 2-20
editing 2-15 to 2-17
members, managing 2-17 to 2-19

H

Hazard detector devices
adding sensors for 6-16 to 6-20
Homeland Security levels, setting 1-17

I

infrared cameras icon 7-22
integrating with third-party alarm sources 11-6 to 11-10

K

Knowledge Service
defined 1-2
starting 1-25

L

locations
adding 4-2 to 4-3
defined 4-1
deleting 4-5 to 4-6
editing 4-3 to 4-5
logs stored by PSOM 16-1

M

maps, designing
background image, adding 7-5 to 7-6
deleting icons from map 7-29
display options, setting 7-14 to 7-15
editing items on map 7-29

Map Design Mode, starting 7-1 to 7-4
monitoring area, drawing on map 7-18 to 7-20
monitoring zone, drawing on map 7-16 to 7-18
navigation, adding 7-24 to 7-27
origin coordinates, setting 7-6 to 7-8
scale, setting 7-6 to 7-8
sensor name, showing 7-15, 12-10
sensor range, showing 7-15, 12-10
sensors, placing on map 7-21 to 7-24
tools for 7-4
URL links, adding 7-27 to 7-29
Map View Pane, what is 1-4
MARSEC levels, setting 1-17
monitoring alerts, diagnosing 16-3 to 16-5
monitoring area
adding 5-2, 5-6, 5-14
defined 5-1
deleting 5-23
deleting from map 7-20
drawing on map 7-18 to 7-20
editing 5-20 to 5-23
monitoring tree, adding to 5-16
monitoring zone, adding to 5-8
planning A-7
showing on map 7-15
monitoring environment, setting up
locations 4-2 to 4-3
maps, designing 7-1 to 7-30
monitoring areas, adding 5-2, 5-6
monitoring tree, setting up 5-16
monitoring zones, adding 5-6 to 5-10
sensors, access control 6-2 to 6-6
sensors, video cameras 6-7 to 6-12
monitoring rule
applied to monitoring areas 9-7, 14-49
Monitoring Service
starting 1-25
monitoring services
defined 1-2
starting and stopping 1-25
monitoring tree
adding
monitoring area 5-16
monitoring zone 5-10 to 5-13
node properties, viewing 5-17
setting up 5-16
monitoring zone
adding 5-6, 5-6 to 5-10
adding maps, monitoring area 5-19
adding multiple levels 5-13
defined 5-1
deleting 5-23, 5-26
deleting from map 7-20
drawing on map 7-16 to 7-18
editing 5-23, 5-23 to 5-24
members, adding 5-8
monitoring tree, adding to 5-10
planning A-6
showing on map 7-15

N

navigation
adding to maps 7-24 to 7-27
setting up 5-16
Navigation Pane, what is 1-4

O

Operation Console
overview 1-3 to 1-6
Operator Alert Count Report 10-2
Operator Alert Response Time Report 10-2
operators, defined 2-1
origin coordinates for map, setting 7-6 to 7-8
overview of Administration Console 1-10 to 1-13
overview of Operation Console 1-3 to 1-6

P

password, changing 2-5
physical spaces in PSOM, setting up 4-1
planning
  access control system integration A-2
  EZ-Track configuration A-10
  monitoring areas A-7
  monitoring zones A-6
  response tasks rules A-9
  task items A-8
  user accounts A-3
  video camera settings A-5
PSOM Server
  database
    backing up manually B-3 to B-5
    restoring B-5 to B-7
    scheduled backups B-1, C-1, C-22
  defined 1-2
PSOM UI
  defined 1-2
PTZ cameras
  EZ-Track, using with 12-3
  icon 7-22

R

range angle for camera, adding 6-11
range distance for camera, adding 6-11
registering third-party alarms 11-6 to 11-10
  deleting alert types 11-10 to 11-11
  modifying alert types 11-10 to 11-11
removing user accounts 2-7 to 2-8
reports
  Alert Count Daily Report 10-1
  Alert Count Hourly Report 10-1
  Alert Detail Report 10-1
  Alert Response Time by Alert Type Report 10-1
  customizing default 10-2 to 10-8, 13-1
    alert types to include 10-5
    chart type to use 10-7
    deleting 10-9
    modifying 10-8
    monitoring areas to include 10-6
    monitoring zones to include 10-6
    sensors to include 10-6
    severity levels to include 10-5
    time period for reporting 10-6
  Operator Alert Count Report 10-2
  Operator Alert Response Time Report 10-2
  Top X Alert Response Time Report 10-2
  Top X Alerts by Alert Type Report 10-2
  Top X Alerts by Area Report 10-2
  Top X Alerts by Sensor Report 10-2
  types of 10-1 to 10-2, 13-5
response task items
  adding new 8-3 to 8-7
  alert acknowledgeable 8-5
  alert closeable 8-5
  deleting 8-8 to 8-9
  in Operation Console 8-1
  modifying 8-7 to 8-8
  sub-task checklist items 8-6
  what are 8-1
response tasks rules
  planning A-9
Response Workflow Pane in Operation Console 8-1
response workflow rules
  adding new 8-9 to 8-13
  alert closeable task, must have one 8-13
  applying by alert type 8-15 to 8-19
  deleting 8-15
  help, URL to provide 8-12
  in Operation Console 8-1
  modifying 8-14
  response task items, adding first 8-3
  what are 8-1, 8-9
restore PSOM database B-5 to B-7

S

scale for map, setting 7-6 to 7-8
sensor group
  Access Control/Camera Group, defined 6-24
  adding 6-24, 6-30
  deleting 6-29 to 6-30, 6-35
  editing 6-27 to 6-28, 6-33 to 6-34
  monitoring area, adding to 5-5
sensor mapping, defined 11-1
sensors
  access control devices, adding 6-2 to 6-6
  connecting to 6-2, 6-5, 6-9
  connecting to access control devices 6-2
  displaying icons on map 7-15, 12-10
  grouping 6-24
  location, associating with 6-5, 6-10
  mapping
    creating new 11-2 to 11-4
    defined 11-1
    deleting 11-6
    editing 11-5 to 11-6
  monitoring area, adding to 5-5
  name, showing on map 7-15, 12-10
  placing on maps 7-21 to 7-24
  planning integration 6-2
  types of 6-1
  video cameras
    adding 6-7 to 6-12
    field of view, adding 6-11
    range angle, adding 6-11
    range distance, adding 6-11
    sensor range, showing on maps 7-15, 12-10
    view direction, adding 12-7
    view distance, adding 12-7
    view orientation, adding 6-11
    view range, adding 12-7
starting monitoring services 1-25
stationary cameras icon 7-22
stopping monitoring services 1-25
suspects, following with EZ-Track 12-1
system alert type, creating 11-15

T

task items
  planning A-8
tasks, administration 1-6
  tools to use 1-11
third-party alarms, registering with PSOM 11-6, 11-6 to 11-10
  deleting alert types 11-10 to 11-11
  modifying alert types 11-10 to 11-11
topology for EZ-Track, configuring 12-11 to 12-16
Top X Alert Response Time Report 10-2
Top X Alerts by Alert Type Report 10-2
Top X Alerts by Area Report 10-2
Top X Alerts by Sensor Report 10-2
tracking suspects with EZ-Track 12-1
troubleshooting
  administrative alerts 16-1 to 16-3
  monitoring alerts 16-3 to 16-5

U

undock window 1-13
URL links, adding to maps 7-27 to 7-29
user accounts
  adding 2-2 to 2-4
  administering 2-1
  deployment planning 2-2
  monitoring zone, privileges to 5-9
  name, cannot change 2-6
  password, changing 2-5
  planning A-3
  removing 2-7 to 2-8
user group
  creating 2-12 to 2-15

deleting 2-19 to 2-20
editing 2-15 to 2-17
members, managing 2-17 to 2-19
user roles, types of 2-1

V

video cameras
adding sensor for 6-7 to 6-12
adding to PSOM 3-1 to 3-2
connecting to 6-2, 6-9
EZ-Track, configuring for 12-3 to 12-7
field of view, adding 6-11
integrating with PSOM 3-1 to 3-4
location, associating with 6-10
placing on map 7-21 to 7-24
range angle, adding 6-11
range distance, adding 6-11
sensor range, showing on maps 7-15, 12-10
suspects, following with EZ-Track 12-1
topology for EZ-Track, configuring 12-11 to 12-16
view direction, adding 12-7
view distance, adding 12-7
view orientation, adding 6-11
view range, adding 12-7
Video Control Services Database
starting 1-25
view direction for camera, adding 12-7
view distance for camera, adding 12-7
view orientation for camera, adding 6-11
view range for camera, adding 12-7

W

worksheets
access control system integration A-2
EZ-Track planning A-10
monitoring areas planning A-7
monitoring zones planning A-6
response tasks rules planning A-9
task items planning A-8
user accounts A-3
video camera view settings A-5