Cisco Urban Security Design Guide

Last Updated: June 2, 2010

Cisco Validated Design

Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

© 2010 Cisco Systems, Inc. All rights reserved

Solution Authors

John Carney

John Carney, Senior Manager, CMO ESE, Cisco Systems

John is a senior manager responsible for leading the definition of safety and security architectures on the Industry Solutions Engineering team. He joined Cisco in January of 2007 and has served as the Industry Solution Architect responsible for the Healthcare, Financial Services, and Public Sector verticals.

With over 25 years experience working in a service provider/data center environment, John's strength lies in his unique ability to understand the business issues facing our customers and how they relate to the components in a large computing environment. During his career, John has obtained various industry certifications, including Novell's Certified Network Engineer, Microsoft's Certified Systems Engineer and various levels of Citrix certifications.

Fernando Macias

Fernando Macias, CCIE#11777, Vertical Solutions Architect, CMO ESE, Cisco Systems

Fernando is a member of the Industry Solutions group at Cisco. As a Solutions Architect within the Enterprise Solutions Engineering (ESE), he is responsible for developing networking solutions that impact the Public Sector industry. With ten years of experience at Cisco, Fernando has developed networking solutions for Cisco's Physical Security Business Unit and was a member of Advanced Services, where he provided network design support to large customers, including Fortune 50 companies. Fernando was also a Systems Engineer for Cisco's commercial region.

With over 20 years of networking experience, Fernando has also worked for international manufacturing and construction engineering companies. In addition to Masters degrees in Technology Management and Software Engineering, Fernando holds a CCIE#11777 certification in Routing and Switching.

Jenny Cai

Jenny Cai, Vertical Solutions Architect, CMO ESE, Cisco Systems

Jenny currently works with the Industry Solutions Engineering team and is responsible for developing and validating education solutions. Since joining the team, she also worked on validating solutions for the Financial Services vertical. Prior to this group, Jenny worked on the Cisco 7600 series router.

Prior to Cisco, Jenny worked on a fault-tolerant server for the Financial Services industry while at Stratus Computer, and a continuous-feed printer for the oil industry while at Atlantek.

CONTENTS

CHAPTER 1

Overview

Executive Summary

In large and complex urban environments, it is critical for decision makers to reduce the time from detection of an incident to response by first responders. Additionally, it is very important that the information collected by the system supports the human operators in making key decisions and building confidence in those decisions. Finally, the system must allow for the dissemination of the right information (whether audio, video, pictures, and so on) to the right people at the right time. Cisco's use of the network to integrate various technologies and provide vital information in seconds to decision makers is key to the solution presented.

This solution shows how the integration of multiple sensors, video, computer command-and-control, and communications greatly aid in decision making and in reducing the time to send responders to the scene of a crisis. In addition to reducing time, this solution demonstrates how integrating these technologies across the network permits better situational awareness and command-and-control in a complex environment.

Solution Description

The Cisco Urban Security solution focuses on the products that are integrated into a solution and the services necessary to create a deployment for everyday operations that scale to support environments and their crisis situations. The scope of this solution's testing focuses on the functional interaction between the products tested and includes the actions and reactions necessary to properly monitor, interact, and respond to any situation. Specific use cases have been tested to show the capabilities of the products, components, and systems that have been included.

The focus areas of the solution include command-and control, sensing and actuation, and citizen-authority interaction. More information is available on these functions in Chapter 2, "Architecture Framework." Tying all of the products together to address these key elements of a large scale deployment is shown in Chapter 4, "Designing the Solution."

This is not a blueprint for how to deploy a large-scale safety and security implementation. Rather, this document shows the interaction between the components, explains how to accomplish the integration between components, and provides the direction that enables a successful deployment into an existing security environment.

Solution Benefits

If not properly planned, urban global growth patterns strain city services well beyond breaking point. As urban populations continue to grow at the expected rates, it is implausible to expect security services to scale commensurately without leveraging technological advances and innovations. This is especially true for Africa and Asia where the population growth rates are the highest. The specter of global terrorism exacerbates this problem because densely populated centers make ideal targets for exploitation, destruction, and disruption.

There is also a growing dependence on privately-owned (often government-regulated) infrastructures that are managed within, or are adjacent to, urban boundaries. Examples of this include petrochemical processing/distribution centers, seaports, harbors, and airports, as well as major stock exchanges and bourses. This interdependence stipulates that urban security designs should maintain an open architecture for assimilating outside data and sharing situational awareness among constituent groups.

The benefits of this approach include the following:

- More comprehensive awareness of emergency situations
- Faster retasking of critical resources and better coordination of inter-organizational response efforts
- Capability to easily link private and public security systems together, sharing response talk groups but also sharing important rich media such as videos, pictures, and maps
- Leveraging existing investments to provide a system that is more resilient, more adaptable, and better able to respond to the diverse threat environment
- Transforming Unified Communications to a mass notification system, supporting full response tracking for management of notification and awareness, covering response teams, stakeholders, and mass populace
- Interoperability with facility-based mass notification systems
- Interoperability with ubiquitous social networks and Web 2.0 capabilities
- Introducing personnel accountability capabilities, ensuring personnel are accounted for during emergency situations
- Interoperability with crowd-sourced (public-originated) events and public event sources
- Better capability for expansion and adaptability over time

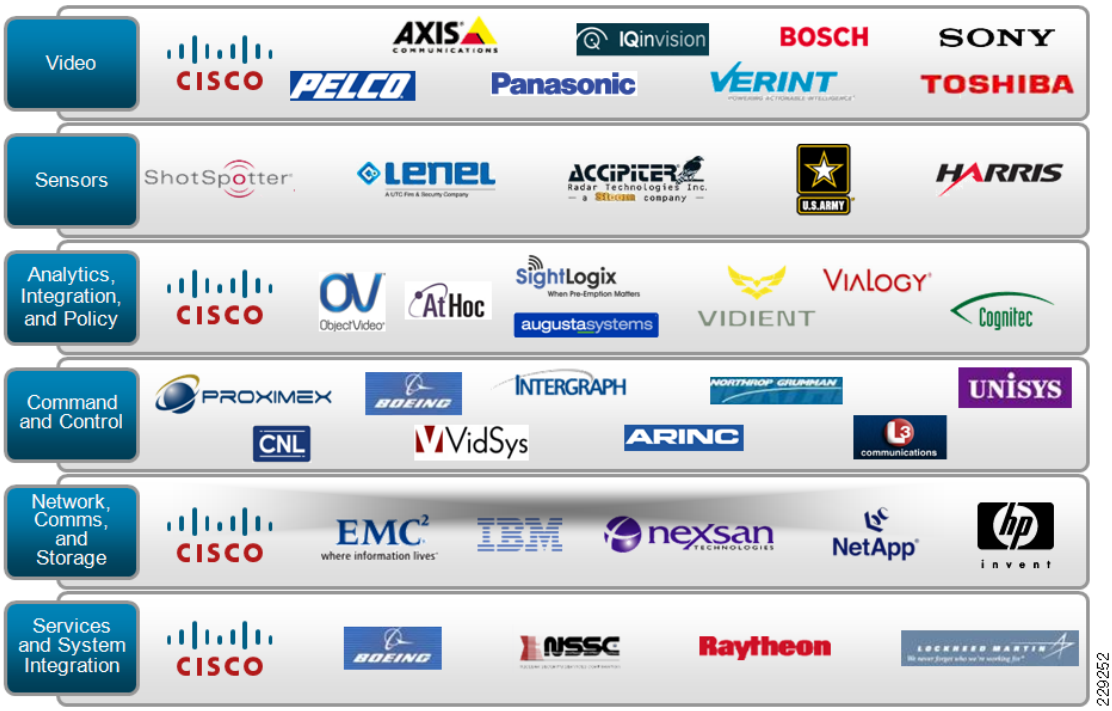
Scope of the Solution

Chapter 4, “Designing the Solution.”highlights the thought process used to determine which components to use and the best way to go about integrating them. Typically, there are multiple ways to integrate the various components.

The focus of this design guide is to help the reader understand the capabilities of the components. There are many ways to integrate different products, and the design guide shows just one way on how the integration testing was accomplished.

Additionally, there are multiple partners that provide the same capabilities in various spaces. As shown in Figure 1-1, there are many different partners that provide similar capabilities.

Figure 1-1 Physical Security Partner Eco-System



Every customer situation is different, and each customer is likely to have a different set of requirements and existing partner components. Understanding how the functions interact versus which partner provided which component is the more important lesson to learn.

Chapter 5, "Integrating the Applications" provides the details of how the components were integrated for testing purposes, showing enough detail so that the reader can understand and integrate this or similar components in their own environment.

This design guide is intended to show how the components used in this solution can be integrated to solve particular business problems. Where HA and scalability documentation exists for a particular component, it is referenced. However, it is best to refer to the product documentation wherever possible for those specific design details.

Use Cases

The following use cases were selected to assist in identifying the products and integration necessary to address these challenges. This is merely a subset of a much greater list of functionality that one would expect to see in designing an Urban Security solution. However, this subset does allow for the identification of specific design criteria and should provide real-life examples of how these components would/could be used in the real world.

Fire Alarm/Smoke Alarm

Multiple scenarios can be used to simulate fire and smoke alarms. These include smoke detectors, fire alarms, infrared cameras, and citizen-reported incidents. While there are strict regulations on the deployment of fire alarm systems, the incident can be handled using a consolidated interface to quickly resolve the incident.

Scenario 1

1. A fire/smoke detector is triggered (simulated in the lab).
2. Cameras in close proximity to the sensor that initiated the alarm are trained on the location.
3. Central Operations is notified of the situation:
   a. Audio alarm
   b. Text notification via phone system
   c. Video notification via digital media
4. Central Operations assesses the situation and takes appropriate actions:
   a. Notification of first responders with location, video feed
   b. Citizen notification via loud speaker, digital media
   c. Initiation of a perimeter monitoring situation, with tripwire crossing notifications when unauthorized personnel pass into the area
5. Central Operations continues to monitor situation via video feeds and provides coordination between first responders
   a. Creates a private communications channel between fire, police, and authorized persons for the duration of the incident
   b. Streams video to the personnel on-site
6. Central Operations sends an accountability notification to facility personnel, and tracks responses to ensure all affected personnel is accounted for.

Unattended Object/Loitering

There are many locations and situations where detecting an unattended object is considered safe practice. In the more obvious situations, detecting a package or piece of luggage left unattended in a train station or airport can be cause for concern. A less obvious situation is the presence of a vehicle in a forbidden location or an area where it has been left unattended for a period of time. In addition, there is typically a lot of background movement of people or vehicles, making it harder to pick out specific objects. There are situations where either of these may not be cause for concern, so including the ability to evaluate the situation is imperative.

Scenario 2

1. Normal video surveillance of a typical environment that includes foot or vehicle traffic is in operation.
2. A person walks into the frame and sets down a package.
   a. Small package
   b. Large package
3. The individual walks away and leaves the package behind.
4. Video surveillance should identify the package left unattended via video analytics.
5. The policy engine re-trains other cameras in the area on the package.
6. Notification is made to Central Operations:
   a. Appropriate audio/video alarms are initiated
   b. Video surveillance from all cameras available

7. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone, desk phone
   b. Citizen notification via loud-speaker, digital media displays

Scenario 3

1. Normal video surveillance of a typical environment that includes foot or vehicle traffic is in operation.
2. A vehicle pulls into a no-parking location and stops.
3. After a set period of time, it is determined that this situation needs to be investigated.
4. Notification is made to Central Operations:
   a. Appropriate audio/video alarms are initiated
   b. Video surveillance from all cameras available
5. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone, desk phone
   b. Citizen notification via loud-speaker, digital media displays

Video Tripwire Crossing

Tripwire crossing can have various meanings based on the location and type of sensors. In a large area such as an airport or oil refinery, sensors can be monitoring the fence line, watching for suspicious movement. In a border situation, it can be monitoring a state or country line, or a river for illegal crossings. In a train station, it can be watching for track crossings, but having the need to differentiate between a track crossing and a worker on a catwalk. From a harbor port perspective, it can be the detection of a ship crossing into local waters, either in a port area or up to 10 miles off-shore.

Scenario 4

1. Normal video surveillance of an area identified as off-limits is in operation.
2. A person walks into the frame.
   a. Audio alarm initiated requesting person to leave area
   b. Central Operations notification occurs, providing video feed
3. The individual leaves and no further action is required.
4. Normal video surveillance of an area identified off-limits resumes.

Scenario 5

1. A person walks into the frame.
   a. Audio alarm initiated requesting person to leave area
   b. Central Operations notification occurs, providing video feed
2. The individual continues into the unauthorized area.
3. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone, desk phone
   b. Additional audio alarms initiated via loudspeaker

Unauthorized Building Access/Forced Entry

Controlling physical access to a location is as much about keeping unauthorized persons out of an area as it is about allowing authorized persons into the same area. To make this a bit more difficult, this profile can change based on situational conditions or time of day.

For example, consider a lab environment. During normal conditions, there are lab workers that are allowed into the area to perform their job. If, however, a situation arises where a spill occurs in the lab, there should be an alarm to evacuate the area, and that area should now be off-limits to normal workers but still allow first responders into the area. So, dynamically changing the security profile based on situational or operational awareness is a requirement.

This example can be expanded to include access for shift workers, allowed access only during their particular shift, or allowing only maintenance personnel access after hours.

Scenario 6

1. Forced entry is detected on a door location.
2. Central Operations is notified of the situation:
   a. Text notification
   b. Audio alarm in Central Operations and door location
   c. Video surveillance of the door is available
3. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone
4. Central Operations continues to monitor the situation.

Scenario 7

1. Door access is set up to allow workers into the area.
2. A situation occurs within the location; that is, a fire or chemical sensor alarm occurs in the area.
3. Central Operations is notified of the situation:
   a. Text notification and desktop notification
   b. Audio alarm in Central Operations and alarm location
   c. Video surveillance of the entire area
4. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel are notified via loud speaker to evacuate the location and report to muster station
   b. Door access profile is changed to allow all workers egress, but only first responders ingress to the location
   c. Personnel are provided further instructions via digital media at the muster station
5. Central Operations continues to monitor the situation.

CHAPTER 2

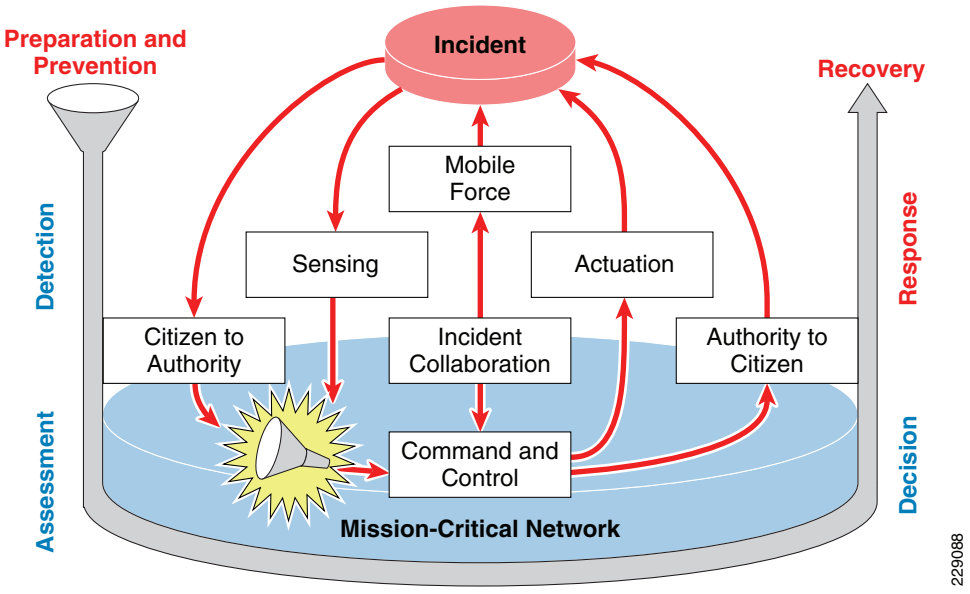
Architecture Framework

The Cisco Open Platform for Safety and Security (Cisco-OPSS) is an architecture framework that technology architects can use to develop solutions for Urban Security. The framework offers public safety officials the flexibility to adopt new technology to meet evolving operational requirements, including real-time decision-making and networked command and control.

Cisco-OPSS consists of the following six major architecture building blocks as shown in Figure 2-1.

- Command and Control
- Mission-Critical Networks
- Incident Collaboration
- Sensing and Actuation
- Mobile Force
- Citizen-Authority Interaction

Figure 2-1 Cisco Open Platform for Safety and Security



Each architecture building block contains an hierarchy of functional building blocks. In combination, these building blocks provide a rich set of capabilities to support a particular organization's safety and security goals.

For this release of the *Urban Security Design Guide*, the focus is limited to the following three architecture building blocks of the COPSS architecture:

- Command and Control
- Sensing and Actuation
- Citizen-Authority Interaction

Future releases of this design guide will expand on the concept and address the rest of the architecture building blocks not included in this release.

Cisco and its partners defined functional building blocks logically, rather than specifying a particular product offering. This gives organizations the flexibility to select various solutions based on their country and individual requirements. It also makes it easier to identify any missing capabilities in a specific solution.

The following sections provide brief descriptions of each of the six architecture building blocks of the Cisco Open Platform for Safety and Security.

Command and Control

Command and Control provides the emergency management team with up-to-date situational awareness, actionable intelligence, and decision support tools. Command and control contains the following functional building blocks:

- Common Operational Picture (COP)
- Unified Management
- Simulation and Investigation

Sensing and Actuation

The *Sensing and Actuation* building block streams information from the incident scene to the operations center and provides the means for swift and automated remote action. It contains the following functional building blocks:

- Quantitative sensors
- Qualitative sensors
- Human identification based on physical characteristics that are part of a system (biometrics, as opposed to video analytics, where no specific identification is made)
- Object identification, possibly including RFID
- Real-time video analytics
- Sensor correlation and baselining
- Actuators
- Legacy integration

Citizen-Authority Interaction

The *Citizen-Authority Interaction* building block provides two-way communications capabilities. Service codes, also known as N11 codes, are used to provide three-digit dialing access to special emergency support services. Examples of these numbers include 112, 911, or 999. Conversely, authorities can alert a specific group of individuals about immediate danger, such as a fire, bomb, or biological attack. This capability is sometimes called *Reverse 911*.

The Citizen-Authority Interaction contains the following functional building blocks:

- Authority-to-Citizen—Public alert notification and information systems
- Citizen-to-Authority—Public Safety Answering Point (PSAP)

Mission-Critical Network

Public safety and security organizations today rely on a variety of heterogeneous networks to carry out all their activities. Consolidating these networks into a unified Emergency-Grade Network platform optimizes emergency operations. The Emergency-Grade Network must be scalable, resilient, secure, and intelligent.

The *Mission-Critical Network* functional building blocks include the following:

- IP-layer abstraction
- Traffic optimization, including quality-of-service (QoS), resilience, multicast, and traffic engineering
- Self-defense, including network access control, VPN, and firewall
- Mobility, including wireless access and geolocation
- Data center technologies, including high-performance computing, WAN acceleration, and load balancing
- Rapid deployment

The Mission-Critical Network uses IP to support multiple transmission standards, including Terrestrial Trunk Radio (TETRA), WiMax, Wi-Fi, 3G, and satellite communication technologies.

Incident Collaboration

The effectiveness of communications between first responders and the command and control center can have life-or-death consequences. The *Incident Collaboration* building block helps to ensure that teams can communicate using any available technology, including IP and analog or digital radio, as well as any media, including voice, video, instant message (IM) or short message service (SMS), and data. Incident Collaboration contains the following functional building blocks:

- Core systems, which include call processing, user and device provisioning, communication provisioning, monitoring, interoperability and open interfaces, system recovery, security management, presence services, and gateways
- User terminal, which can be defined in terms of its connectivity and functionality
- Notification services, which include instant messaging, SMS, E-mail, and paging
- Conferencing, which includes data sharing, voice, video, and Cisco TelePresence

Emergency responders must be able to spontaneously create communications groups that link people in a geographical area, regardless of their organization or the communication device they use.

Mobile Force

The *Mobile Force* building block ensures that human resources are as effective in the field as they are in the central monitoring room. The following are some examples:

- Security guards can monitor and control video surveillance cameras from a hand-held device.
- Police officers in their vehicles can securely access central databases through a mobile access router.
- Fire commanders can monitor conditions at the scene through the biosensors on firefighters' suits.
- First responders can receive events with visual verification to determine validity of event and severity of the threat level.
- On the way to a disaster scene, rescue teams can receive up-to-the-minute information such as location, type of accident, and casualties.
- Emergency services personnel receive appropriate information based on their role, access information using a graphical, intuitive interface, and can use it to rapidly decide on the best operational tactic.

The Mobile Force architecture building block contains the following functional building blocks:

- Mobile devices—Personal passive devices, personal computing devices, and vehicle computing devices
- Mobility types—Nomadic, seamless, and adhoc
- User-based services—Location-based services, application and databases access, automatic alerting and notification, zero-touch configuration and management, and a communications and collaboration interface.

CHAPTER 3

Solution Components

The Urban Security solution includes Cisco security products such as physical access control and video surveillance, in addition to networking and unified communications products. It also includes partner products from Proximex, ObjectVideo, and AtHoc.

Cisco Video Surveillance

Video surveillance has been a key component of the safety and security groups for many organizations. As an application, video surveillance has demonstrated its value and benefits countless times by providing real-time monitoring of a facility's environment, people, and assets by recording events for subsequent investigation, proof of compliance, and audit purposes.

For environments that need to visually monitor and/or record events, video surveillance has become more important as the number of security risks increase. In addition to video analytics, the value of video surveillance has grown significantly with the introduction of access control, motion, heat, and environmental sensors.

In typical environments, several systems are deployed to monitor disparate applications, such as access control, fire and smoke detection, and video surveillance. These applications typically do not communicate with each other and require different management and support personnel. As a result, owners and operators suffer from a lack of operational consistency, interoperability, and capabilities that translate into higher capital and operational costs, which limit the return on their system investments.

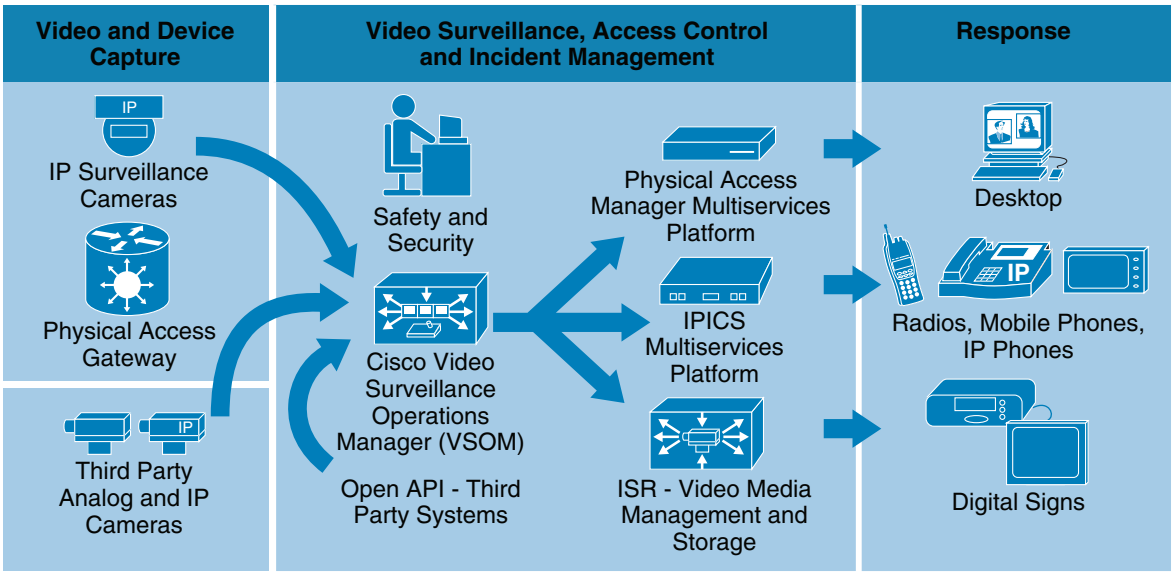
Cisco's solution offers hardware and software to support video transmission, monitoring, recording, and management. Cisco video surveillance solutions work in unison with the advanced features and functions of the IP network infrastructure—switches, routers, and other network security devices—to enable secure, policy-based access to live and recorded video.

Through the Cisco architecture, video can be accessed at any time from any place, enabling real-time incident response, investigation, and resolution. The open, standards-based Cisco infrastructure enables the deployment and control of new security applications and maximizes the value of live and recorded video, interacting with multiple third-party applications and video surveillance cameras.

The Cisco Video Surveillance solution relies on an IP network infrastructure to link all components. The designs of a highly available hierarchical network has been proven and tested for many years and allows applications to converge on an intelligent and resilient infrastructure.

Figure 3-1 shows the main components of the Cisco Physical Security solution, including video surveillance, access control, incident response, and integration with third-party systems.

Figure 3-1 Cisco Physical Security Components



The benefits of Cisco's Video Surveillance solution include the following:

- Access to video at any time from any network location, enabling real-time incident response and investigation
- Transfer of control and monitoring to any other point in the network in an emergency situation
- Ability to manage devices and alerts from a centralized location
- Ability for products from various vendors to interoperate in the same network
- An open, standards-based infrastructure that enables the deployment and control of new security applications

The main components of the Cisco Video Surveillance solution include the following:

- Cisco Video Surveillance Media Server—The core component of the network-centric Video Surveillance Manager. This software manages, stores, and delivers video from a wide range of cameras and encoders over an IP network.
- Cisco Video Surveillance Operations Manager—The Operations Manager authenticates and manages access to video feeds. It is a centralized administration tool for management of Media Servers, Virtual Matrixes, cameras, encoders, and viewers and for viewing network-based video.
- Cisco Video Surveillance IP Cameras—The high-resolution digital cameras are designed for superior performance in a wide variety of environments.
- Cisco Video Surveillance Virtual Matrix—The Virtual Matrix monitors video feeds in command center and other 24-hour monitoring environments. It allows operators to control the video being displayed on multiple local and remote monitors.
- Cisco Video Surveillance Encoding Server—This all-in-one appliance encodes, distributes, manages, and archives digital video feeds. Each server encodes up to 64 channels and provides up to 12 TB of storage.
- Cisco Video Surveillance Storage System—This complementary component allows the Media Server's internal storage to be expanded with direct attached storage (DAS) and storage area networks (SANs). The Storage System allows video to be secured and accessed locally or remotely.

The following sections describe the components used for this solution.

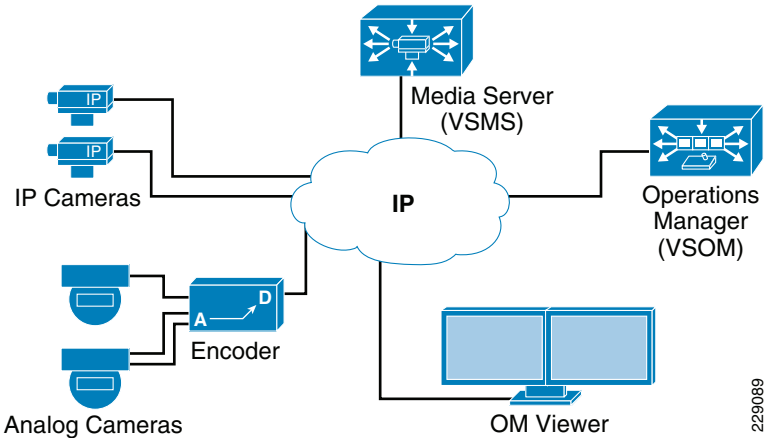
Cisco Video Surveillance Media Server

The Cisco Video Surveillance Media Server (VSMS) is the core component in the Cisco Video Surveillance Manager and performs the following networked video surveillance system functions:

- Collection and routing of video from a wide range of third-party cameras and video encoders over an IP network
- Event-tagging and recording of video for review and archival purposes
- Secure local, remote, and redundant video archive capabilities

As shown in Figure 3-2, the Media Server is responsible for receiving video streams from various IP cameras and encoders and replicating them as necessary to various viewers.

Figure 3-2 Video Surveillance Media Server



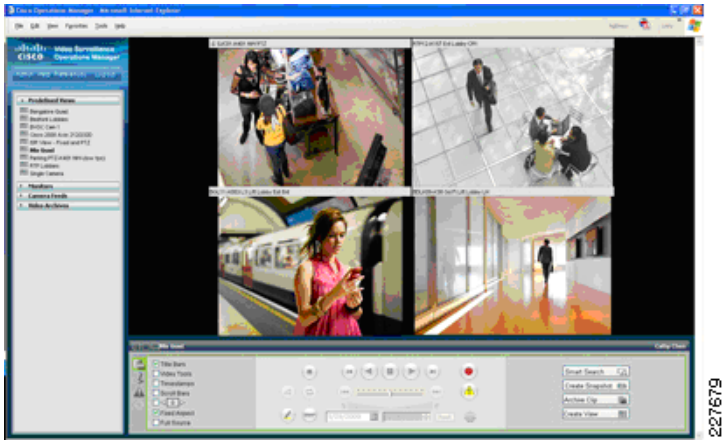
By using the power and advanced capabilities of today's IP networks, the Media Server software allows third-party applications, additional users, cameras, and storage to be added over time. This system flexibility and scalability supports the following:

- Hundreds of simultaneous users viewing live or recorded video
- Standard video compression algorithms such as MJPEG, MPEG-2, MPEG-4, and H.264 simultaneously via a single Media Server
- Conservation of storage using events and loop-based archival options
- Integration with other security applications

Cisco Video Surveillance Operations Manager

Working in conjunction with the Cisco Video Surveillance Media Server, the Cisco Video Surveillance Operations Manager (VSOM) enables organizations to quickly and effectively configure, manage, and view video streams throughout the enterprise. Figure 3-3 shows the Operations Manager main screen, which is accessed via a web browser.

Figure 3-3 Video Surveillance Operations Manager



The Operations Manager meets the diverse needs of administrators, systems integrators, and operators by providing the following:

- Multiple web-based consoles to configure, manage, display, and control video throughout a customer's IP network
- The ability to manage a large number of Cisco Video Surveillance Media Servers, Cisco Video Surveillance Virtual Matrixes, cameras, and users
- Customizable interface, ideal for branded application delivery
- Encoder and camera administration
- Scheduled and event-based video recording
- Interface to Media Server and Virtual Matrix software for pushing predefined views to multiple monitors
- User and role management
- Live and archived video views
- Friendly user interface for PTZ controls and presets, digital zoom, and instant replay
- Event setup and event notifications
- "Record Now" feature while viewing live video

Cisco Video Surveillance IP Cameras

Cisco 2500 Series Video Surveillance IP Camera

The Cisco 2500 Series Video Surveillance IP camera is a high-definition, feature-rich digital camera designed for secure performance in a wide variety of environments. The camera supports MPEG-4 and MJPEG compressions with up to 30 frames per second.

Contact closure and two-way audio allow integration with microphones, speakers, and access control systems. By providing wired and wireless models, the Cisco 2500 IP camera provides an ideal platform for integration and operation as an independent device or as part of the Cisco Video Surveillance network. Figure 3-4 shows both the wired and wireless models of the Cisco 2500 IP Camera.

Figure 3-4 Cisco 2500 Series IP Cameras

The Cisco 2500 Series IP Camera provides several features, including the following:

- The camera employs powerful digital imaging technology, allowing it to capture high-quality images in a wide variety of indoor and outdoor lighting conditions. It uses a progressive scan image sensor with global electronic shuttering to ensure natural color rendition, and minimal motion blurring.
- The wireless IP camera model supports 1 x 2 Multiple Input Multiple Output (MIMO) communication, which provides better data throughput and higher link range than single antenna designs. The wireless IP camera offers strong wireless security using Wi-Fi Protected Access (WPA)/WPA2 and supports various network protocols for 802.1x authentication.
- Power-over-Ethernet (PoE) 802.3af or DC power through an optional external power supply.
- Support for the Cisco Media API, an open, standards-based interface that allows integration with compatible video surveillance management systems.
- Support for 802.1x authentication on both the wired and wireless models.

Cisco 2000 Series IP Domes

The Cisco Video Surveillance 2000 Series IP Domes are high-resolution, feature-rich digital IP cameras that can be deployed in a wide variety of environments. The cameras use MPEG-4 compression of up to 30 frames per second (fps) at D1 NTSC resolution for efficient network utilization and high-quality video. They also support MJPEG compression. Figure 3-5 shows the Cisco 2400 and 2500 IP Dome cameras.

Figure 3-5 Cisco 2400 and 2500 IP Domes

The following models are available in the Cisco 2000 Series:

- The Cisco IP Dome 2421 is an indoor-only, ceiling tile mount camera for retail and common office deployments.
- The Cisco IP Dome 2520V is a vandal-resistant indoor camera for schools, railway platforms, or other public areas.
- The Cisco IP Dome 2530V is a vandal-resistant, ruggedized, outdoor camera for difficult environments with high or low temperatures, moisture, or dust. This camera does not support Power-over-Ethernet (PoE).

The Cisco 2000 Series IP Domes provides features such as the following:

- Wide dynamic range—The cameras employ powerful digital imaging technology, allowing them to capture high-quality images in a wide variety of indoor and outdoor lighting conditions. They use a progressive scan image sensor with global electronic shuttering to ensure natural color rendition, zero blooming and smear, and minimal motion blurring.
- Dual streaming—The cameras can stream MPEG-4 and MJPEG video simultaneously. Each video stream can be configured with individual resolution, quality, and frame rate settings.
- Embedded security and networking—The cameras provide 802.1X authentication and hardware-based Advanced Encryption Standard (AES). For enhanced bandwidth management, the cameras support IP Multicast.
- Flexible power options—The Cisco 2500 and 2400 IP Domes support Power-over-Ethernet (PoE) 802.3af, and 12 VDC or 24 VAC power through an optional external power supply. The 2530 IP Dome does not support PoE.
- Event notification—The cameras can examine designated areas in the video for motion activity and then notify users or other applications when they detect activity that exceeds a predefined threshold.
- Day/Night operation—The cameras provide true day/night operation and include an IR filter that automatically switches to night mode in low-light scenes. This function can be set to manual or automatic control.

Cisco 4000 Series Video Surveillance IP Camera

The Cisco Video Surveillance 4000 Series IP Cameras employ true high-definition (HD) video and H.264 compression, streaming up to 30 frames per second at 1080p (1920 x 1080) resolution. The Cisco 4000 Series IP Camera also supports contact closure and two-way audio that allow integration with microphones, speakers, and access control systems.

The Cisco 4000 Series includes two models: the CIVS-IPC-4300 and CIVS-IPC-4500. These cameras have identical feature sets, with the exception of the additional digital signal processor capabilities specifically designed to support real-time video analytics at the edge on the CIVS-IPC-4500. On this model, applications and end users have the option to run multiple analytics packages, without compromising video streaming performance on the camera.

This guide focuses on server-based analytics, because support for edge-based analytics is not available for deployment as of the writing of this guide.

Figure 3-6 shows a Cisco 4000 IP Camera with an optional DC Auto Iris Lens.

Figure 3-6 Cisco 4000 Series IP Camera

The Cisco 4000 Series IP Camera provides the following features:

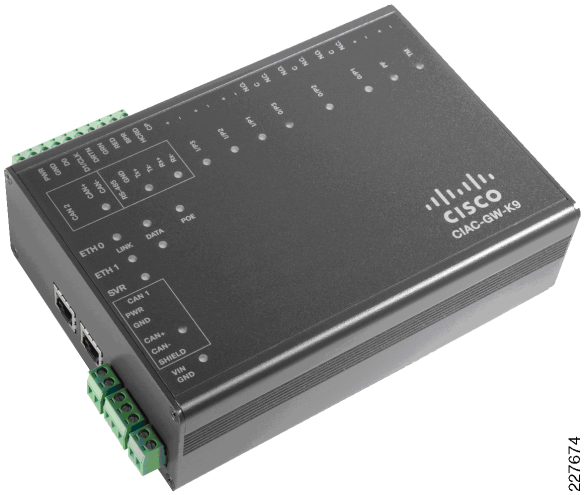
- True high-definition video—The camera streams crisp and clear 1080p (1920 x 1080) video at 30 frames per second while maintaining surprisingly low network bandwidth.
- Progressive scan video—The camera captures each frame at its entire resolution using progressive scan rather than interfaced video capture, which captures each field of video.
- Embedded security and networking—The camera provides hardware-based Advanced Encryption Standard (AES).
- IP Multicast for enhanced bandwidth management.
- Event notification—The camera can examine designated areas for activity and notify users or other applications when it detects activity that exceeds a predefined sensitivity and threshold.
- True day/night functionality that includes an IR filter that automatically switches to night mode in low light scenes.
- The camera supports Power over Ethernet (PoE) 802.3af, 12 VDC or 24 VAC power through an optional external power supply.
- The camera can be installed with a fixed mount or with an optional external pan/tilt mount and motorized zoom lens.

Cisco Physical Access Control

The Cisco Physical Access Control solution is a comprehensive solution that provides Electronic Access Control using the IP network. The solution consists of hardware and software products and is modular, scalable, and easy to install. It allows any number of doors to be managed using the IP network. The Cisco Physical Access Control is also integrated with Cisco Video Surveillance Manager.

Cisco's Physical Access Control solution has two main components: Cisco Physical Access Gateway and Cisco Physical Access Manager. The Cisco Physical Access Gateway is installed near a door and connects existing door hardware (readers, locks, and so on) through a controller area network (CAN or CAN-bus). It also has Ethernet ports to be connected to an IP network. CAN-bus enables the Cisco Physical Access Gateway to function normally when the network is down, while the Ethernet connection enables it to be controlled over the network. Figure 3-7 shows a Physical Access Gateway.

Figure 3-7 Physical Access Gateway

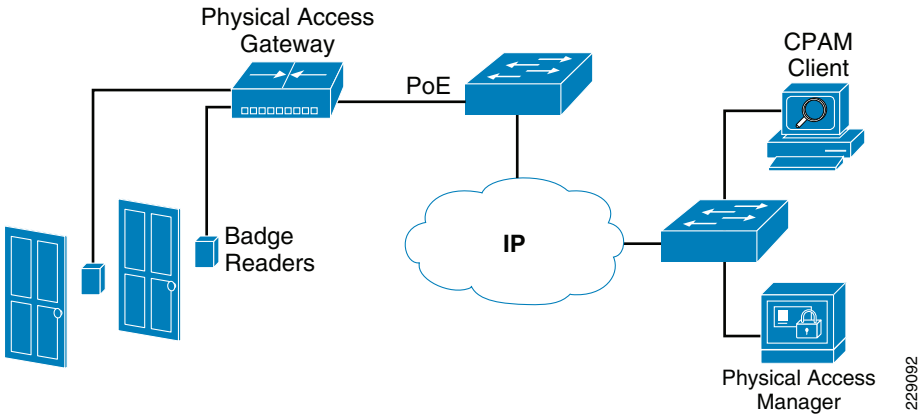


The Cisco Physical Access Manager (CPAM) is a management appliance for configuration, monitoring, and report generation. It can manage up to 2,000 Cisco Physical Access Gateways distributed across different network locations. Figure 3-8 shows a CPAM appliance.

Figure 3-8 Cisco Physical Access Manager

Figure 3-9 shows a typical physical access control deployment with badge readers located at different locations. With the proper authorization, users are able to connect to the CPAM remotely to manage the environment.

Figure 3-9 Physical Access Control Deployment



Cisco IP Interoperability and Collaboration System (IPICS)

The Cisco IP Interoperability and Collaboration System (IPICS) integrates server, routing, and IP communications elements to provide on-demand incident communications across agencies and interoperability and operational efficiencies for public safety agency and support personnel.

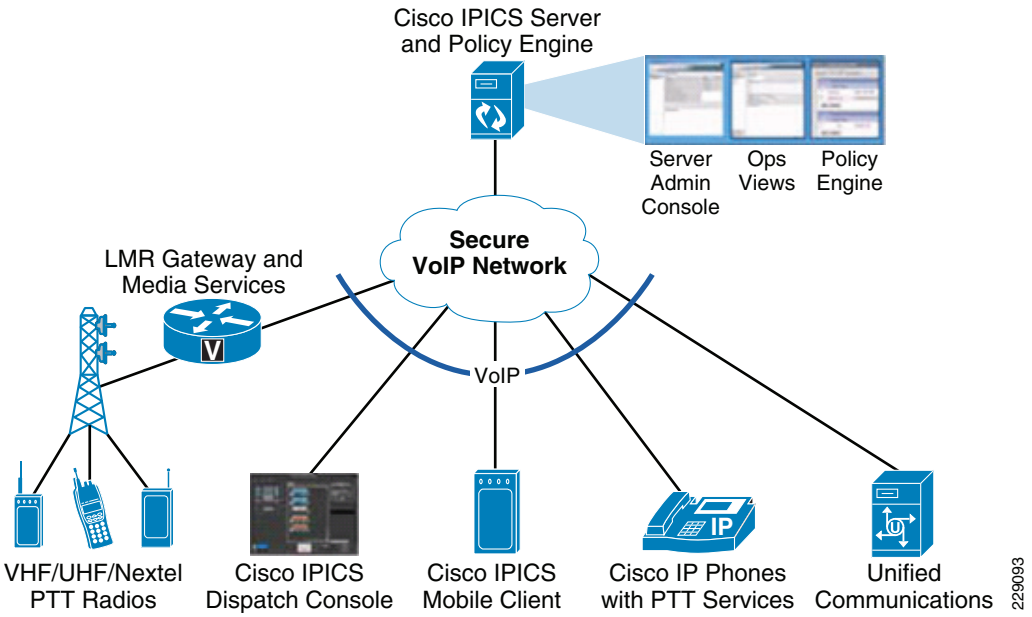
IPICS Functions

Cisco IPICS enables radio interoperation. When different first-responder organizations convene at an incident scene, they cannot communicate among each other directly because their radios operate over different frequencies and use different techniques. With Cisco IPICS, security officers can use any communication device: existing analog or digital radios, new Project 25 (P25) radios, Push-to-Talk (PTT) devices, standard analog phones, cell phones, IP phones, and PCs and laptops with the appropriate software. IPICS combines different channels into a virtual talk group. Usually the same type of radios is used by a small organization. These radios talk over the same channel. For example, the police department of a city may talk on one channel while the fire department may use another channel. One channel can have hundreds of radios. One incident can require the use of multiple unique channels that corresponds to various responder groups.

Cisco IPICS converts radio frequencies to IP multicast streams and then mixes different channels to a virtual talk group. Customers typically set up many talk groups to deal with various situations. For example, one virtual talk group can be set up to bring together all fire emergency personnel, while another talk group can be reserved for another responder team.

Figure 3-10 shows the operations of Cisco IPICS.

Figure 3-10 Cisco IPICS Facilitates Comprehensive Communications Interoperability



With IPICS, an organization's radios can be at any location. For example, if an organization has offices in Boston and Bangalore, the security forces at these two locations can talk to each other through the radios that are using the IPICS network services.

With IPICS, phones can function as radios by using the PTT service of IPICS. Because many people have cell phones, an organization can save the cost of buying everyone a radio by connecting phones via the Public Switched Telephone Network (PSTN) through IPICS.

With IPICS, communications among security officers can be automatically triggered by incidents. Traditionally, people report an incident to an operator. The operator then activates a radio channel for first responders to communicate. With IPICS, a device can activate a talk group. For example, upon detecting a chemical leak, a sensor can send a URL to IPICS to activate communication among a group of people responsible for handling chemical leak, including the situation operator.

The Cisco IPICS Dispatch Console (see Figure 3-11) and IPICS mobile client have made IPICS a multimedia collaboration platform. A dispatcher can monitor radio communications from any PTT device. The dispatcher can add any organization, person, or department to the talk group as a situation changes. The dispatcher or a first responder can transmit and receive real-time video, pictures, and text information related to an incident. For example, if a dispatcher receives a call about fire, she creates a "fire" incident response and opens the IPICS dispatcher console. From the console, she adds virtual talk groups. While the incident is active, an IPICS mobile client (such as an iPhone) can also act as a PTT device and communicate with radios. Figure 3-12 shows the menu on the IPICS moble client. If a police officer with an IPICS mobile client captures an image of a criminal, she can upload the video to share with other first responders (see Figure 3-13). To enable IPICS mobile client function on iPhone, a user can download "incident" application using the following steps:

Step 1 Click the **App Store** icon in the iPhone.

Step 2 Search for the application.

Step 3 Install it.

Description of the application can be found at the following URL:

http://itunes.apple.com/au/app/incident-4-0-1/id362035991?mt=8

Figure 3-11 IPICS Dispatch Console

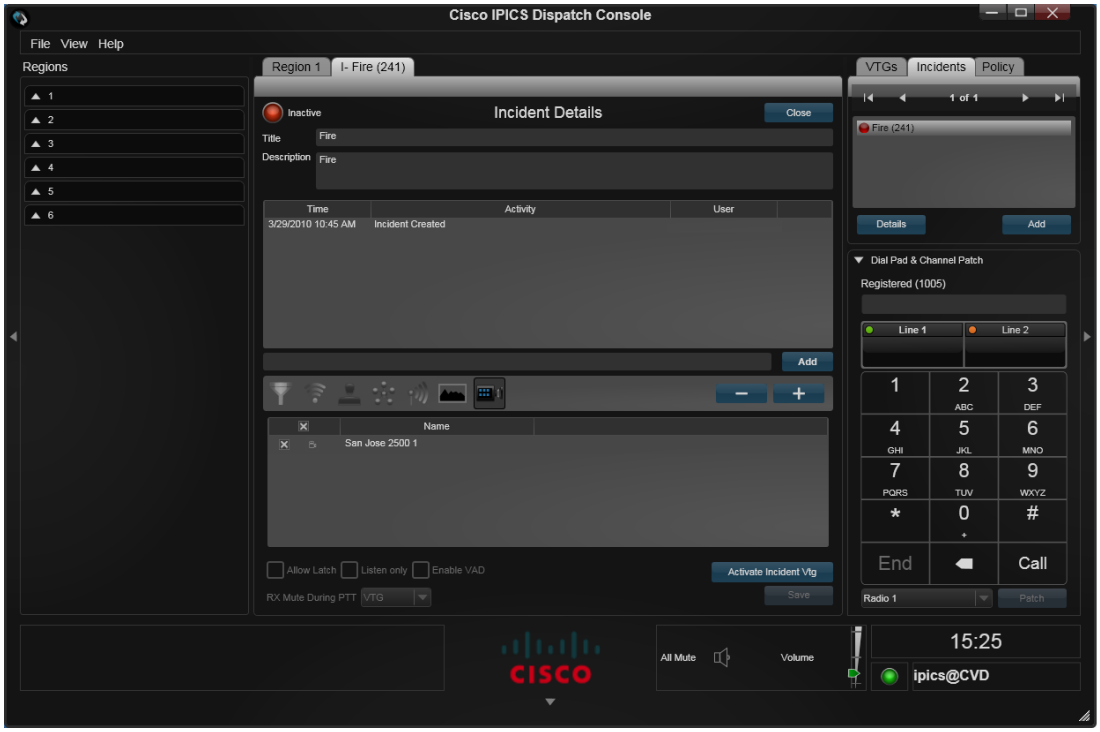
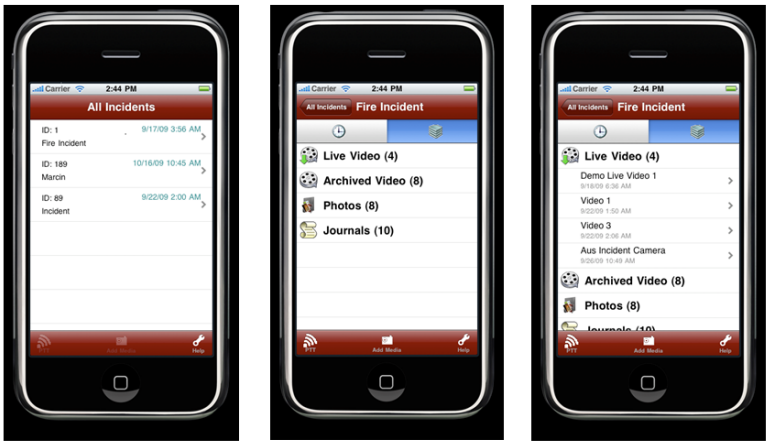


Figure 3-12 Menu on IPICS Mobile Client



View assigned incidents

View available media choices within an incident

Figure 3-13 Live Video on IPICS Mobile Client

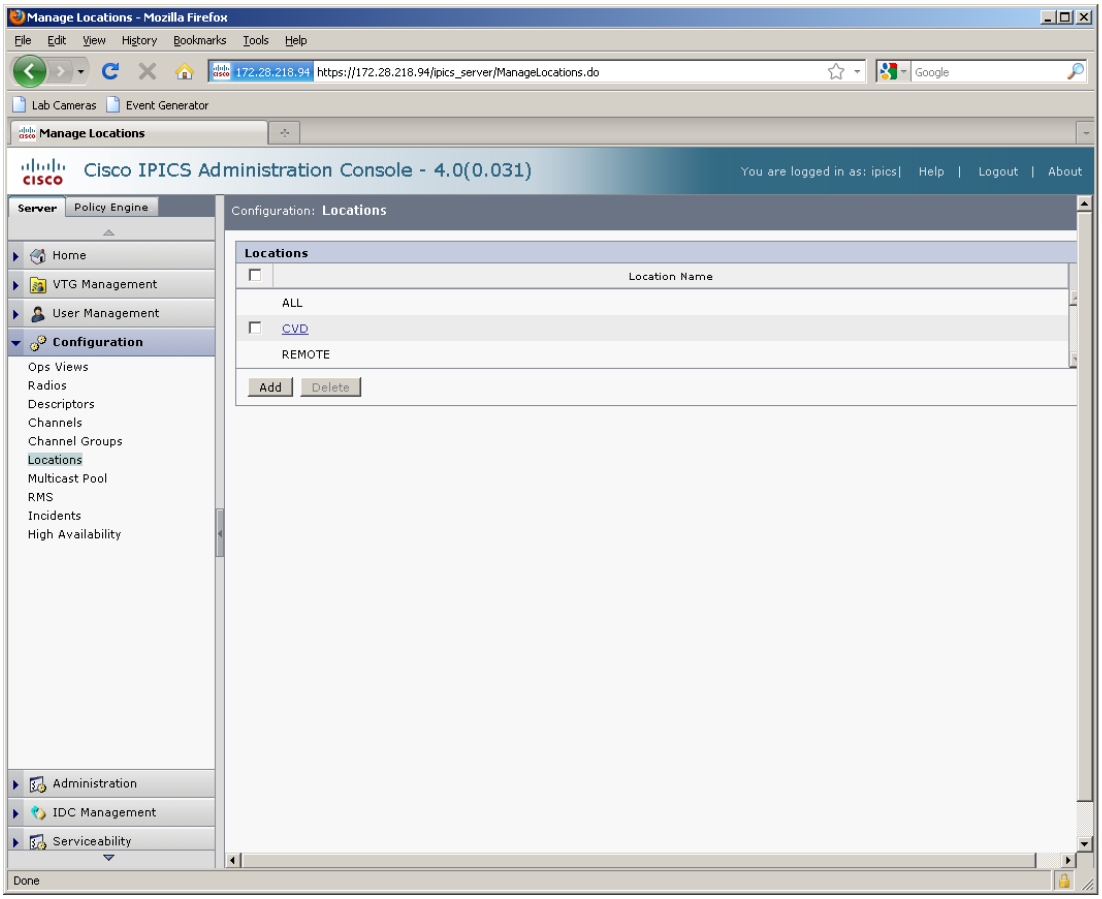
Components of IPICS

A Cisco IPICS deployment involves several hardware and software components to enable interoperability and collaboration. Key components include a Cisco IPICS server, a Land Mobile Radio (LMR) gateway, and a router media service (RMS). The functions of each of these components are described below.

Cisco IPICS Server is the center of all Cisco IPICS activities. Cisco IPICS server software (Figure 3-14 shows the IPICS console) runs on the Cisco Linux operating system and performs the following functions:

- Hosts the Cisco IPICS Administration Console, which is an incident management framework administration GUI that enables dynamic resource management for users, channels, and virtual talk groups (VTGs)
- Provides Cisco IPICS authentication and security services
- Stores configuration and operational data
- Enables integration with various media resources, such as RMS components, Cisco Unified IP Phones, Cisco Unified Communications Manager, and Cisco IOS SIP gateways
- Hosts the Cisco IPICS policy engine (hereafter referred to as policy engine), which enables telephony dial functionality and maintains responsibility for the management and execution of policies and user notifications

Figure 3-14 IPICS Server Console



An LMR gateway converts between radio frequencies and IP multicast packets, thus providing voice interoperability between radio and non-radio networks. It also provides keying signals to key radio transmissions. Its functionality is usually installed as an additional feature in a supported Cisco router.

The Router Media Service (RMS) provides various mixing functions. It supports, through its loopback functionality, remotely attaching (combining) two or more VTGs. The RMS mixes multicast channels in support of VTGs. The RMS also converts between unicast packets and multicast packets when a user is not located on a multicast domain.

The overall IPICS environment can support a large array of endpoints, such as radios, IPICS dispatch consoles on laptops, and cell phones (also called mobile clients).

Cisco Unified Communications

Cisco Unified Communications offers a new way to communicate. This comprehensive, integrated IP communications system of voice, video, data, and mobility products and applications allows the network to become an intelligent platform for effective, collaborative, scalable, and secure communications.

By integrating the systems with an intelligent IT infrastructure, the network is transformed to a “human network” that offers an organization the ability to access information on demand, to interact with virtual teams wherever they are, and to manage these interactions on the go, in real time.

Cisco Unified Communications offers a way to provide audio and text notification of alerts and can provide information customized for specific alerts. For example, specific alerts may be sent by AtHoc IWSAlerts or Cisco IPICS to all IP phones or other IP-enabled communications devices, such as sirens and public address (PA) systems.

The minimum configuration required for a Cisco Unified Communications system is a call control server (Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition, Cisco Unified Call Manager Express, or Unified Communications 500), IP phones (hard phones and/or soft phones), and a gateway to communicate with the PSTN. Additional components that are typically deployed are a Presence Server to provide presence information (available, on the phone, in a meeting, and so on), either Unified Messaging or Voice Mail, and collaboration via WebEx.

Cisco Unified Communications Manager

The Cisco Unified Communications Manager (formerly Cisco Unified CallManager) is the powerful call-processing component of the Cisco Unified Communications solution. It provides voice, video, mobility, and presence services for businesses with up to 30,000 users and is designed to lower the total cost of ownership for organizations and improve the communications experience for end users as well as system administrators.

The Cisco Unified Communications Manager creates a unified workspace that extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice over IP (VoIP) gateways, mobile devices, and multimedia applications. Additional services, such as unified messaging, multimedia conferencing, presence, collaborative contact centers, and interactive multimedia response systems, are made possible through open telephony APIs.

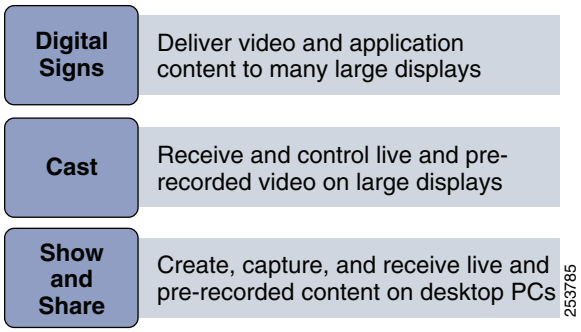
The Cisco Unified Communications Manager, deployable on the Cisco 7800 Series Media Convergence Servers or on third-party servers, offers the following features:

- Highly scalable, supporting up to 30,000 lines per server cluster
- Able to support a full range of communications features and applications, including SIP-based devices and applications
- Highly available for business continuity, supporting multiple levels of server redundancy and survivability
- Support for a broad range of phones to suit varying user requirements
- Choice of operating system environments—Windows server-based implementation or Linux-based appliance model implementation
- Available in an easy-to-manage single-server solution, Cisco Unified Communications Manager Business Edition, that combines call processing and unified messaging

Cisco Digital Media Suite

The Cisco Digital Media Suite (DMS) is a comprehensive suite comprised of Cisco Digital Signs, Cisco Cast, and Cisco Show and Share applications that allow companies to use digital media to increase sales, enhance customer experience, and facilitate learning. Figure 3-15 shows the three subsystems of Cisco DMS.

Figure 3-15 DMS Functional Subsystems



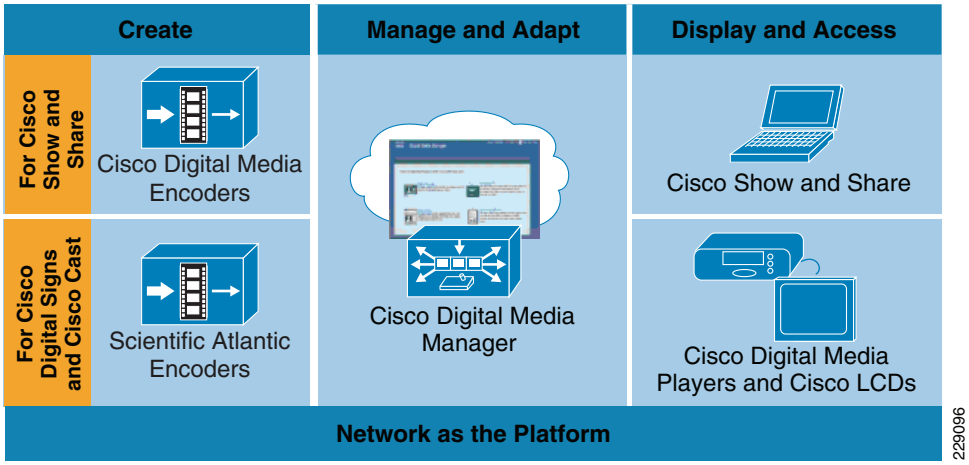
Digital Media draws viewers whether the content is marketing, internal communications, training, advertising, or entertainment materials. More and more organizations are using digital media to deliver timely and targeted communications. Digital Media is creating a new kind of customer experience and facilitating business transformation.

The Cisco Digital Media Suite extends digital media to new, compelling applications for real-time and on-demand communications with flexible digital media creation, management, and publishing of content in various formats to multiple devices.

During emergencies, the Cisco Digital Media Suite can also be used to communicate critical information to reach a large number of users in public places.

The Cisco Digital Media Suite allows for the creation, management, and access of content for several applications from a single platform, as shown in Figure 3-16.

Figure 3-16 Digital Media Suite



The following describe the components shown in Figure 3-16:

- Cisco Digital Media Encoders (DME)—The Cisco Digital Media Encoders capture and digitize media from a variety of inputs into a variety of digital formats for live and on-demand delivery across an IP network, along with monitoring functions.

- Cisco Digital Media Manager (DMM)—This web-based centralized media-management application allows both business and IT users to remotely perform management tasks based on roles for Cisco Digital Signs, Cisco Cast, and Cisco Show and Share. DMM allows content designers to customize Cisco Digital Signs screen layouts and brand the Cisco Show and Share interface. IT users can remotely configure, manage, and monitor the network of Cisco Digital Signs.
- Content publishing to Cisco Digital Media Players (DMPs)—The Cisco Digital Media Manager publishes content to and manages networked Cisco DMPs. Cisco DMPs are highly reliable IP-based hardware endpoints that enable Cisco Digital Signs and Cisco Cast by playing high-definition live and on-demand video, motion graphics, web, and dynamic content on digital displays for Cisco Digital Signs and Cisco Cast. The DMP hardware options include support for standard- and high-definition (SD and HD, respectively), MPEG2 and MPEG4/H.264, Flash, Really Simple Syndication (RSS), and other web content formats and dynamic data.
- Access through Cisco Show and Share—This social video system allows users to browse, search, and view digital media interactively at their desktop. Features include secure login and access to user-specific content, video playlists, keyword search and program guide, full-screen video playback, slide synchronization alongside video, question submission with live webcasts, video sharing, and detailed content and user access reporting.

Cisco Digital Signs provides scalable, centralized management and publishing of high-quality content to networked, on-premise digital signs. It can interoperate with Cisco Cast, or can operate as a standalone application.

Increasingly more government agencies, financial services organizations, retail stores, and educational institutions are using DMS for Digital Signs. Examples of industry applications include the following:

- Sports and entertainment—Deliver high-definition event broadcasts, live streaming statistics, sales and marketing of products and services, and directional informational on digital signs and video walls throughout the event venue, and in fan lounges and suites
- Government—Use digital signs to provide useful information for people waiting in line at government offices to help speed transactions or to send mass notification alerts in case of emergencies
- Healthcare—Share relevant healthcare information through digital signs around the hospital; offer cost-effective training options for hospital personnel.

The Digital Media Player acts as a powerful, customizable digital media endpoint and may be fully managed as a standalone device or as part of the Cisco Digital Media Suite. For the purpose of this solution testing, standalone DMPs were used to send alert messages to screens. The messages were originated from AtHoc IWSAlerts. Figure 3-17 shows a standalone DMP.

Figure 3-17 Digital Media Player

ObjectVideo

ObjectVideo is the leading provider of intelligent video software for physical security, public safety, business intelligence gathering, process improvement applications, and building automation. With its patented intelligent video technology, ObjectVideo software is employed in hundreds of organizations worldwide to enhance security, streamline operations and provide ongoing business intelligence.

Through advanced computer vision science, the ObjectVideo software brings an unmatched set of capabilities to operational challenges, including those in critical infrastructure, retail, banking, education, transportation and gaming. As it relates to Urban Security, ObjectVideo actively detects, classifies, and tracks objects, then immediately generates useful output for a wide variety of situations, including real-time alerts, and triggers for connected applications when user-defined rules are violated.

ObjectVideo's industry-leading software is available to market as a high-value ingredient through two innovative programs: ObjectVideo OnBoard, which enables original equipment manufacturers such as Cisco to embed ObjectVideo analytics into video devices (for example, the Cisco 4500 IP Camera) for customers to deploy; and OV Ready, an interoperability program that ultimately enables end customers to use intelligent video analytics in the easiest, most practical way possible.

Some of ObjectVideo's capabilities include the following:

- Object detection, classification and tracking—ObjectVideo's numerous patented algorithms enable the software to intelligently discern objects of interest; distinguish between humans, vehicles, and other objects and continuously track positions for all moving and stationary targets.
- Rule-specific intelligence—In addition to analyzing video for object detection, classification, and tracking, ObjectVideo enables users to create responses and notifications appropriate for those rules. Users can create rules that mimic defined security policies and generate real-time, actionable alerts when those rules are violated. Available rule types include detection of objects crossing a single or multiple Video TripWire, loitering, entering or exiting areas of interest, left behind or taken away objects, occupancy, and dwell time.
- Co-located processing—All user-defined rules are processed within the intelligent device itself for immediate comparison to the other video analysis functions. Co-locating the video analysis and the rule inference enables end-users to deploy intelligent video at any point in the video ecosystem. Significant network bandwidth is not required to bring together the video analysis and rule inference, nor is massive storage required to save video frames for after-the-fact processing.

- Multi-view—ObjectVideo can add intelligence to any PTZ camera by allowing multiple camera views/positions to be defined, each with its own unique set of rules. ObjectVideo OnBoard automatically recognizes which view the camera is using and quickly engages the appropriate rule set.
- Event Counting Suite—The Event Counting Suite (ECS) is highly optimized for event-based and occupancy counting scenarios, which can be applied to multiple urban surveillance scenarios. ECS also enables multi-rule and cross-camera counting scenarios, and provides a new web-enabled user interface to easily manage, monitor, and report on counting data.
- Crowd Density—In addition to using ECS for quantitative applications to count people and vehicles, ObjectVideo's Crowd Density feature enables a more qualitative means to detect user-defined crowding conditions. For example, at a subway station, there is a normal ebb and flow of crowds as trains and passengers come and go. Crowd Density can be configured to ignore the normal sporadic crowding and only alert when a "high density" crowd persists for a long period of time. That can indicate a possible delay in train arrival or a broken escalator, but most importantly, it identifies a potential public safety threat.
- ObjectVideo Forensics—The ObjectVideo Forensics feature enables users to discern critical intelligence about the environment based on past events. With this add-on, users can repeatedly apply rules to any repository of collected or stored video, and understand how to better define rules in the future. Additionally, with the video already processed and stored in the form of "video metadata", rules can be applied as search criteria to search through this metadata and retrieve events at speeds much greater than real-time video processing.

Proximex Surveillint

Proximex leads the physical security information management (PSIM) market by leveraging its innovative IT software expertise to drive security transformation and create synergy between logical and physical security departments.

The company's flagship product, Proximex Surveillint, is the premier physical security solution for policy-based incident discovery, connection, and resolution. Surveillint wraps around existing security systems to speed incident response times, improve suspect apprehension rates, and shorten the time required to resolve incidents and generate reports.

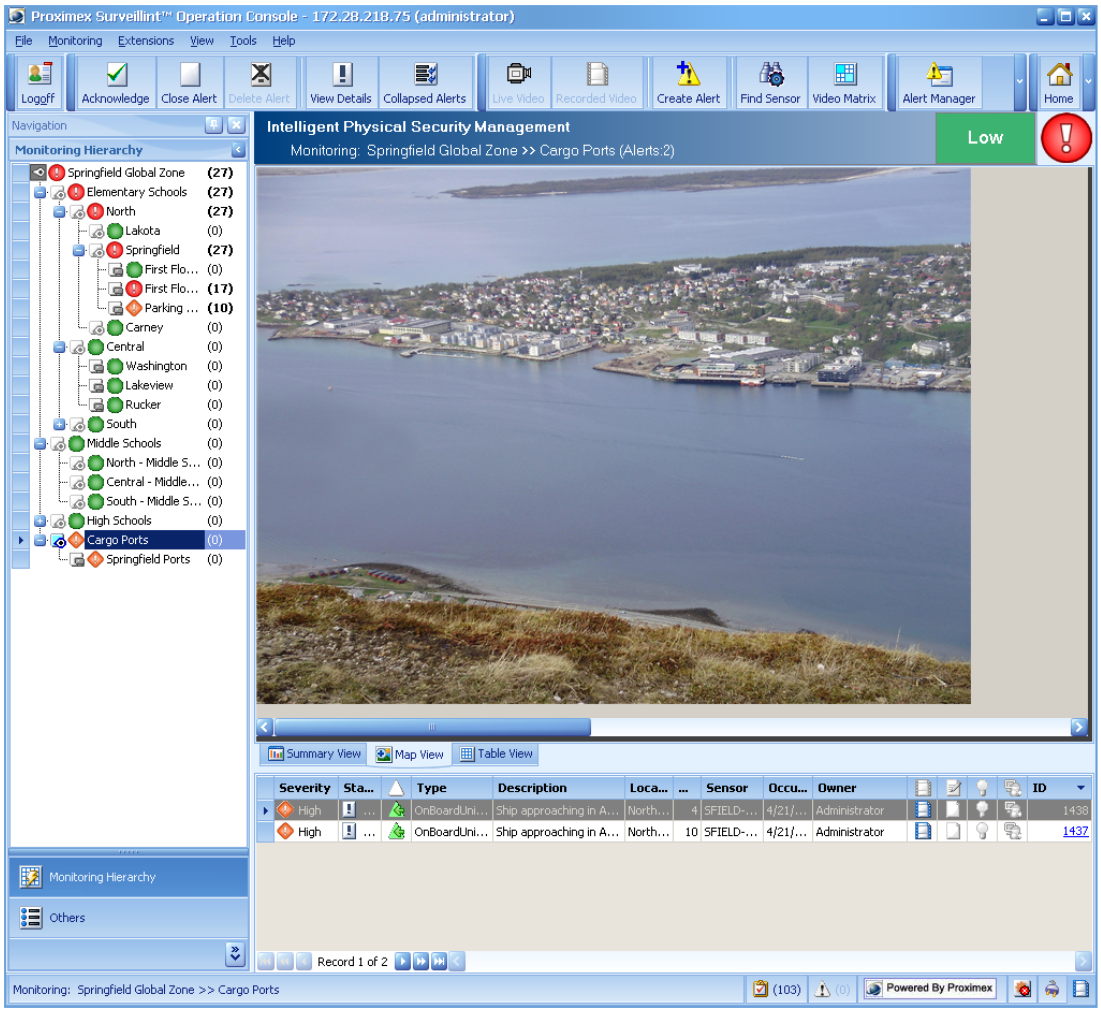
Surveillint connects disparate information to mitigate risk across an enterprise by providing actionable intelligence, speeding security incident resolution, and reducing security operations costs.

- Discover—Surveillint manages alerts and tracks suspects to speed incident response time and boost suspect apprehension rates.
- Connect—Surveillint lets operators quickly see all pertinent incident information and links incidents that seem unrelated, leading to effective resolution.
- Resolve—Surveillint helps companies create rules for security incident resolution according to company policies. To complete the resolution process, Surveillint provides automated, yet configurable, reporting to generate reports fast while reducing the risk of errors.

Centrally Monitor and Control Security Systems

Surveillint offers a complete picture of all security activity in a single view, in real-time; no longer is it necessary to try to watch all the consoles in the security center at the same time. Multiple resources can also be controlled through the centralized system, as shown in Figure 3-18.

Figure 3-18 Surveillint Window



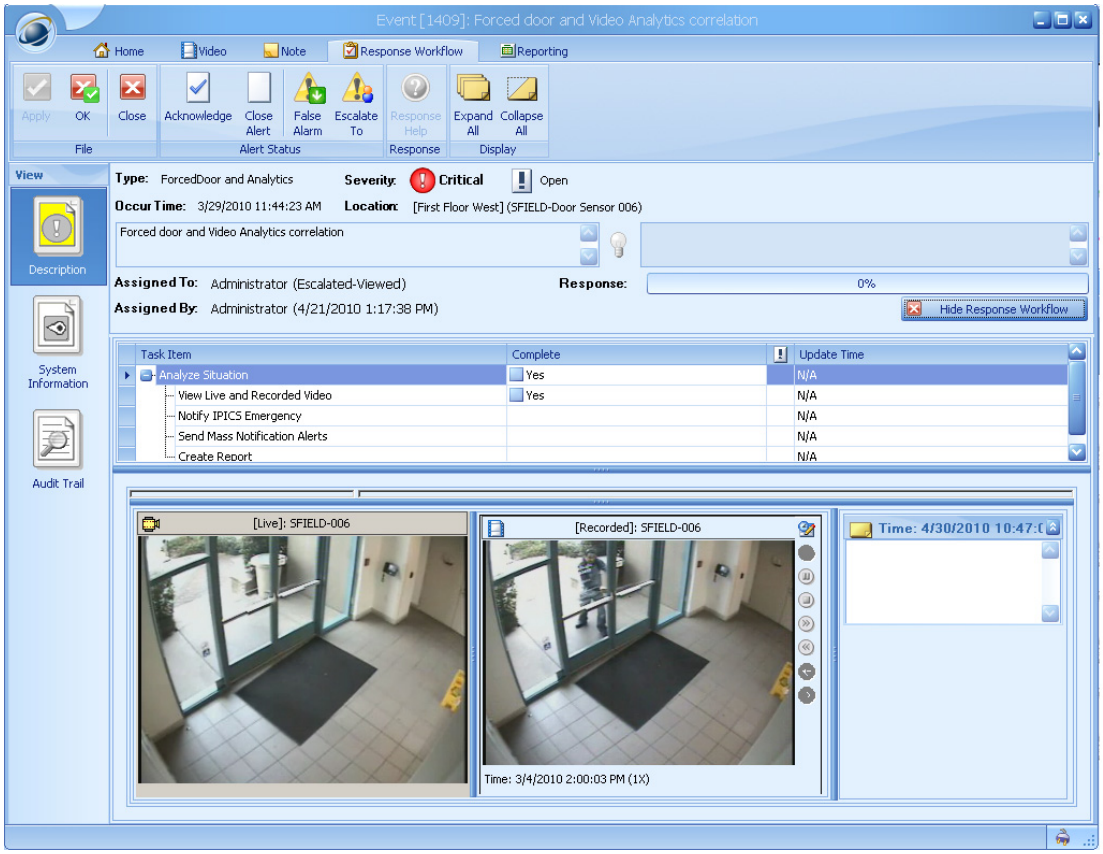
The hierarchical maps enable security teams to find resources and quickly identify the precise location of incidents. Operators can visualize sensor and alert locations, simultaneously view live and recorded video, view asset/external event location displays, and execute sensor commands directly from the map.

- Centralized alert management—The centralized console allows generated alerts to be automatically shown on the maps. Alerts rise to the top so operators can quickly drill from the top map down to the most detailed map.
- Control security sensors, devices, and resources—Interactive maps allow operators to click on a sensor or device and take control directly through the Surveillint interface.
- Sensor integration—Operators are able to view live and recorded video from diverse video systems, take control of PTZ cameras, initiate door commands, and export video directly from the map.
- Security system health—Operators can monitor the health of Surveillint and connectivity to related security systems. If any of the security systems are down or connectivity between the Surveillint server or database and security systems is lost, the administrator can be notified.
- Interactive geospatial maps and tree—Surveillint provides a complete view of facilities, sensors, and alerts in an easy-to-use and intuitive graphical interface. Operators are able to navigate the interactive map by clicking on security zones and areas or by using the hierarchical tree-view.

Incident Assessment and Business Logic

Surveillint automatically displays incident and related information based on the specific security policies and procedures defined by corporate security teams. (See Figure 3-19.)

Figure 3-19 Incident Information



- Alert details—Specific information about the alert, the system that generated the alert and the location on a map.
- Live video—Live video of the event reporting area from one or more cameras and ability to move PTZ cameras.
- Recorded video—Recorded video starting seconds prior (configurable) to the alert from one or more cameras.
- Response tasks and instructions—Instructions for the tasks operators must take to respond to and clear a priority alert.
- Contextual information—Additional information collected from various systems including access control, sensor, badge, and human resource databases to provide a comprehensive understanding of an incident.
- Operator notes—Notes page enables operators to capture observations associated the alert.
- Security system control—Operators can take action on a camera, intercom, security door to temporarily open or lock/unlock a door, or other resource.

- Incident reporting—Security teams create consolidated incident reports (Incident Dossiers) and exported video within minutes. These reports can be used for management reporting or forensic purposes include all alert details, photos, access attempts, mini-maps, and video files. Trending reports are also available for proactive management of resources and systems.
- Business logic engine—Business Logic facilitates capturing and enforcing best practices, building subject dossiers in minutes, as well as taking actions. Flexible decisions and activities can be defined in workflow to automate tedious tasks and capture expert knowledge.

Open Platform for Integration

Surveillint offers an open, flexible platform to service any security environment, and delivers commercial, off-the-shelf (COTS) integration. Designed using Microsoft .NET and service-oriented architecture (SOA), the platform can scale to support thousands of sensors, and can flexibly support any type of security system.

- Integrate with any security system—The Surveillint framework enables easy integration with diverse security systems using standards-based protocols such as XML, ODBC, web services, and so on. With its open systems approach, the Surveillint framework enables an immediate and cost-effective integration of security systems including CCTV, digital video, access control, intelligent video, radar, intrusion detection systems, RFID, enterprise database systems, and virtually any security system.
- Console and communications—The Surveillint intuitive and easy-to-use graphical interface is delivered through the Console and Communications layer, enabling end-to-end incident management and delivery of information through E-mail, PDA, and an open interface with third-party notification and computer-aided dispatch systems.
- Bi-directional communications—Surveillint not only receives real-time data from security systems, but it automatically synchronizes alert updates and issues operational commands to security sub-systems, ensuring efficient incident workflow and management.

Powered by sophisticated rules and workflow engines, Surveillint integrates new and existing security systems into a common platform and serves as the command and control center for a holistic security environment.

AtHoc IWSAlerts

AtHoc IWSAlerts is an enterprise-wide network-centric mass notification system that supports the emergency alerting needs of large, distributed organizations and helps facilitate a safe and effective response. The solution integrates with multiple alerting channels and provides a single, unified web-based console for managing the emergency notification process. This allows facilities to quickly and efficiently communicate a consistent alert to personnel, first responders, senior management, security managers and surrounding communities. The information is sent via multiple and redundant means, including audio/visual alerts to computers and Cisco IP phones, landline and cell phones, PDAs, BlackBerry devices, digital display boards, TV, radio, PA systems and sirens, and more. The system provides bi-directional communication capabilities to capture end user responses and generate real-time reports, providing senior leadership and security operators with an Enterprise Personnel Accountability Picture.

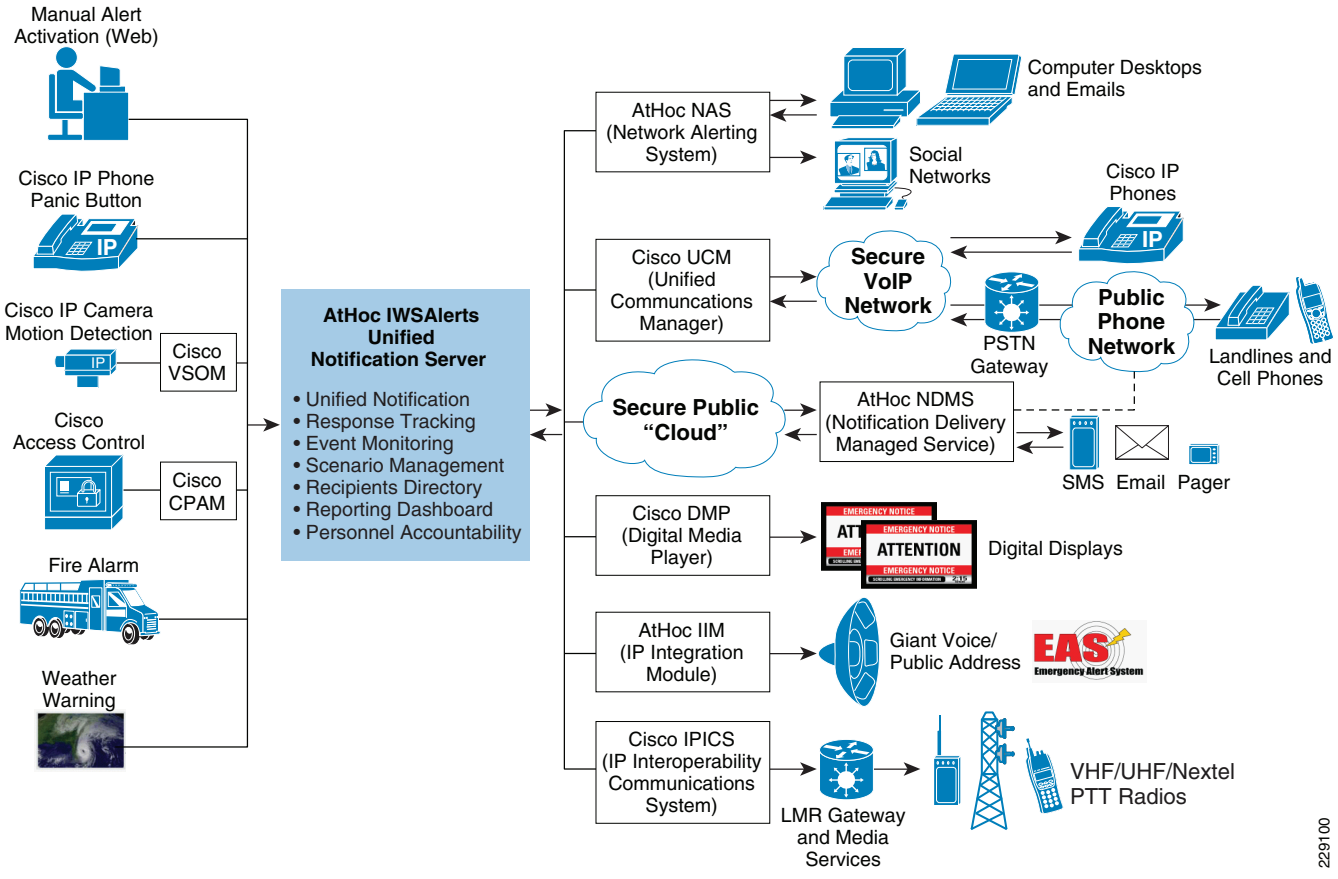
AtHoc IWSAlerts provides several benefits, including the following:

- Transforms an existing IP network into a comprehensive, enterprise-class mass notification system for rapid communication, boundless reach and cost effectiveness

- Unifies all communication channels and devices, including networked computers, land/mobile phones, Cisco IP phone displays, voice telephony alerts to Cisco IP phones and PSTN lines, sirens, display boards, social networks and others, into a single system to simplify activation, ensure message consistency, and reduce alerting time
- Provides an Enterprise Personnel Accountability Picture via real-time response tracking reports for an enterprise-wide view of the status and safety of all personnel
- Provides enterprise capabilities for multi-tenancy centralized deployment to support an entire user population, while providing each remote site its own “private” alerting system
- Manages the emergency notification process across the enterprise by providing pre-defined scenarios, access policies, multi-location support, alert activation flow
- Monitors video feeds, physical sensors and external data sources to automatically trigger notification scenarios
- Ensures continuous accuracy of personnel contact information by integrating with enterprise directories, providing operator user management tools and end user self-service
- Deployment options include both secure private cloud, secure public cloud and hybrid architecture

Figure 3-20 shows the various integrations points into IWSAlerts.

Figure 3-20 Integration Points between IWSAlerts, Event Sources, and Delivery Points



CHAPTER 4

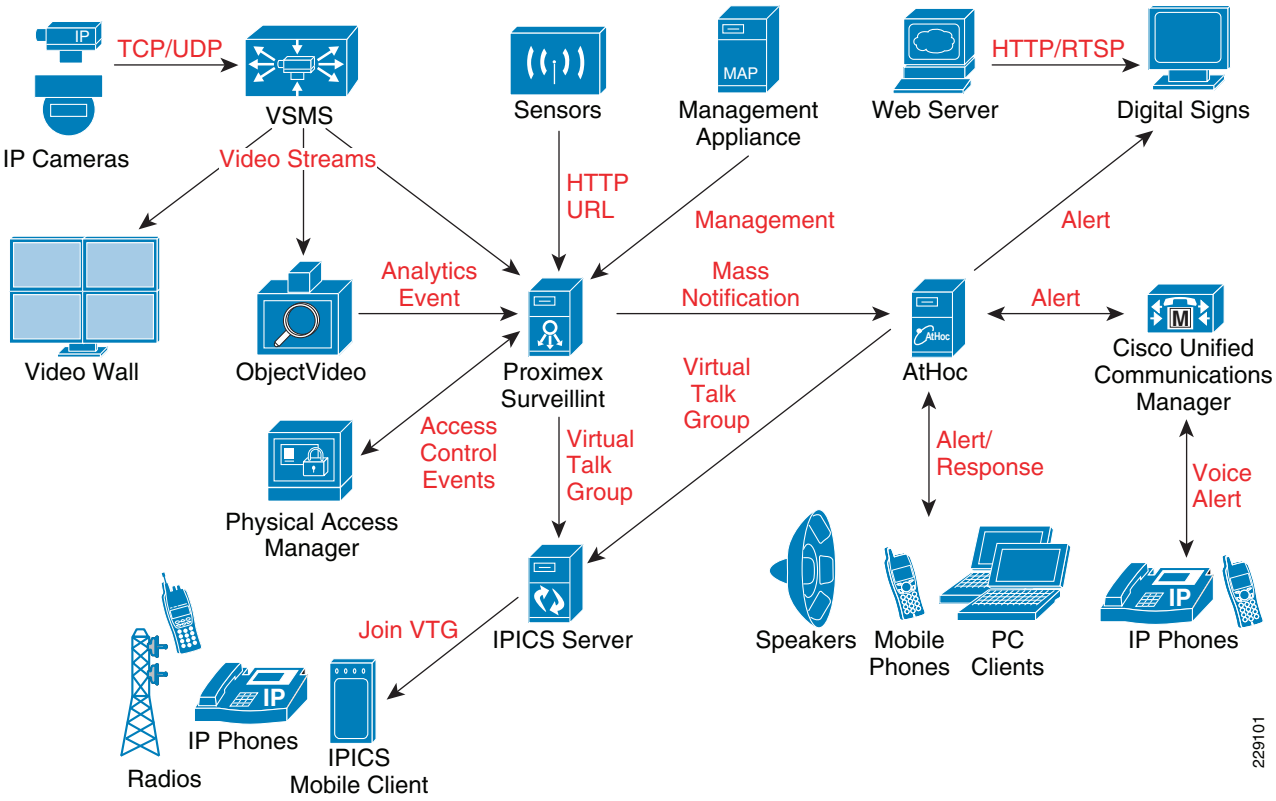
Designing the Solution

Application Traffic Flows

The focus of this release of the Urban Security solution is to integrate various physical security systems using the Cisco IP network as the platform. An open architecture framework enables various solutions to work together and provides the flexibility to integrate solutions from multiple companies. Understanding the various requirements and communication protocols that take place between those systems is critical for successful deployments.

Figure 4-1 shows the various components used in the solution and how they communicate to send/receive alerts and to enhance incident resolutions. In the center of Figure 4-1, the Proximex Surveillint receives events from multiple sources, including the Cisco Management Appliance, sensors, VSMS, ObjectVideo, and CPAM. Surveillint listens to these events and based on an individual event or correlation of the events, it triggers IPICS for first responders to collaborate or triggers AtHoc to quickly send a mass notification to a large number of users and devices.

Figure 4-1 Application Traffic Flows



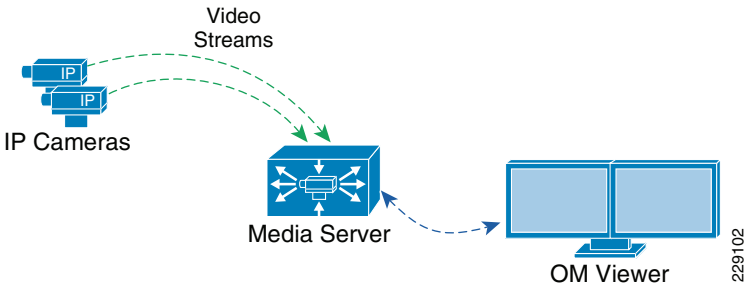
Cisco Video Surveillance

Video Surveillance Media Server

The Video Surveillance Media Server is the core component of the solution, providing for the collection and routing of video from IP cameras to viewers or other Media Servers. The system is capable of running on a single physical server or distributed across multiple locations, scaling to handle thousands of cameras and users.

Figure 4-2 shows how IP cameras send a single video stream to the Media Server. The Media Server is responsible for distributing live and archived video streams to the viewers simultaneously over an IP network.

Figure 4-2 Media Server



For archive viewing, the Media Server receives video from the IP camera or encoder continuously (as configured per the archive settings) and sends video streams to the viewer only when requested.

In environments with remote locations, this becomes very efficient because traffic needs to traverse the network only when requested by remote viewers. Remote traffic remains localized and does not have to traverse wide area connections unless it is requested by other users.

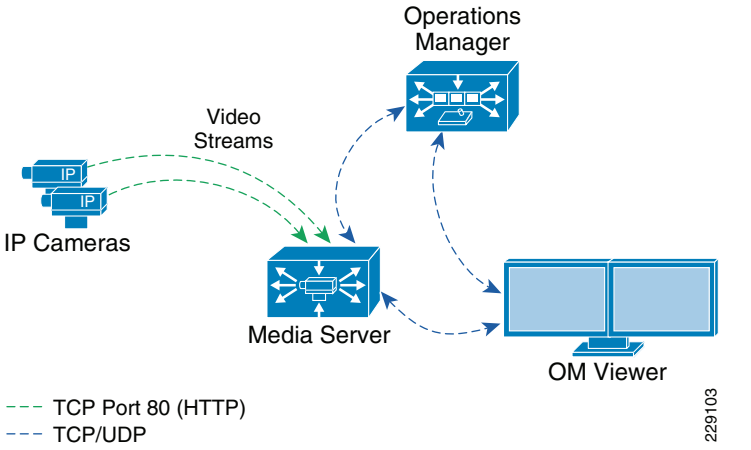
Video requests and video streams are delivered to the viewer using HTTP traffic (TCP port 80).

Video Surveillance Operations Manager

The Operations Manager is responsible for delivering a list of resource definitions, such as camera feeds, video archives, and predefined views to the viewer. After this information is provided to the viewer, the viewer communicates directly with the appropriate Media Server to request and receive video streams. Viewers access the Operations Manager via a web browser.

Figure 4-3 shows the traffic flow of video requested by a viewer.

Figure 4-3 Operations Manager Traffic Flows



After the user authenticates to the Operations Manager, the user is presented with a list of predefined views, available camera feeds, and video archives, based on defined access restrictions. From this point forward, the user interacts directly with the Media Server to retrieve video feeds. The connection remains active until the OM Viewer selects a different video feed.

The Media Server acts as a proxy between the camera and the viewer, who receives video feeds over TCP port 80 (HTTP). If another OM Viewer requests the video from the same IP Camera, the Media Server simply replicates the video stream as requested, and no additional requests are made to the camera (each feed is sent via IP unicast to each viewer).

To allow video streams to flow between the Media Server, edge devices, and viewers, the proper security must be in place to allow TCP/UDP ports to traverse the various subnets or locations.

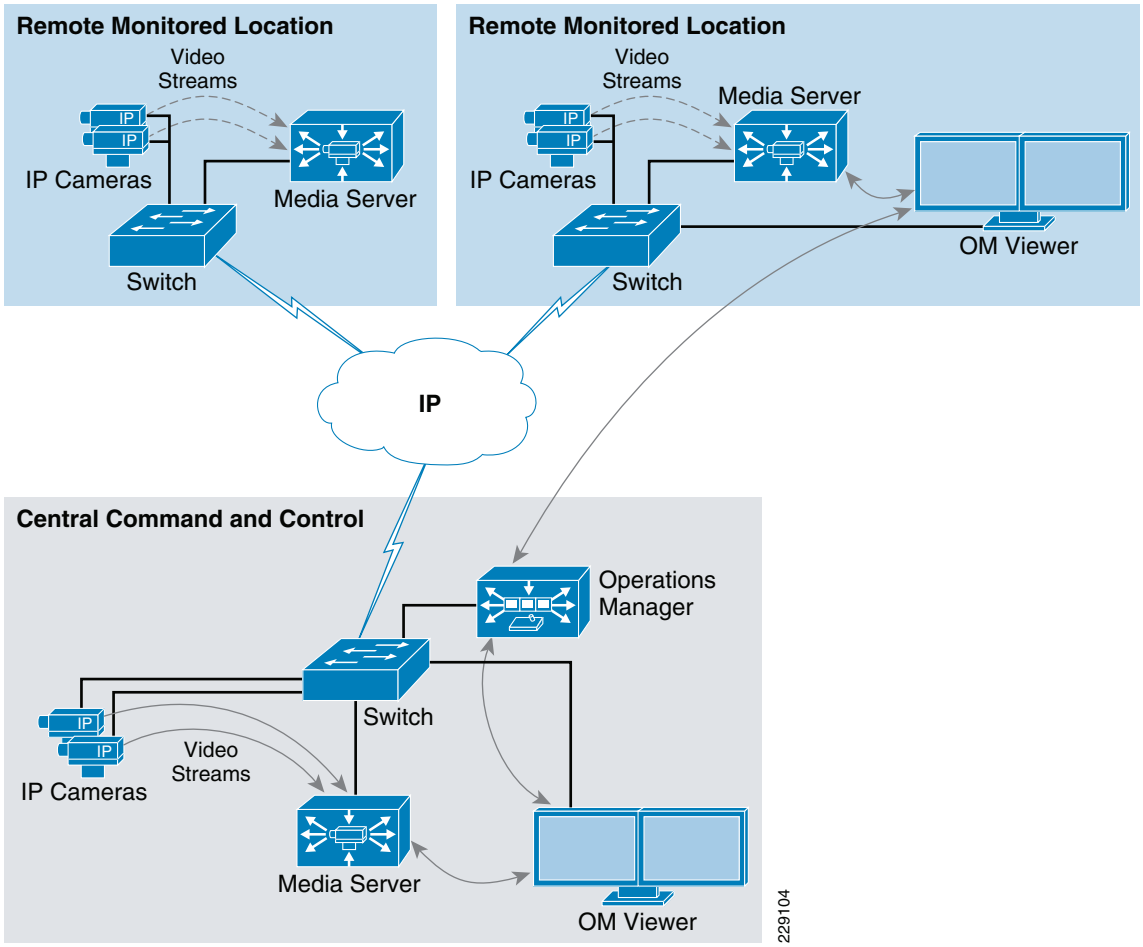
Distributed Media Servers

Figure 4-4 shows a deployment with several remote locations, each with a local Media Server acting as the direct proxy and archive for local IP cameras. In this scenario, all recording occurs at the remote sites and live video streams are viewed by OM Viewers and VM (video walls) Monitors at the headquarters.

OM Viewers can also be installed at remote locations to allow operators to view local camera feeds. The traffic remains local to the site, unless the viewer selects video from remote cameras.

Note A single Operations Manager is able to manage video resources from all locations.

Figure 4-4 Distributed Media Servers



The Media Server at the headquarters can also have parent-child proxies to each remote Media Server and request the remote streams only when required at the headquarters. This would have less bandwidth impact when the same stream is requested by more than one viewer, because the traffic would be contained locally in the headquarters LAN.

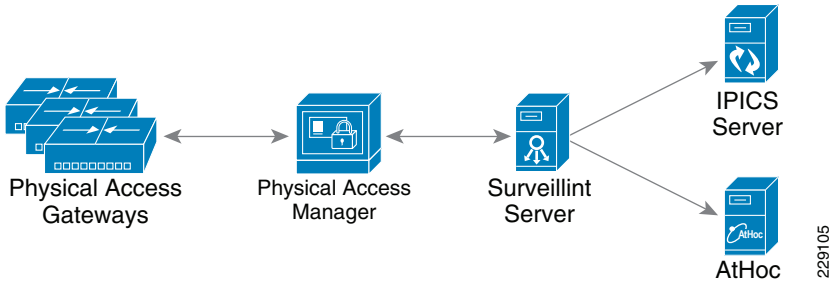
Cisco Physical Access Control

The Cisco Physical Access Control solution benefits from a distributed architecture while lowering deployment and operational costs. CPAM is centrally located at the Command and Control center and is able to manage thousands of gateways installed at remote locations. Through CPAM, a user can configure the policy for any physical access gateway. For example, a main building entrance door may remain locked after hours while it may be unlocked during normal business.

CPAM and Proximex Surveillint

Physical access gateways report an event, such as a forced entry or multiple invalid access attempts by the same card, to CPAM. CPAM can send events to as well as receive actions from other applications. In this design, CPAM sends events to Proximex Surveillint. Proximex Surveillint decides what actions to take based on the alerts it receives. For example, if there is a chemical leak alert in building 1, Surveillint sends “disable access for regular employees for building 1” to CPAM. Figure 4-5 shows the interaction between CPAM and Surveillint.

Figure 4-5 Interaction Between CPAM and Proximex Surveillint



The Cisco Physical Access Gateway and CPAM exchange information through an encrypted protocol over MAN or WAN. While the traffic is light, a QoS policy is required to guarantee this important traffic during congestion.

The CPAM server can have a redundant CPAM server in a Linux high-availability mode so that if the primary server fails, a redundant server is available to continue operations. However, if CPAM fails or the WAN connection goes down, the Cisco Physical Access Gateway continues providing normal card reader access. Also, the gateway will be able to perform the device I/O rules even without CPAM. Therefore, a door forced open or door held open event can cause an output alert to be triggered on the gateway locally.

Other input alerts from the gateway, such as a glass break sensor or duress signal, can trigger the output alert locally. The input alerts trigger the local output alarm using the device I/O rules similar to the door forced open example.

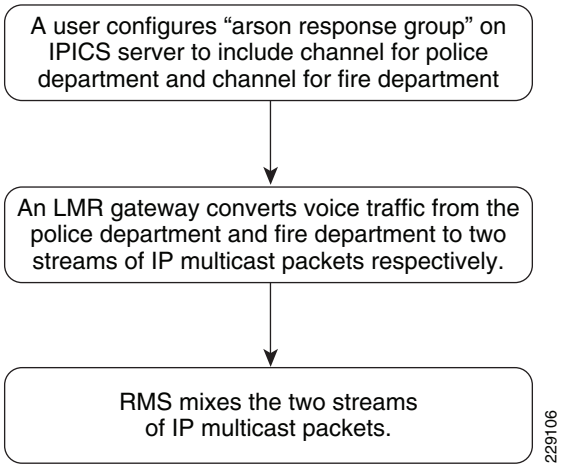
IPICS

This section includes specific functions of IPICS components, interactions of IPICS components, difference between policy and incident response, and high availability.

Specific Functions of Each IPICS Component

The IPICS solution is modular and each component performs a specific function. The gateway converts radio frequency to IP multicast packets, at which point the RMS mixes these packets so they can be transported over the WAN. IPICS servers control which packets are converted or mixed, and configures RMS dynamically according to the virtual talk group (VTG) configured by a user. Figure 4-6 shows the functions performed by each component.

Figure 4-6 Specific Functions of each IPICS Component



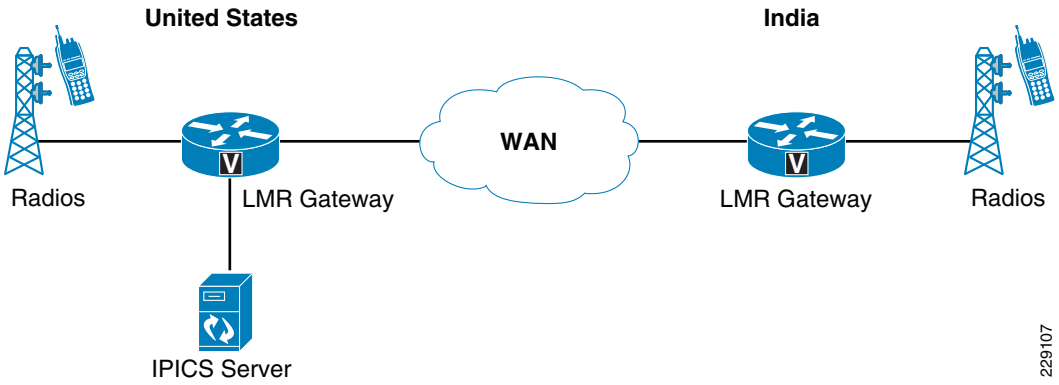
Select Components for IPICS

The functions that a customer chooses determine what components are needed. The list includes an IPICS server, an LMR gateway, RMS, and Cisco Unified Communication Manager (CUCM). Three scenarios are depected below.

Scenario 1—Radios at Two Locations Need to Communicate

If a customer has two sites located in Boston and Bangalore, and the radios communicate over the same channel, only an IPICS server and LMR gateways are needed, as shown in Figure 4-7.

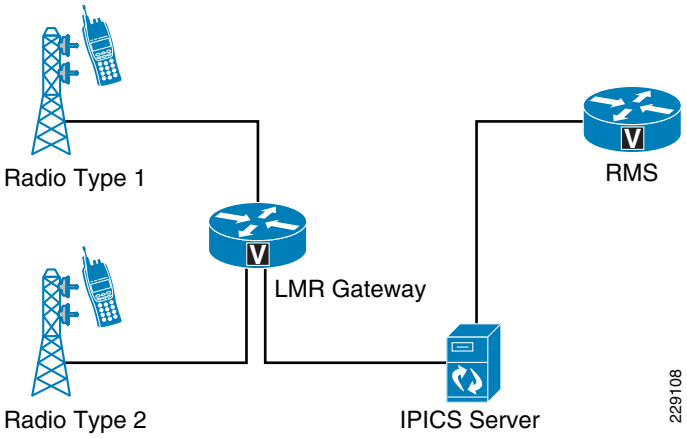
Figure 4-7 Radios at Two Sites



Scenario 2—Multiple Channels

If more than one channel is used, a virtual talk group is required, as shown in Figure 4-8. Various types of radios with unique frequencies go through the LMR gateway. The various frequencies of the radios are converted to IP multicast packets. RMS mixes them into one virtual talk group.

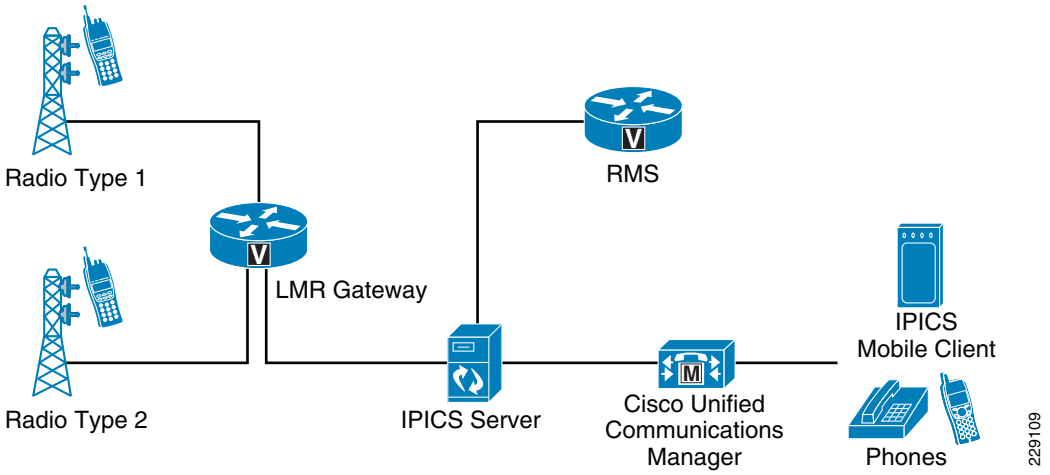
Figure 4-8 Virtual Talk Group Consists of More than One Channel



Scenario 3—Push-to-Talk Service of Various Types of Phones

Push-to-Talk (PTT) is required for this communication scenario, as shown in Figure 4-9. To support land lines and cell phones, the dial engine option is required.

Figure 4-9 PTT Service of Various Types of Phones



Interaction of IPICS Components

IPICS server is the primary component required for deployment. It drives the interaction with the LMR gateway, RMS, and CUCM as described below:

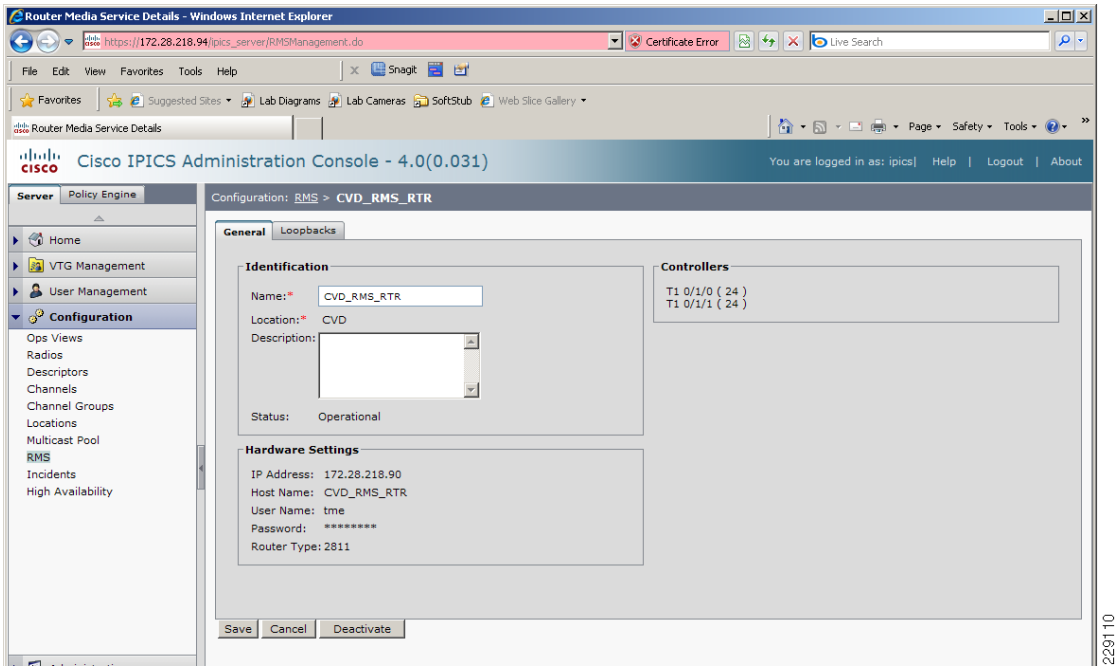
Step 1 IPICS server and the LMR gateway configuration:

On the LMR gateway, configure a multicast address for each channel. On the IPICS server, configure the same multicast addresses. It is not necessary for the IPICS server and LMR gateway to know the address of the other device.

Step 2 IPICS server and RMS configuration:

On the IPICS server, configure how the authentication type for the RMS router, as shown in Figure 4-10. The RMS router does not need to know the IP address of the IPICS server.

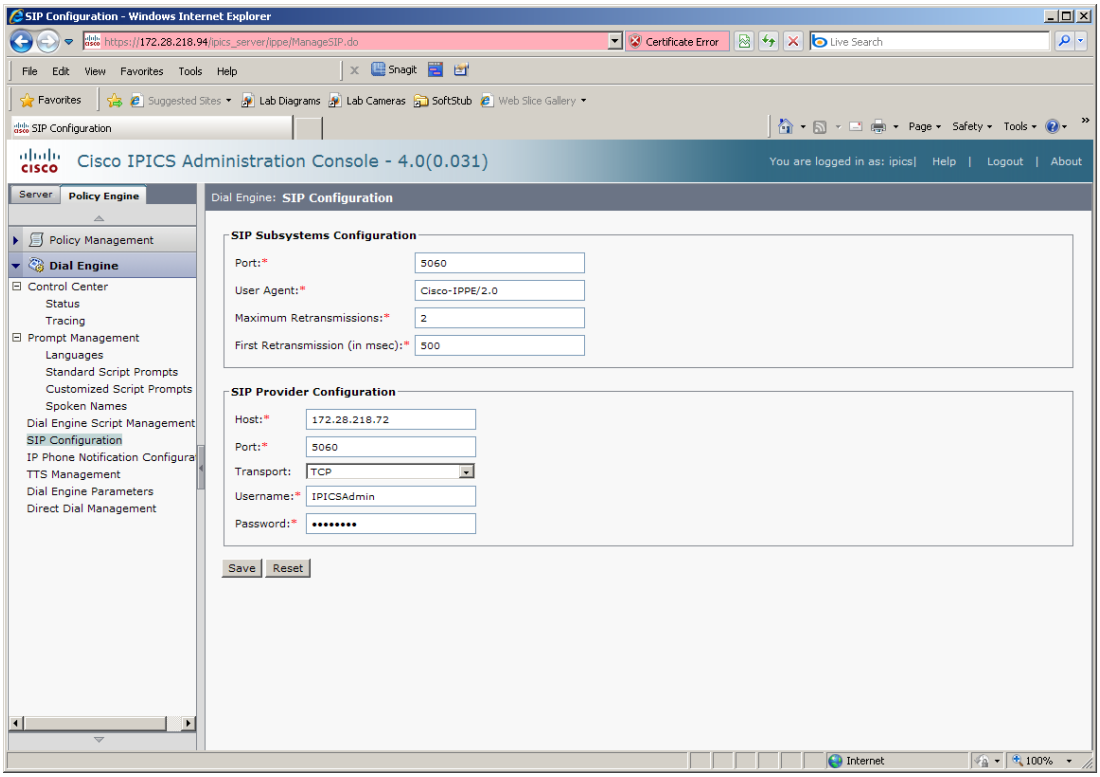
Figure 4-10 Configure IPICS Server for RMS Authentication



Step 3 IPICS server and CUCM configuration:

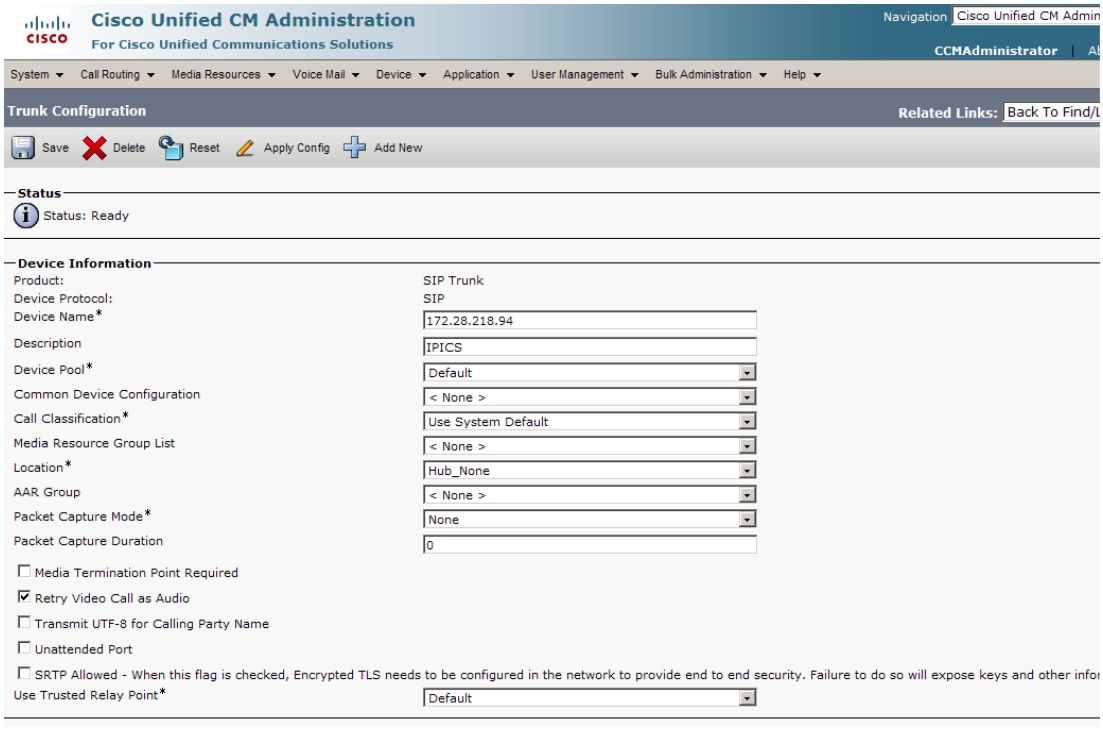
The IPICS server and the CUCM system need to be configured with the proper IP address of the other device. Configure the IP address of CUCM on the IPICS server under “Dial Engine”. See Figure 4-11.

Figure 4-11 Configure CUCM Information on IPICS Server



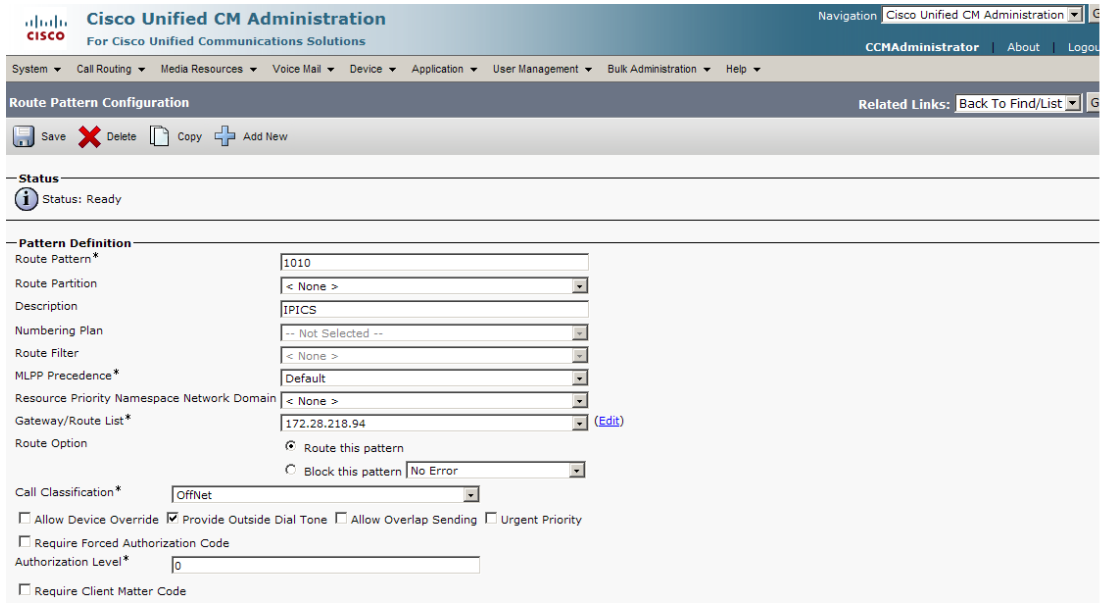
Step 4 In CUCM, create a SIP trunk and point to the IPICS server. See Figure 4-12.

Figure 4-12 Configure IPICS Server Information on CUCM



Step 5 In CUCM, create a Route Pattern. Figure 4-13 shows that extension 1010 has been created for IPICS.

Figure 4-13 Create Route Pattern for IPICS in CUCM



When a user dials extension 1010, a SIP trunk to the IPICS server is created. When a user picks up the extension, an interactive voice response (IVR) will announce *"This is IPICS calling. Please enter your credentials"*. After the user enters user ID and PIN, it will announce that the user has joined VTG "first responder", then instructs the user to "*press 1 to talk*; *press 2 to listen*".

Deployment Models

Deployment models includes single site models and multiple site models, depending on whether a WAN is used or not. For more details, refer to the Cisco IPICS Deployment Models section of the IPICS SRND listed in Appendix A, "Reference Documents."

For smaller deployments, the LMR gateway and RMS typically reside in the same router. For large deployments, a best practice is to separate the functions.

If there are small numbers of radio, the LMR gateway can be installed in the data center. Otherwise, the LMR gateway should be installed near the radios. An LMR gateway can support up to six ports. Each port supports one channel. For each channel, there can be hundreds of unique end-user devices.

Use Remote IDC

In IPICS 4.0, a user can use IPICS dispatch console (IDC) installed on a laptop to interact with other radio and phone users. IDC replaces the previous Push-to-Talk Management Center (PMC) client on IPICS 2.2. In normal use, users in the field use mobile devices (a radio or a phone) while an operator uses an IDC. The IDC has two phone lines. An operator can use it to call a security officer's mobile phone and then transfer the officer's line to a talk group. The operator can upload video, the same as a user with a mobile phone.

A user working outside the multicast domain can still be included in the calls. In this case, the user would VPN into the network and RMS converts the unicast packets from this user to multicast IP packets. This is called *Remote IDC*.

Policies and Incident Responses

A user can configure a policy on the IPICS server to specify a talk group for an incident. The policy can be triggered by other applications, such as Proximex Surveillint. Configuring a policy for each type of incident allows fast response. For example, for fire, configure a policy to include the fire department and a dispatcher in the talk group; for chemical detection, configure a policy to include chemical response personnel and a dispatcher in the talk group. However, the policy-driven talk group does not allow to add additional first responders or allow video upload. The solution is to use policy and incident response at the same time. For instance, when a chemical detection policy is triggered automatically, the dispatcher creates an incident response and adds the current talk group. From that point, more people can be added to the talk group, and video sharing is also allowed.

An alternative is to report all incidents to a dispatcher. According to a specific incident, the dispatcher executes a policy or selects a collection of videos, sensor events, and access events, and then creates an incident response that displays on the IPICS Dispatch Console and pushes out to the Mobile Client.

Multicast, Quality-of-Service, Security

Multicast needs to be enabled to run IPICS. Cisco recommends using bidirectional PIM for Cisco IPICS. If the IPICS dispatch console is connected over a Wi-Fi, the Wi-Fi network does not need to support multicast.

Quality-of-Service (QoS) is recommended in LAN and WAN environments for high quality VoIP using the following best practices:

- Classify voice RTP streams as expedited forwarding (EF) or IP precedence 5 and place them into a priority queue on all network elements.
- Classify voice control traffic as assured forwarding 31 (AF31) or IP precedence 3 and place it into a second queue on all network elements.

In addition, IPICS 4.0 supports video sharing among users. For QoS on real-time streaming traffic, see the Network requirements section in the *Cisco Digital Media Suite 5.2 Design Guide for Enterprise Medianet* at http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/DMS_DG/DMS_DG.html.

Integration between the IPICS server and RMS and integration between the IPICS server and CUCM are password protected. Triggering IPICS also requires authentication.

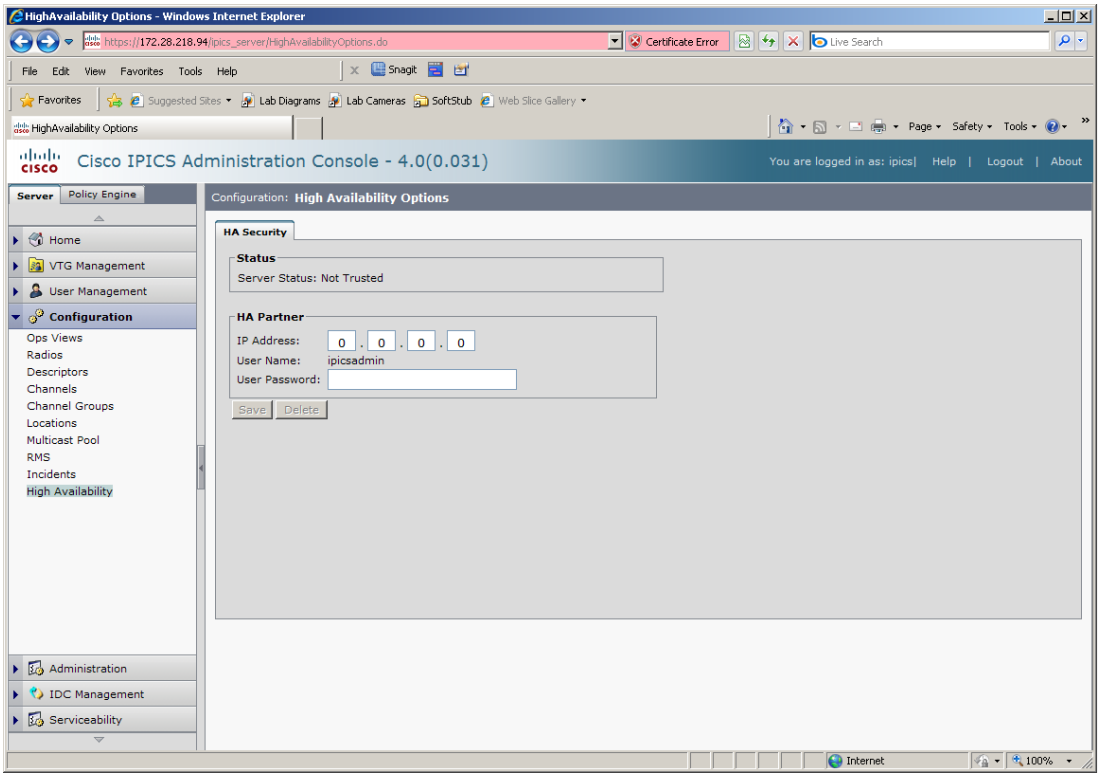
For details on multicast, QoS, and security, refer to the "Cisco IPICS Infrastructure Considerations" chapter in the IPICS SRND listed in Appendix A, "Reference Documents."

High Availability

High availability (HA) has not been tested in this solution. This section provides an overview and points to related documents. To achieve HA, a secondary IPICS server and a secondary RMS are deployed. Because there is no redundant LMR gateway, a key first responder should be equipped with a radio and a cell phone. If the LMR gateway is down and the radio cannot be used, this person can use the PTT service of a phone, practically using a phone as radio. Because there is no redundancy for the LMR gateway, it should be monitored (for example, Cisco MAP), so that an alert can be generated in case of failure.

IPICS 4.0 supports HA of the IPICS server. If there is more than one data center, a secondary IPICS server should be placed in the secondary location. This ensures recovery not only from hardware failure of the primary IPICS server but also from a building failure (such as a power loss). To configure HA for IPICS, a user specifies the IP address of secondary IPICS server, as shown in Figure 4-14. The IPICS servers periodically synchronizes configuration changes. When there is no heartbeat from the primary server, the secondary server takes over.

Figure 4-14 Specify Secondary IPICS Server



For RMS HA, see the ection “Redundant RMS Configuration” in the “Cisco IPICS Infrastructure Considerations”chapter of the *Solution Reference Network Design (SRND) for Cisco IPICS* (listed in Appendix A, “Reference Documents”).

For IPICS compatibility with CUCM, IP phones, applications, see http://www.cisco.com/en/US/products/ps7026/products_device_support_tables_list.html.

Digital Media Player

Digital Media Players (DMP) decode and display unicast VoDs and multicast live streamed video as well as Flash content. DMPs connect directly to large format displays through HDMI. Other output connections are available but normally not used. DMPs may be centrally controlled by a Digital Media Manager (DMM) or can be used in a standalone mode, receiving content directly from a Web Server.

DMP Specifications

Table 4-1 shows the different capabilities and differences between two Cisco DMP models: the 4305G and 4400G.

Table 4-1 Cisco DMP Models—4305G and 4400G

	4305G	4400G
Jitter Buffer	• 4 MB • 1500 ms for multicast	• 5.5 MB • 1500 ms for multicast
Multicast Support	IGMP v3	IGMP v3
Video Support	• MPEG-2 • MPEG-4 Part 2	• MPEG-2 • MPEG-4 Part 10 H.264 • WM9/VC-1 (VoD only)
Bandwidth Required	• MPEG-2 • SD—3 to 5 Mbps • HD—13 to 25 Mbps	• H.264/WM9 • SD—1.5 to 5 Mbps • HD—8 to 25 Mbps
Flash Application Support	Flash 7	Flash 10

- Jitter buffer—The jitter buffers in the DMPs are sufficient to deal with even extreme cases of jitter for live streams. The only reasonable scenario for failures resulting from exceeding the jitter buffer is when the jitter from streaming HD VoDs exceeds 1000 ms. A properly designed network should not allow this threshold to be exceeded.
- Multicast support—The DMPs join multicast MPEG-2 and H.264 streams as the only method of displaying live streaming video. DMPs support Internet Group Management Protocol (IGMP) v3, although a multicast source cannot be defined when defining multicast streams or channels within the Cast interface. This means that source-specific multicast cannot be fully implemented directly from the DMPs, and that all multicast join messages are sent as (*,g) messages.
- Video support—The following are common video formats:
  - MPEG-4 Part 2—A video compression technology developed by the Moving Picture Experts Group (MPEG). It belongs to the MPEG-4 ISO/IEC standard (ISO/IEC 14496-2). It is a discrete cosine transform compression standard, similar to previous standards such as MPEG-1 and MPEG-2. Several popular codecs, including DivX, Xvid, and Nero Digital, are implementations of this standard.
  - MPEG-4 Part 10 (H.264)—H.264 is a standard for video compression, and is equivalent to MPEG-4 Part 10 or MPEG-4 for advanced video coding (AVC).
  - WMV9/VC-1—Windows Media Video 9 (WMV9) is a common Windows media format now supported for VoD playback only. WMV9 supports variable bit rate, average bit rate, and constant bit rate, as well as several important features including native support for interlaced video, non-square pixels, and frame interpolation.

  These formats are supported by the various Cisco DMPs as follows:
  - Cisco DMP 4305G—Supports standard MPEG-2 streams (HD or SD) as well as the rarely used MPEG-4 Part 2. DMP 4305G does not support H.264.
  - Cisco DMP 4400G—Supports standard MPEG-2 streams (HD or SD) as well as MPEG-4 Part 10, also known as H.264. WMV9 is also supported for VoD playback only.

  The bandwidth requirements range between 1.5 and 25 Mbps, depending on several factors including whether the video is SD or HD and what codec is used.
- Flash application support—Flash applications are used with Cisco Digital Signs to display content. The DMP 4400G introduces Flash 10 support, while the 4305G is limited to Flash 7.

Bandwidth Requirements

Digital Signs use the DMP to deliver live and pre-recorded streaming content to displays. Bandwidth used per stream is 1.5 to 5 Mbps for standard definition streaming video content, and 8 to 25 Mbps for high definition streaming video content. With Cisco Digital Signs, streaming video content may be placed on a portion of the screen, with the remaining screen being used by Flash or media content such as information tickers, advertisements, images, or any other non-streaming content supported by the DMPs.

Video resolution can be reduced for partial coverage of the screen. Reducing displayed video resolution allows the reduction of encoded stream resolution, lowering the bandwidth requirements.

Latency Requirements

For live streaming content, moderate latency does not have a significant impact. Significant latency is rarely encountered with the large multicast streams sent to the DMPs because they are normally implemented in a campus environment.

For pre-recorded video content, moderate latency does occur. Pre-recorded content is streamed through HTTP or RTSP-T, with large bandwidth demands because of the TCP mechanisms for transport. This process reduces the throughput maximum as latency increases, regardless of how much bandwidth is available.

With TCP parameters set to optimal levels, tolerances for latency are still quite stringent because of the throughput needed. For SD video, latency must be less than 100 ms round trip. For HD video, latency must be less than 60 ms round trip. Delay beyond these thresholds causes the TCP data stream to slow because of the two-way acknowledgement-based communication.

Packet Loss Requirements

For live streaming content, lost packets are not retransmitted, and with the amount of compression used by the video codecs, even a single packet lost results in degraded video quality. Avoiding any packet loss is the highest priority for live streaming video. With certain configurations, packet loss of 0.001 percent may be considered unacceptable over an extended period of time.

The avoidance packet loss is the single most important factor when implementing live video with Cisco Digital Signs. Any packet loss may be visible and severely impact the video and audio quality of all DMPs experiencing that packet loss.

ObjectVideo

ObjectVideo monitors video feeds for events and generates alerts in real time as events take place. The ObjectVideo Intelligent Sensor Engine (ISE) server receives the video feeds from the Media Server for monitoring through the available DirectShow filter. The components listed below could be run on the same or on separate machines. Components talk with each other through the communication layer provided by ObjectVideo Communication Daemon software.

Server software:

- ObjectVideo Server—The ObjectVideo Server software routes information among the components. The ObjectVideo database stores alerts and other system data and is typically installed on the same machine as ObjectVideo Server.
- ObjectVideo ISE—The ISE software runs on a server that meets the ObjectVideo recommended minimum hardware requirements. Video is fed to the ISE "sensors" to process the video stream in real time and monitor the video for events based on the rules defined. Once the Cisco 4500 Video Surveillance IP Camera supports the embedded analytics, the overall server count will be reduced, providing more flexible deployment architectures.
- Alert Bridge—The Alert Bridge software is the service that runs URL forwarder plug-in which enables real-time http triggers to VSOM.

Client software:

- Alert console—The Alert Console displays alerts as events occur and allows for searching of alerts.
- Rule management tool—The Rule Management Tool is used to set up rules for the sensors. The rules define the security policies that, when violated, generate events.

Figure 4-15 shows how video feeds from IP cameras are sent to the Cisco Media Server for live viewing and archival. The ISE server in turns analyzes the video streams for specific events and generates alerts.

Figure 4-15 System Components

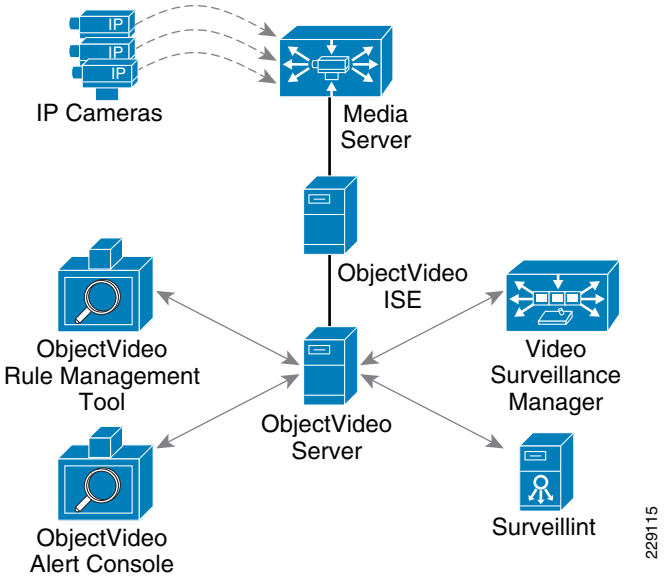
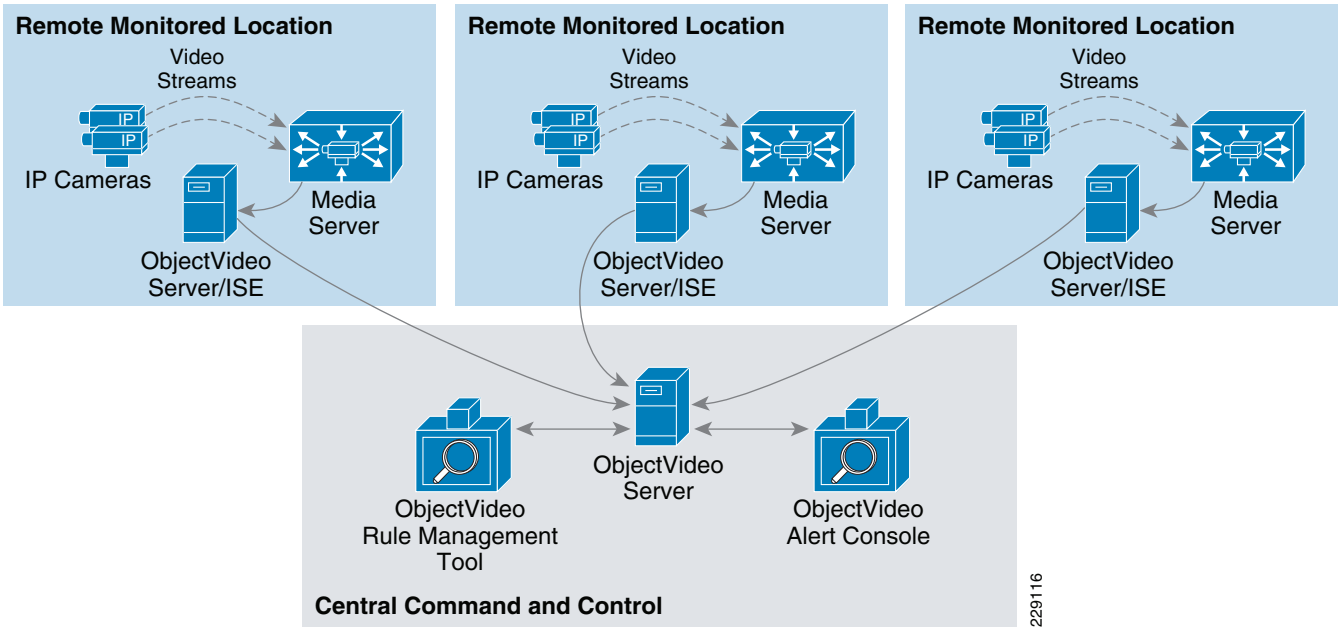


Figure 4-16 shows how servers may be deployed to support a large number of locations. In this case, video feeds are analyzed by each local ISE server and when alerts are generated, they are sent to the central command and control location, where alerts may be reviewed or sent to other systems, such as Proximex Surveillint or VSOM.

Figure 4-16 Multi-site Deployment



ObjectVideo provides several applications that provide guidance for planning and maintaining an ObjectVideo system. These tools include the following:

- ObjectVideo Integrator Toolkit—The ObjectVideo Integrator Toolkit contains several software applications used by customer support personnel and integrators to plan for, maintain, and troubleshoot the ObjectVideo system. The ObjectVideo Integrator Toolkit applications are also used to improve event detection and reduce false alarms.
- Camera Placement Tool—Used to determine the ideal camera location and settings to optimize event detection.
- Object Sizing Tool—Used to determine the size (in pixels) of objects within a camera's field of view. It allows you to determine whether objects of a certain size will be reliably detected by a sensor.
- Parameter Configuration Tool—Used during advanced troubleshooting tasks to improve event detection. The Parameter Configuration Tool allows you to access parameters that determine how events are detected by each sensor. The Tool is also used for some advanced configuration tasks.

Video Feed Requirements

By default, ObjectVideo software processes video at QVGA or CIF (NTSC or PAL). Other sizes are also supported; however, processing larger video frame requires more resources. IP video is being processed using DirectShow multimedia framework.

Table 4-2 shows the recommended system options for ObjectVideo deployments. The number of sensors or channels supported by a server is critical when designing new systems.

Table 4-2 System Recommendations

Form Factor	CPU	RAM	Number of Sensors per ISE Server
Desktop	Intel Core 2 Duo E6550 • 2.33GHz • L2 4MB Cache	3 GB	8
Rack Mount Server	Intel Dual Core Xeon 5140 • 2.33GHz • L2 4MB Cache	2 GB	8
Desktop	Intel Core 2 Quad Q6600 • 2.4GHz • L2 8MB Cache	3 GB	12
Rack Mount Server	Intel Quad Core Xeon E5420 • 2.5 GHz • L2 12 MB Cache	3 GB	12

Proximex Surveillint

Proximex Surveillint serves as central command and control center of the security environment. It integrates information and data from each component of the Cisco physical security solutions suite, including Cisco Video Surveillance Manager, Physical Access Manager, Cisco IPICS, and ObjectVideo. Surveillint provides an open platform to enable new technologies and systems to be integrated together as needed.

Surveillint's solution includes several components that may be distributed to provide a highly available environment to support a large number of users and locations.

Server Software

Server software may be run on a standard Microsoft Windows server or on fault-tolerant servers. Surveillint can also run in a warm or hot-standby configuration providing redundancy and high availability. Additional servers can be added to provide this level of redundancy and failover.

Client Software

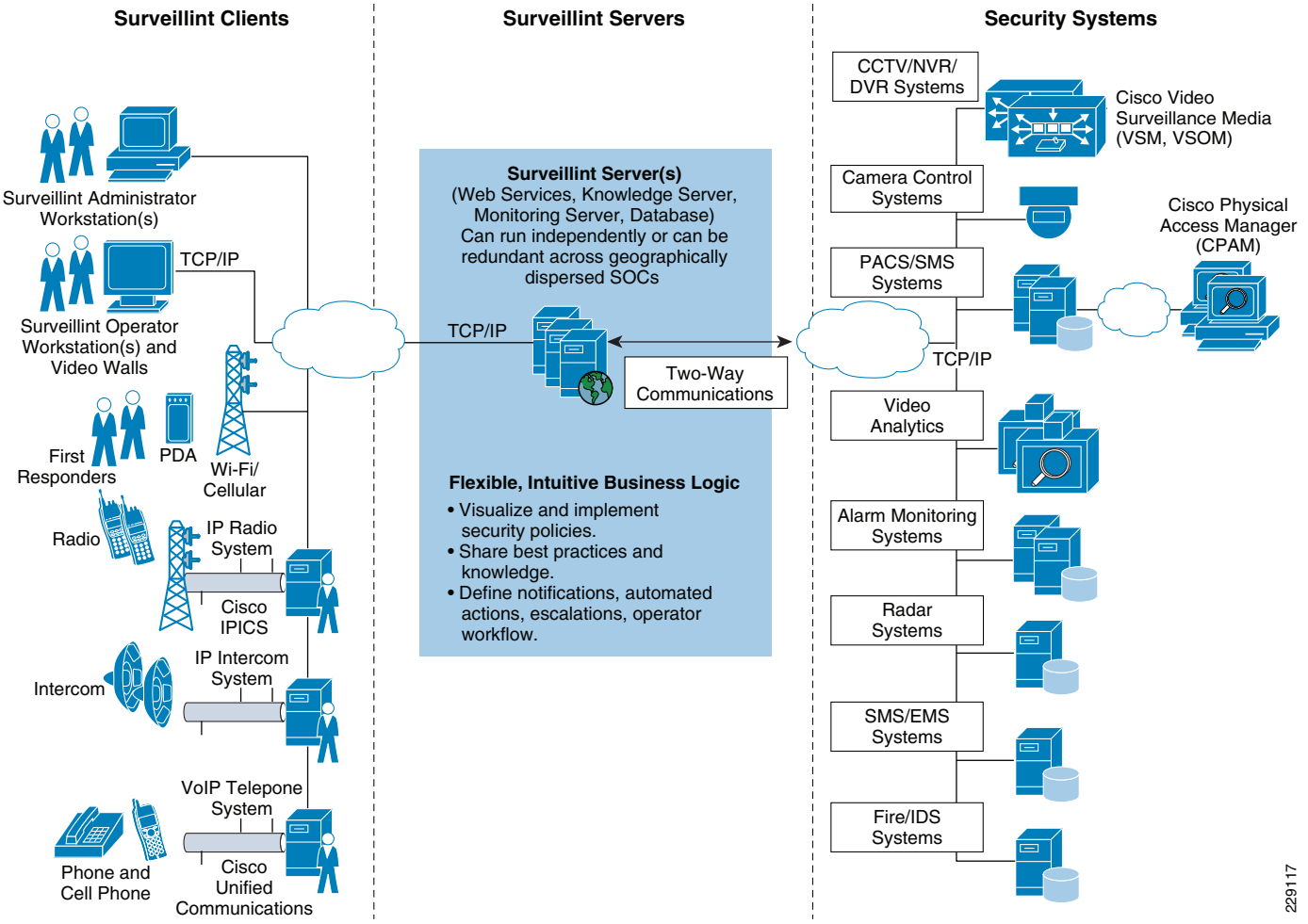
Multiple clients can be operated simultaneously with a server.

- Operator client
- Administrator client
- Windows Mobile PDA client

Integration Modules for Connecting with Subsystems

In addition to integrating with Cisco physical security systems, Proximex offers a library of more than 90 Integration Modules, supporting different manufacturers and models of video systems, access control systems, IT health monitoring systems, fire systems, intrusion alert systems, video analytics systems, intercom systems, computer-aided dispatch (CAD) systems, intercom systems, radar systems, sonar systems, chemical/biological sensor systems and more, as shown in Figure 4-17.

Figure 4-17 Integration Modules



Because Surveillint supports Cisco physical security technologies, a fully integrated security solution significantly improves information sharing between Cisco technologies and other related systems as part of the security ecosystem.

High Availability

Surveillint's Web Services-based Service-Oriented Architecture using Microsoft .NET technology provides operational redundancy across all of its components. To provide high availability, Surveillint supports a redundant multi-site and multi-hierarchy architecture. The redundancy is achieved by:

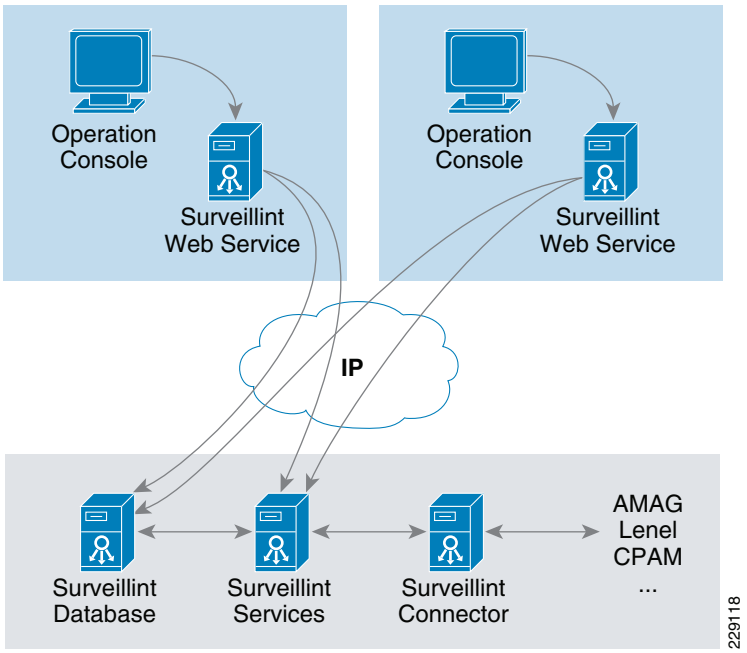
- Database redundancy—Microsoft SQL Server 2005 or 2008 failover cluster and/or database mirroring solution for SQL Server 2005 or 2008 can be used. Additionally, the Surveillint user interface communicates with the backend components using web services, which can be configured to automatically connect to another database if there is a problem with the main database. The backup database server can be at either the local site or a remote site.
- Web services redundancy—Surveillint's middleware components are also built on web services that can be set up to run on multiple computers for redundancy and scalability.
- Application server components redundancy—A cluster server approach (such as either the NEC ExpressCluster or Microsoft Cluster Server) can be used for any and all Surveillint application server components. Other approaches, such as asynchronous synchronization and scripted failover, can also be used for disaster recovery approaches.
- Stateless user interface component—The user interface component is stateless and multiple instances of the user interface (consoles) can run simultaneously. There is no functional limit to the number of workstations that a Surveillint solution can support. The consoles connect to the redundant web services and failover automatically as required.

Distributing Surveillint Components

Surveillint’s flexible architecture may be scaled from a single server to a large deployment, distributing components across multiple sites.

Figure 4-18 shows how the various server components may be installed in multiple instances to support multiple locations. Multiple Operation Consoles (or Administration Consoles) are supported. Each of these instances points to an instance of the Surveillint Web Service. Multiple instances of the Surveillint Web Service may be installed if required to increase load balancing for servicing requests from the Operation Console.

Figure 4-18 Surveillint Deployment



Multiple instances of the Surveillint Integration Modules may be deployed to service interactions with external systems such as Cisco Physical Access Manager, AMAG Symmetry, Lenel OnGuard, SoftwareHouse CCure, Hirsch Velocity, and so on.

AtHoc IWSAlerts

User Requirements

When designing an AtHoc IWSAlerts solution, the following requirements should be gathered first:

- Number of users to be supported
- Delivery speed requirements
- Type of end devices to be supported
- Whether single site or multiple sites are to be supported, and high availability requirements

Functions of AtHoc IWSAlerts Servers

The AtHoc solution is quite modularized and is comprised of both server- and client-side components. The servers include: IWSAlerts DB server, IWSAlerts Unified Notification System (UNS) Application server and IWSAlerts Notification Delivery System (NDS) servers.

AtHoc IWSAlerts server system configuration is composed of the following three server components:

- Database server using Microsoft SQL Server 2005/2008
- UNS application server(s) serving as a web-based application server and job processing server for all logical frameworks (platform, applications, integration, and delivery)

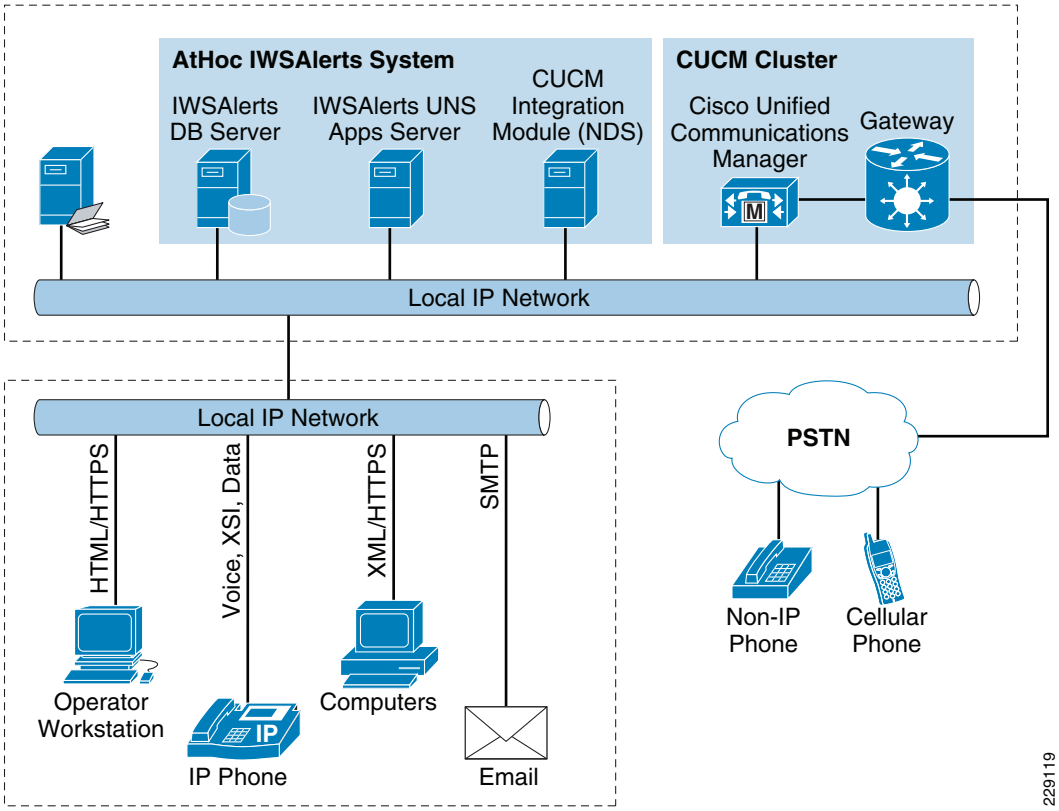
- NDS application server(s) serving as notification delivery gateway function to advanced communication channels, such as Cisco UCM, SMS, or SMTP

A UNS IWSAlerts application server may also be running delivery gateways (NDS) to external delivery systems and services, such as Unified Communication systems or SMTP. The separation to architectural components allows for greater deployment flexibility, depending on customer use case and existing network topology scenarios. In some cases, the NDS function can also be served from the cloud, as a hosted service to provide advanced delivery capabilities.

Although all components can be installed on the same machine, in production environments the database server and the application server are usually separated, and several application servers are deployed in a web farm fashion for scale and redundancy.

Figure 4-19 shows the AtHoc IWSAlerts architecture diagram with CUCM integration.

Figure 4-19 AtHoc IWSAlerts Architecture Diagram and CUCM Integration



In a high availability (failover) architecture, a similar AtHoc IWSAlerts server system will be installed and configured in a remote site, to provide service upon failure of the primary system.

Additionally, AtHoc IWSAlerts architecture contains the following elements:

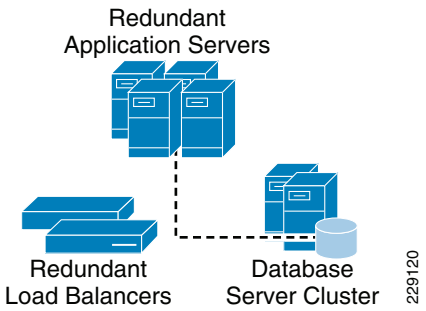
- Communication services—AtHoc provides hosted alert delivery services to deliver voice telephony and text messaging (E-mail and SMS) via scalable and highly available data centers. An account setup and provisioning is required to use the communication services.
- Desktop notifier (NAS)—Small footprint Windows and Mac compatible personal desktop notification application; this component is usually installed on every user computer (desktop, laptop) in the organization using a centralized desktop configuration management system, and provides audio/visual notifications to end users.

- AtHoc IP Integration Module (IIM)—Network appliance allowing integration with legacy non-IP supporting alert delivery systems such as indoor and outdoor public address systems; this component is installed near the interconnected system.

Deployment Models

AtHoc IWSAlerts system architecture is designed to support flexible deployment configurations, answering different needs and customer requirements (see Figure 4-20).

Figure 4-20 Flexible System Architecture



The flexibility is designed in multiple dimensions, covering the IWSAlerts server(s) system, the failover (alternate) system, and the alert delivery (communication) systems.

- Single site-based installation—Hardware and software applications are physically installed at the customer site, and then share specific resources within the organization. Such shared resources may be an Active Directory that is maintained centrally, or centralized telephony alerting capability (i.e., enterprise wide UCM and/or a commercial telephony alerting service).
- Site-by-site with cascading alert capability—Similar to above, but with ability to inter-connect the systems at different sites in a way that “cascades” an alert from one site to another. This capability allows a system based in Virginia to activate a system based in California and vice versa.
- Centralized enterprise—Hardware and software applications are physically installed in a centralized location. The IWSAlerts application is then configured to support multiple local instances (multi-tenancy) of the application which run on the same (centralized) servers, giving each site exactly the same operational control and functionality it would have if they were running it on their own hardware locally.

Scalability

By supporting web farm server configurations, AtHoc IWSAlerts UNS and NDS components cater for scaling up operations, by employing additional application servers to handle service requests and background processes.

Typically, a single AtHoc IWSAlerts system with two dual-quad core CPU application servers can handle up to 20,000 concurrent NAS (desktop alerting) users with a three minute polling period, usually equivalent to 30,000 to 40,000 actual users (considering typical network concurrency rates). In a similar way, such a single IWSAlerts system can handle up to 200,000 users when working with telephony and text alerts.

For very large organizations, more than one AtHoc IWSAlerts system can be installed, while portioning the users serviced by each system. The IWSAlerts inter-system cascade support, the multiple IWSAlerts system can be cascaded to provide single action activation across the organization in a transparent manner. This way IWSAlerts cascaded system can support alerting to hundreds of thousands to millions of users from a single unified console.

High Availability

AtHoc IWSAlerts application server design supports internal redundancy configuration to prevent single point of failure:

- The application servers can be installed in a web farm configuration behind a load balancer, to allow multiple application servers to service incoming requests and process background jobs in a completely transparent redundancy. The application server configurations are completely identical, and if one is down, others take over its service requests. This configuration also allows for greater scalability by distributing load across multiple application servers.
- The database server can be installed in a clustered environment, maintaining internal redundancy for high availability.
- Critical installations use other redundant components to ensure no single point of failure; these include redundant load balancer, IP switches, redundant power supplies from separate power circuits, and internal RAID storage configurations. An advanced high availability configuration uses two or more identical sites, configured in an active-passive manner with online data replication between the sites and active monitoring to start the alternate site operation when a primary site fails.

CHAPTER 5

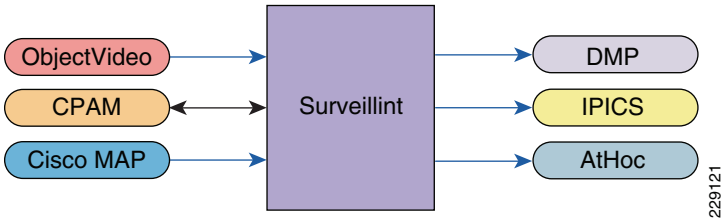
Integrating the Applications

When integrating multiple technologies into a solution, a user needs to select an integration application that is capable of both receiving events from other applications and sending commands to other applications. Today, most technologies (such as CPAM and AtHoc) have this capability. One of these technologies, such as CPAM, can be selected as the integration application if a system consists of only a couple of components. If a system has a large number of components, a dedicated integration application is needed. For example, Augusta EdgeFrontier is used as the integration application in the Physical Safety for Schools solution (see http://www.cisco.com/en/US/docs/solutions/Verticals/Education/safe_sec_ed_dg.html). If the purpose is to manage the day-to-day operations and to be able to bring together information from disparate security systems, a user needs to choose a primary application capable of visualization, correlation, and workflow logic.

After selecting an integration application, a user needs to select the components that interact with the integration application. The components usually interact with the integration application through HTTPS or application program interface (API).

In this solution, the Proximex Surveillint is selected as the integration application. Figure 5-1 shows the interaction between Surveillint and other components in the solution.

Figure 5-1 Interactions between Surveillint and Other Components



As shown in Figure 5-1, ObjectVideo, CPAM, or Cisco Management Appliance (MAP) sends events to Surveillint. Depending on the event type and combination, Surveillint triggers AtHoc, DMP, or IPICS. An event by itself may have low priority, but two events happening within a short time may indicate a severe incident. For example, if ObjectVideo reports motion detected during off hours, and within a couple of minutes Cisco MAP reports a camera failure, this requires immediate attention from a security officer, since the camera may have been damaged by someone about to commit a crime.

Note Underlying technologies are not shown here, including VSMS/VSOM, CUCM, IP cameras, and physical access gateways. Nevertheless, they are integrated components of the solution. For example, CUCM supports the functionalities of IPICS and AtHoc.

The following procedures are recommended for integrating multiple technologies:

Step 1 Select the components and an integration application.

Step 2 Determine whether a component should be placed centrally or at each remote location.

Step 3 Define an IP address scheme for the devices and/or applications.

Step 4 Perform basic functionality tests for each component. For example, for CPAM, a door needs to be created and a door lock can be controlled remotely.

Step 5 Integrate each component with the integration application.

Step 6 Identify the events to be managed and configure correlation logic on the integration application.

Tip Some applications support only Internet Explorer, while others support both Internet Explorer and Firefox. When running into problems with one browser, switch to another browser.

Integration examples are listed in Table 5-1. This chapter is organized such that each example has a section on how to make that product work, then how to integrate that product into the solution. The examples are selected to enable customers to integrate the technologies, regardless of the existing infrastructure or the combinations they decide to use.

Table 5-1 List of Integration Examples

CPAM	CPAM <-> Surveillint -> AtHoc (through Surveillint's business logic)
IPICS	AtHoc -> IPICS
DMP	AtHoc -> DMP
ObjectVideo	ObjectVideo -> Surveillint
Surveillint	Correlation example (CPAM and ObjectVideo <-> Surveillint)
AtHoc IWSAlerts	Surveillint -> Athoc (through manual action from Surveillint's operation console)

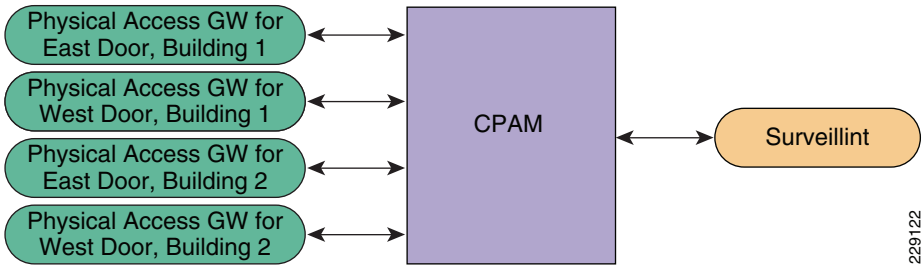
CPAM Integration

Integration with CPAM can be done through the CPAM API or HTTPS. Integration between CPAM and Surveilint is through the CPAM API and the Surveillint CPAM Integration Module.

Integrating CPAM and Surveillint

In the example shown in Figure 5-2, four doors are controlled by a physical access gateway. The gateways connect to the same physical access manager. Surveillint groups each door as a Surveillint "sensor". In this example, Surveillint sees four "sensors", corresponding to the four doors.

Figure 5-2 Four Doors Connected to CPAM



A door may have multiple sensors, such as a "glass broken sensor" or a "chemical detection sensor". These sensors connect to different inputs of the physical access gateway. Surveillint does not distinguish the different sensors from the same gateway (corresponding to a door).

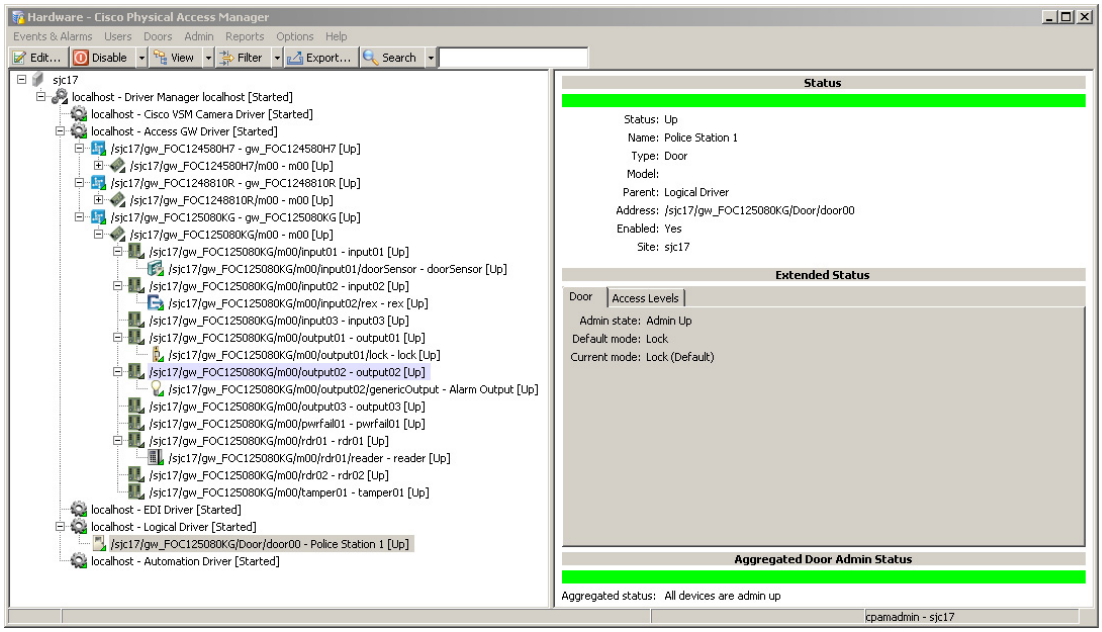
In short, from the perspective of Surveillint, one door equals one Surveillint "sensor".

When Surviellint receives an alert from CPAM, it relies on CPAM to provide the alert description (glass broken or chemical detected) and maps to a system alert for that physical access gateway, such as "for sensor named 'West Door, Building 2', forced entry alert."

Checkpoints Before Integration

Although Surveillint equates a physical access gateway as a "sensor", a door must be created in CPAM before Surveillint can discover the gateway as a sensor. Figure 5-3 shows that a door has been created under the gateway.

Figure 5-3 Door is Created in CPAM for the Gateway



After a door is created, it is possible to test scenarios such as “grant door access” through CPAM and view alerts such as “invalid card access”.

The integration includes the following steps:

Step 1 Establish connection between CPAM and Surveillint.

Step 2 Allow Surveillint to discover all the physical access control sensors.

Step 3 Assign a sensor to a monitoring area and place the sensor on the map.

Step 4 Configure Surveillint to receive alerts from CPAM.

Step 5 Configure Surveillint to send incident notifications.

Establishing the Connection between CPAM and Surveillint

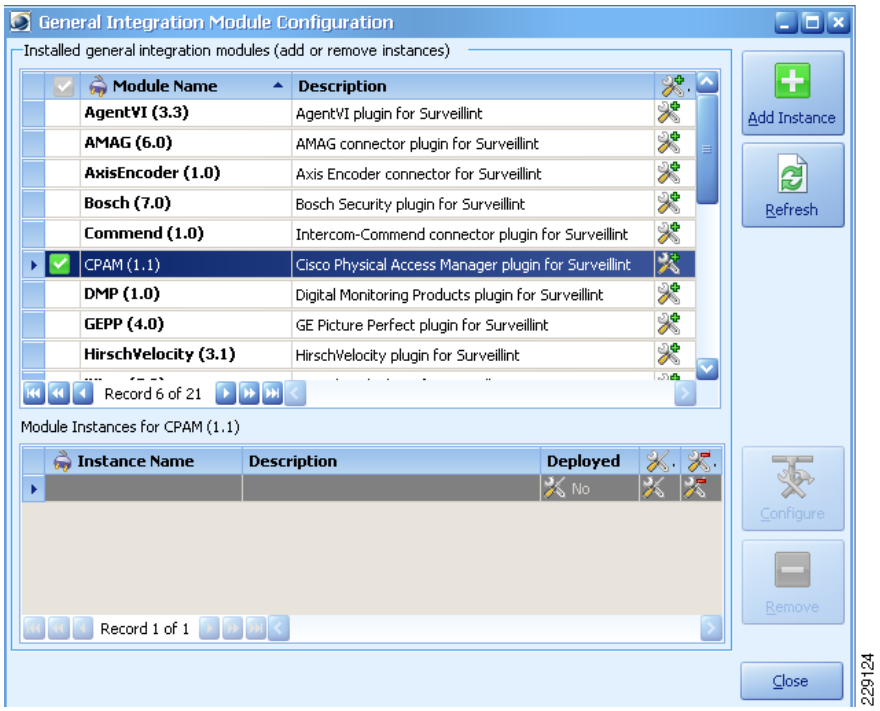
Establishing the connection between CPAM and Surveillint is performed on the Surveillint server through the Event Integration Module. This requires specifying the following information about CPAM: IP address, web service URL, and login. Perform the following steps:

Step 1 Launch the Administration Console at Surveillint's server and select **Event Integration > Integration Modules**.

Step 2 Select **CPAM > Add instance**. (See Figure 5-4.)

Note Surveillint supports both CPAM version 1.1 and 1.2.

Figure 5-4 Select CPAM from the General Integration Module Configuration



Step 3 Click **Add Instance** next to **Cisco PAM plugin for Surveillint**. A new page displays. The administrator will be led through a several short steps in a wizard to provide the following information:

- Instance Name
- Description of the Instance
- Web Server Host/IP Address
- Password
- Connector (Integration Module) Web Service IP Address
- Port for the Connector Communications

At the end of the setup wizard, Surveillint will ask the administrator to check connectivity and verify the login. Detailed logs will also be provided if additional troubleshooting is required. On successful configuration, the new Integration Module Instance Name will be shown.

Troubleshooting

Surveillint maintains activity and error logs in the following server directory:

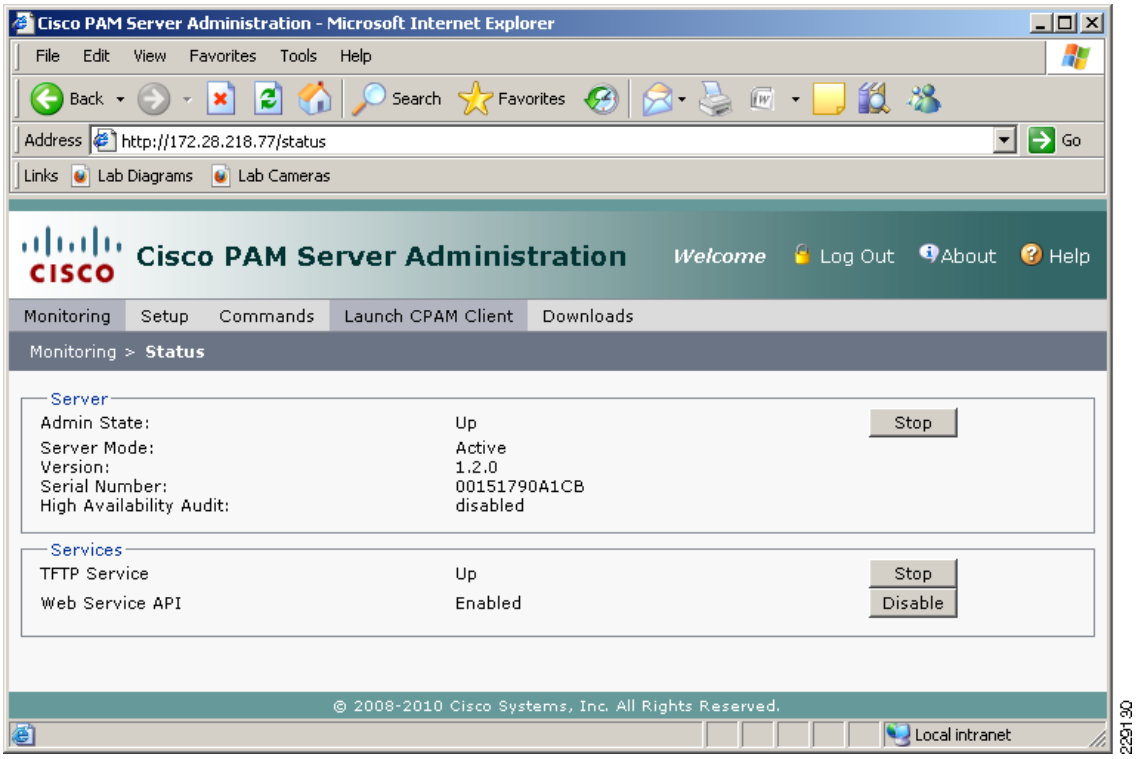
C:\Inetpub\wwwroot\PxConnectorWS\log.

In case there is an error when creating an instance, examine the most recent log in that directory. If the error "*Server Error in '/PxConnectorWS' Application. Request timed out"* is encountered when creating the CPAM instance, complete the following steps:

Step 1 Restart the "Web Service API" on the CPAM server by going to https://<cpamserver_ip_address>.

Step 2 As shown in Figure 5-5, click **Disable**. Wait for several minutes for the command to complete. Click **Enable**. Wait for a couple of minutes for the command to complete, then try to establish the connection between CPAM and Surveillint again.

Figure 5-5 Disable and Enable Web Services API



Auto Discovery of Newly Added Sensors

After establishing a connection with CPAM, Surveillint can automatically discover new gateways ("sensors" in Surveillint's term) that have been added to CPAM. This is done through "sensor management services". The default setting is to update the sensors once a day, but this is a user customizable field.

To update the value, perform the following steps.

Step 1 On the Surveillint server, from the Start menu, select **All Programs > Proximex Services > Services Configuration**. The Services Configuration window appears.

Step 2 Select **6 – Sensor Manager** in the left side of the window. Click the radio button **hourly** to discover newly added sensors more frequently.

Step 3 After adding a new door in CPAM, click **On-Demand > Sync Sensors Now**. The newly created door in CPAM is automatically added as an access control sensor in Surveillint. The sensor is created with the same name as it appears in CPAM.

Assigning a Sensor to a Monitoring Area and Placing the Sensor on a Map

After a sensor is automatically added through "Sync Sensors Now", assign the sensor to a specific monitoring area, such as "Springfield, elementary school, first floor", by performing the following steps:

Step 1 From the Administration Console, select **Environment > Monitoring Areas**. Select the monitoring area, such as "First Floor East", and then click **Edit**.

Step 2 Select **Member > Add**. The "sensor manager – select sensors" window opens.

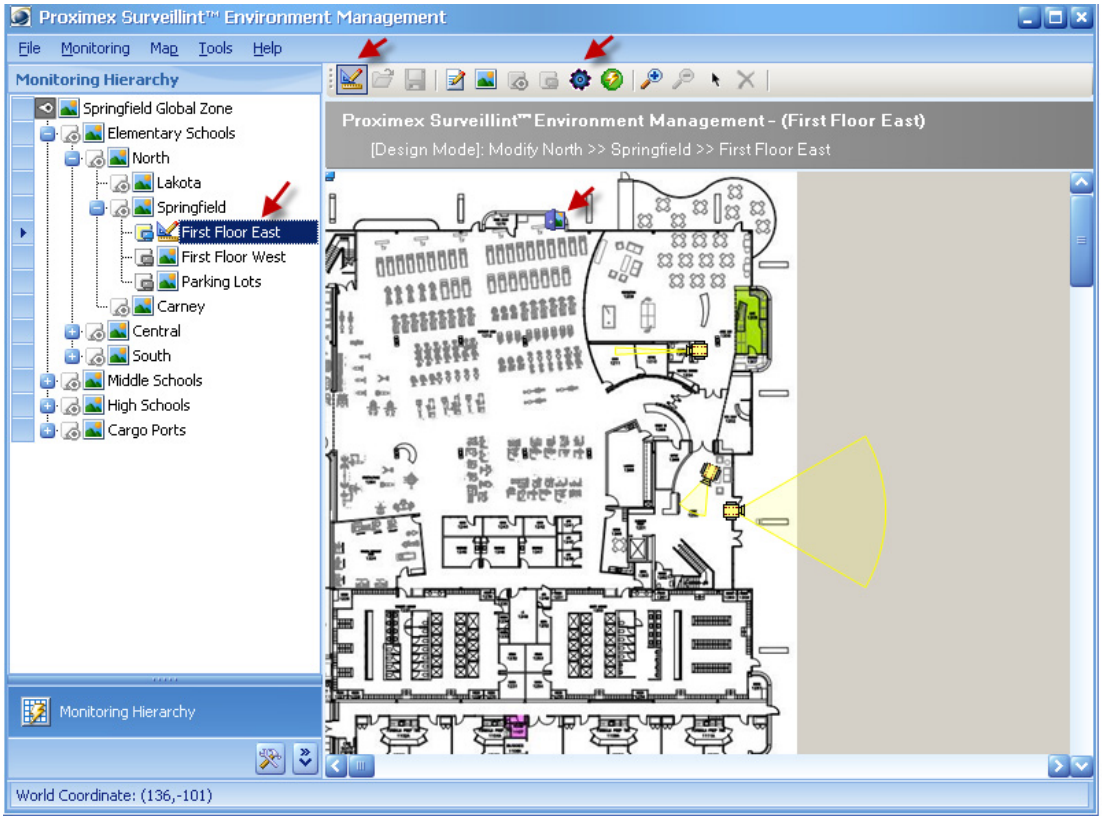
Step 3 Select an entry (such as "entrance door for police station 1") and check the blue box in front of the entry.

Step 4 Click **Add** to close the window and click **OK** to close the monitoring area properties window.

Step 5 The sensor can be placed on the map interface. From the Administration Console, select **Environment > Monitoring Environment**. Select the location and click the **Enter design mode** icon.

Step 6 Double click the **position sensor** icon then select **position sensor (entrance door for police station 1)** from the pulldown menu. Move the cursor to the location for this sensor and click on the map. A user can move the cursor again and click to fine tune the location of the sensor. See Figure 5-6. For more details on the configuration, refer to Chapter 6 of the *Administering Surveillint* document .

Figure 5-6 Place a Sensor on the Map Interface



After placing the sensor on the map interface, a user can proceed to configure receiving alerts from this door.

Configuring Receiving Alerts from Doors

The creation of events in business logic may be performed from any client machine. Surveillint has many event business logic templates predefined for different alarm types (for example, "door held open", "door forced open", etc). These templates are precreated to enable CPAM events or alarms to be raised in Surveillint, but can also be easily customized to raise any alarm based on text found in the CPAM event. A user can create an event in business logic by copying from a template, by performing the following steps:

Step 1 From the Administration Console, click **Business Logic > Event Business Logic**.

Step 2 Select **Create Alert – All > Add Template**. The Add Business Logic Template window appears.

Step 3 Modify the template name accordingly, such as “CPAMInst1 –all alerts”.

Step 4 Click **OK** to close the window.

This business logic instructs Surveillint to capture all events received from CPAM. For more detailed instructions on how to use and customize business logic templates, refer to the *Proximex Surveillint Configuring Cisco Physical Access Manager Integration Module Guide*.

Step 5 After the event business logic is created, apply it to enable Surveillint to receive the alerts. From Administration Console, click **Business Logic > Apply Business Logic > Apply Policies**.

Step 6 Click the radio button on the left of **Event Business Logic** and click **Next**.

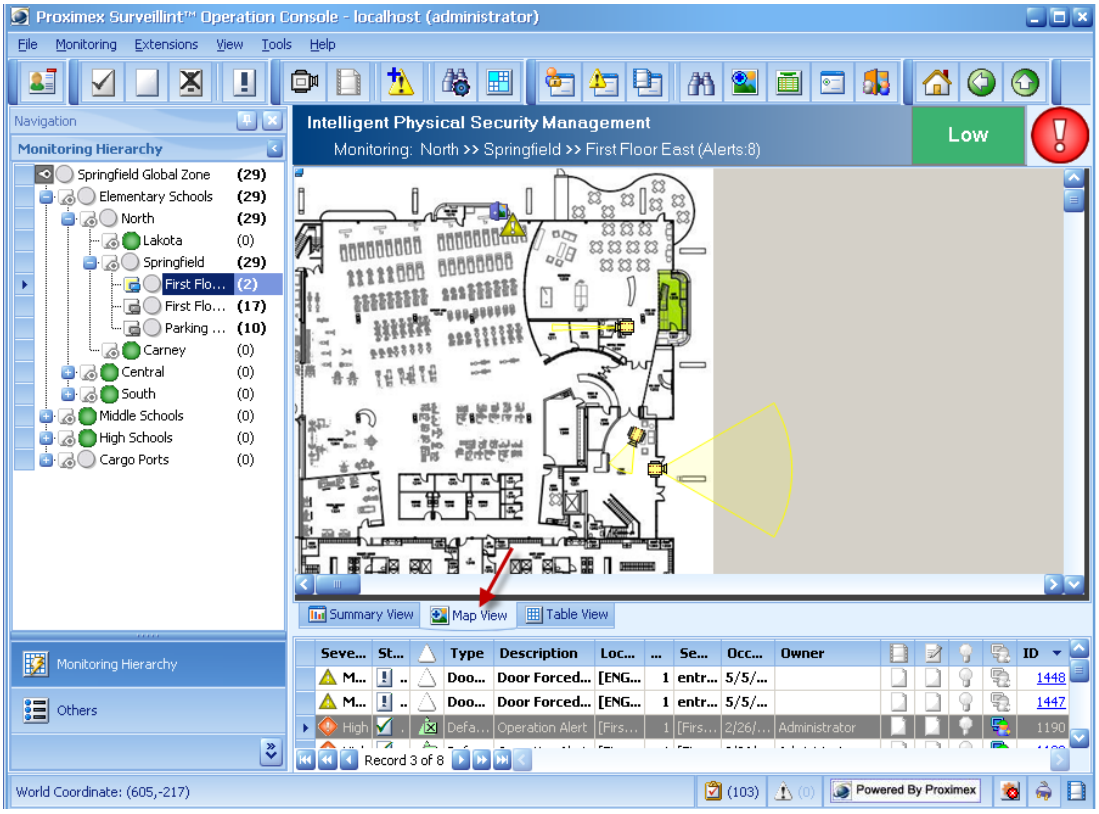
Step 7 Business Logic policies must be applied at the highest level in the hierarchy, select **Global Zone** and click **Next**.

Step 8 Click **Add** then select the business logic, such as “CPAMInst1 –all alerts”, then click **OK > Apply** to close the Policy Manager window. For more detailed instructions on how to use and customize business logic templates, refer to Chapter 14 of the *Proximex Administering Surveillint Guide.*

After the business logic rule is applied, alerts from a door, such as “forced entry”, are viewable in the operation console.

An operator may launch the operation console from **Start > All Programs > Surveillint 5.0 > Operations Console**. The operator may also launch the operation console from the admin console from the Administration Console by clicking **Tools > Operation Console** from the pulldown menu, and then clicking the **Map View** tab. Figure 5-7 shows two “door forced open” events.

Figure 5-7 Map View of Surveillint's Operation Console



Configuring Surveillint to Send Incident Notifications

With the Surveillint's Business Logic Designer, alarms from CPAM can also be easily linked and configured to automatically send a notification through AtHoc. Configuring Surveillint to send incident notifications consists of two steps: create an alert business logic and apply the alert business logic.

Step 1 From the Administration Console, click **Business Logic > Alert Business Logic**.

Step 2 Select one of the templates, such as **Alert Business Logic**, then right-click.

Step 3 From the pulldown menu, click **Add Template** and modify the template name and description.

Step 4 If there are other items other than “start” in the left panel, delete all items except “start”.

Step 5 Click **designer** button on the "activity list" panel.

Step 6 Scroll down then expand the **decisions** tab. Drag **Alert condition** to the left panel.

Step 7 On the left panel, double click **alert condition**. The **alert condition activity properties** window opens.

Step 8 Modify **display name**. uncheck **severity**". Check **alert type(s) in** and the **select alert types** window opens.

Step 9 Click **source** tab to sort entries according to source.

Step 10 Scroll down to see entries with CPAM as source. Check **door forced open** with CPAM as source.

Step 11 Click **OK** to close the Select Alert Types window.

Step 12 Click **OK** to close Alert Condition Activity Properties window.

Step 13 On the activity list panel, drag **HTTP send**, which is under Actions tab, to the left panel.

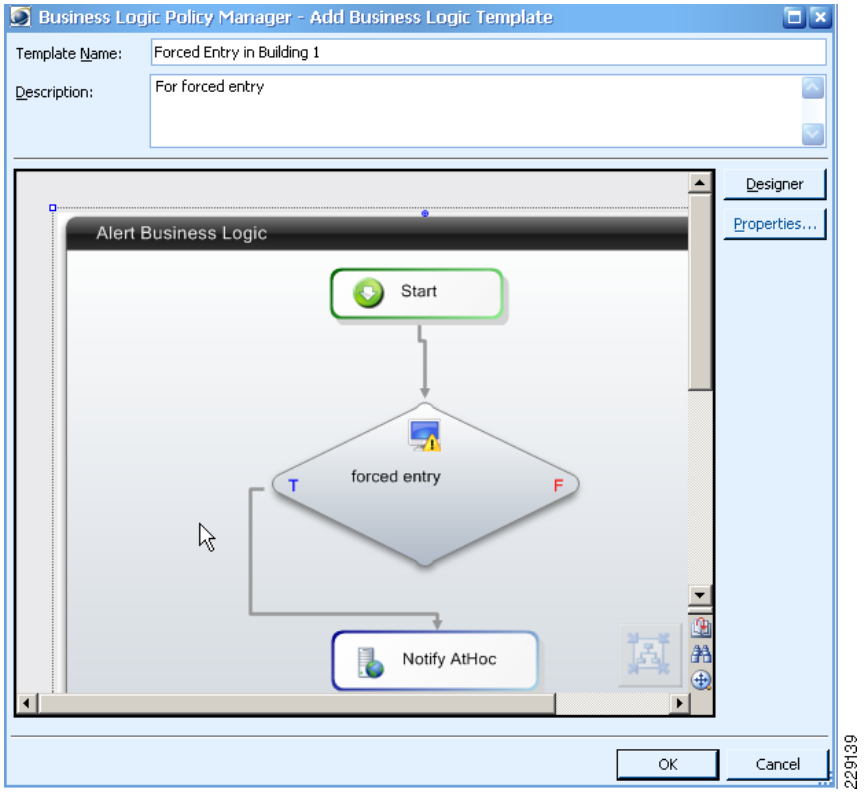
Step 14 Double click **HTTP send** on the left panel and the **HTTP send activity** window opens.

Step 15 Modify display name and URL (see Figure 5-8). In the example, the URL is used to trigger AtHoc.

Step 16 Click **OK** to close the **HTTP send** activity window.

Note In the Activity List panel, under the Sensor Commands tab, a user can select LockDoor, OpenDoor, or OpenDoorMomentarily to build a business logic. This is how Surveillint sends commands to CPAM. For example, an operator can remotely open a door for an employee after verifying the employee's identity.

Figure 5-8 Alert Business Logic was Created



After the alert business logic is created, a user can proceed to apply the logic.

Step 17 From the administration console, click **Business Logic > Apply Business Logic > Next**.

Step 18 Select **Global Zone > next**.

Step 19 In the next page, click **Add** and select "building 1 forced entry".

Step 20 Click **OK > Apply**.

Note After modifying the alert business logic, use **Apply Business Logic** to remove the alert business logic from the global zone, and then reapply the alert business logic to the global zone.

Step 21 Go to the operation console. If a door is forced open, the operation console shows the incident and AtHoc is automatically triggered.

Troubleshooting

If the sensor is not functioning as expected, a user can troubleshoot the connection to CPAM by reviewing the logs at *C:\Inetpub\wwwroot\PxConnectorWS\log*. A user may also troubleshoot and test the Business Logic rule that is being used for the CPAM instance.

CPAM Receives Alerts and Takes the Proper Action

CPAM is capable of receiving events from other applications and taking the proper action. For example, a chemical detection sensor can send a properly formatted URL to the CPAM server, and the server performs the proper function based on the content of the URL. This feature is useful when a system does not have an integration software, such as Surveillint, installed.

To configure CPAM 1.2 to respond to a URL request, do the following:

1. From the CPAM client, click **Events & Alarms > External Events**.
2. Click **Import** and browse to select a XML file and a bundle file previously created.

The CPAM Administrator guide has a sample of these files. In these files, a user specifies what event type to send as a URL. Note that authentication must be done first through API before sending a URL.

Following is a sample URL sent from VSOM to notify CPAM with “motion detected”: *http://10.194.31.14:8080/acws/services/acvsm/recordCameraEvent?eventType=CB.MOTION_START &eventTime=0&cameraId=74*.

IPICS Integration

Integration Checkpoints

The IPICS server IP address and a policy ID are needed to trigger a notification via a URL. The policy is configured using the IPICS web interface. This is where the message text is configured, as well as the users and user groups that will receive the message.

After a policy is configured, obtain the policy ID using the following steps:

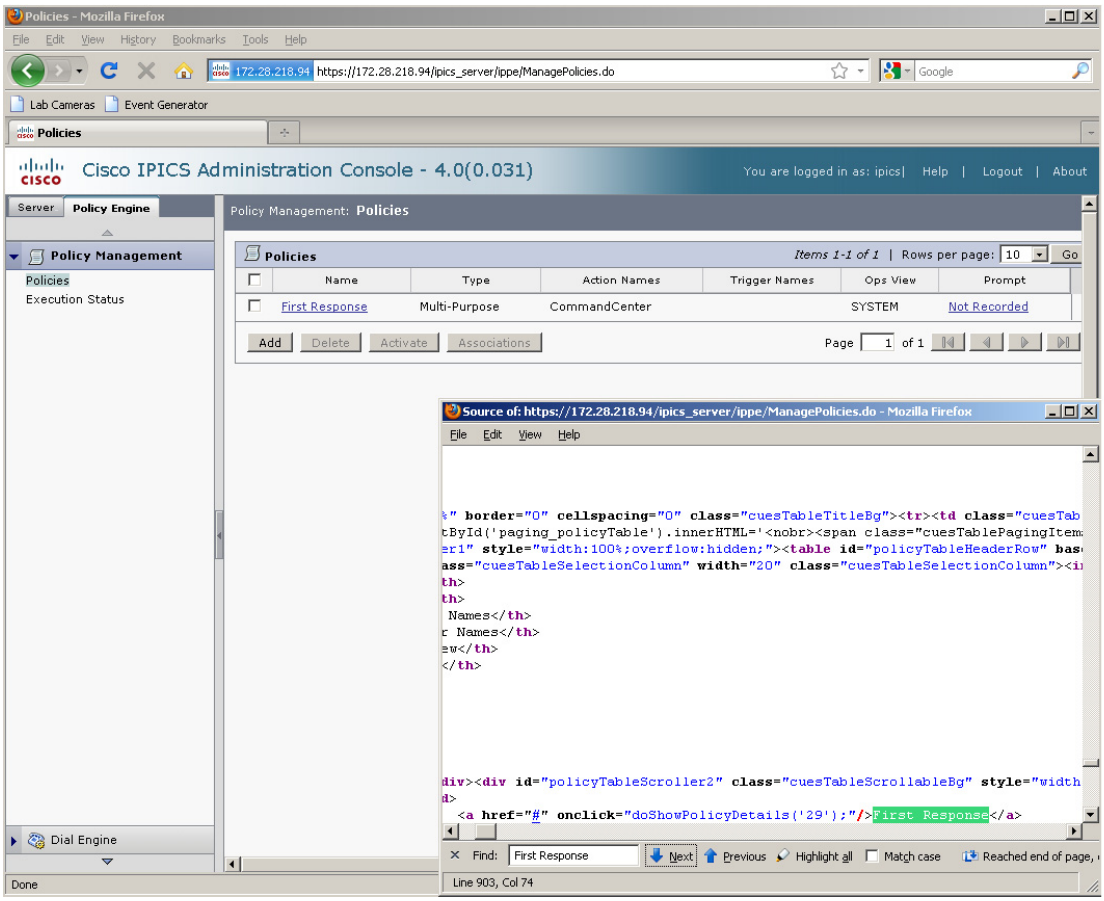
Step 1 Right-click anywhere inside the policy management window (the window on the right).

Step 2 Select the menu item **View Page Source**. A new window opens.

Step 3 Click **Edit > Find**, and type the policy name.

This shows the policy ID on the left of the policy name, as shown in Figure 5-9. In this example, the policy name is “First Response”. Searching for this policy name discovers that the policy ID is 29.

Figure 5-9 Find Policy ID



Step 4 To trigger this message in IPICS using a URL, open a browser and enter the following:

https://<ipics_server_ip_addr>/ipics_server/services/NorthboundService/executePolicy?policyId=<id>

An example is:
https://172.28.218.94/ipics_server/services/NorthboundService/executePolicy?policyId=29.

The browser asks to enter user ID and password.

Or enter the following that includes the credentials in the URL (for Firefox only):
https://ipics:C!sc0123@172.28.218.94/ipics_server/services/NorthboundService/executePolicy?policyId=29.

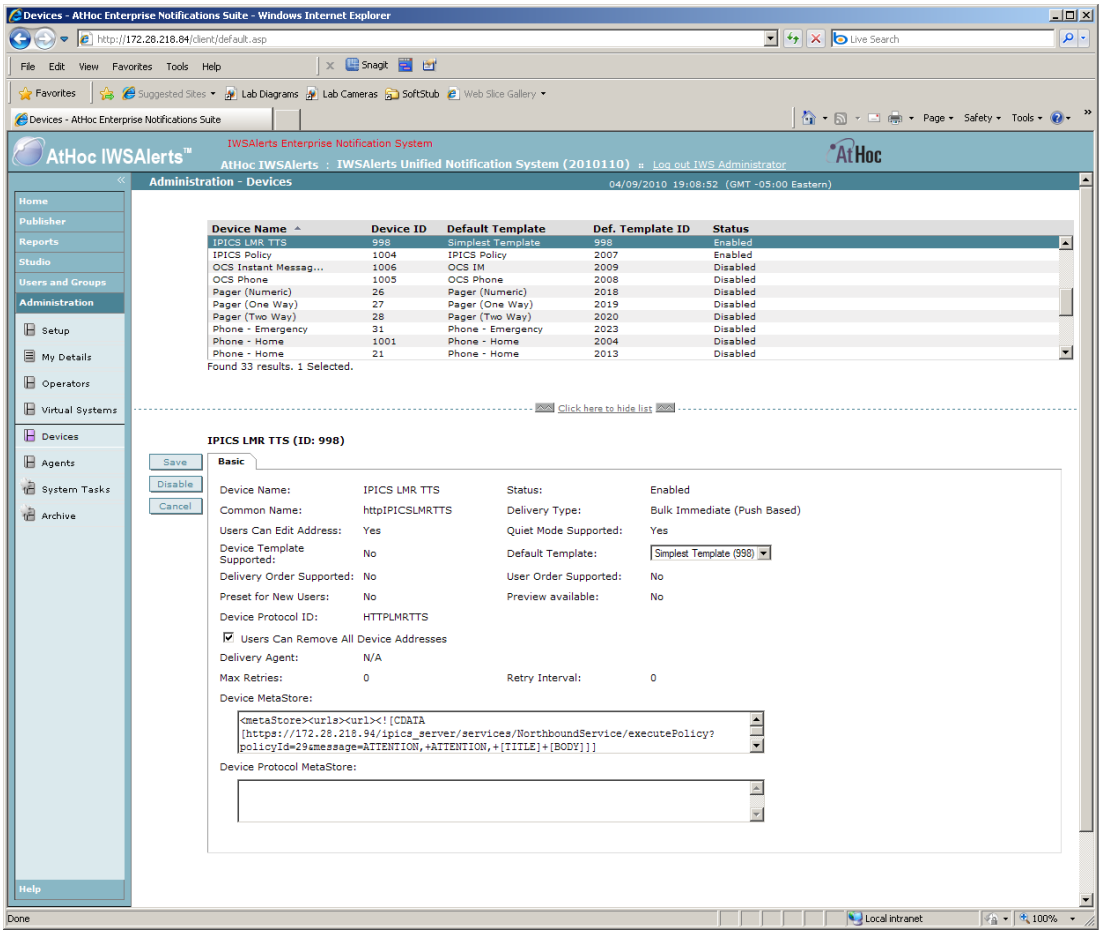
The phone with extension 1000 rings. When a user picks up the phone, the phone announces "This is Cisco IPICS calling. Press any key to continue". This is followed by "*Please enter your User ID and PIN*". Next it plays "*You're invited to join VTG 'first responder'; you're about to join VTG 'first responder'; there may be several seconds delay; you have joined VTG 'first responder'; press 1 to talk; press 2 to listen"*.

IPICS is ready for integration once it can be triggered from a web browser.

Integrating IPICS and AtHoc

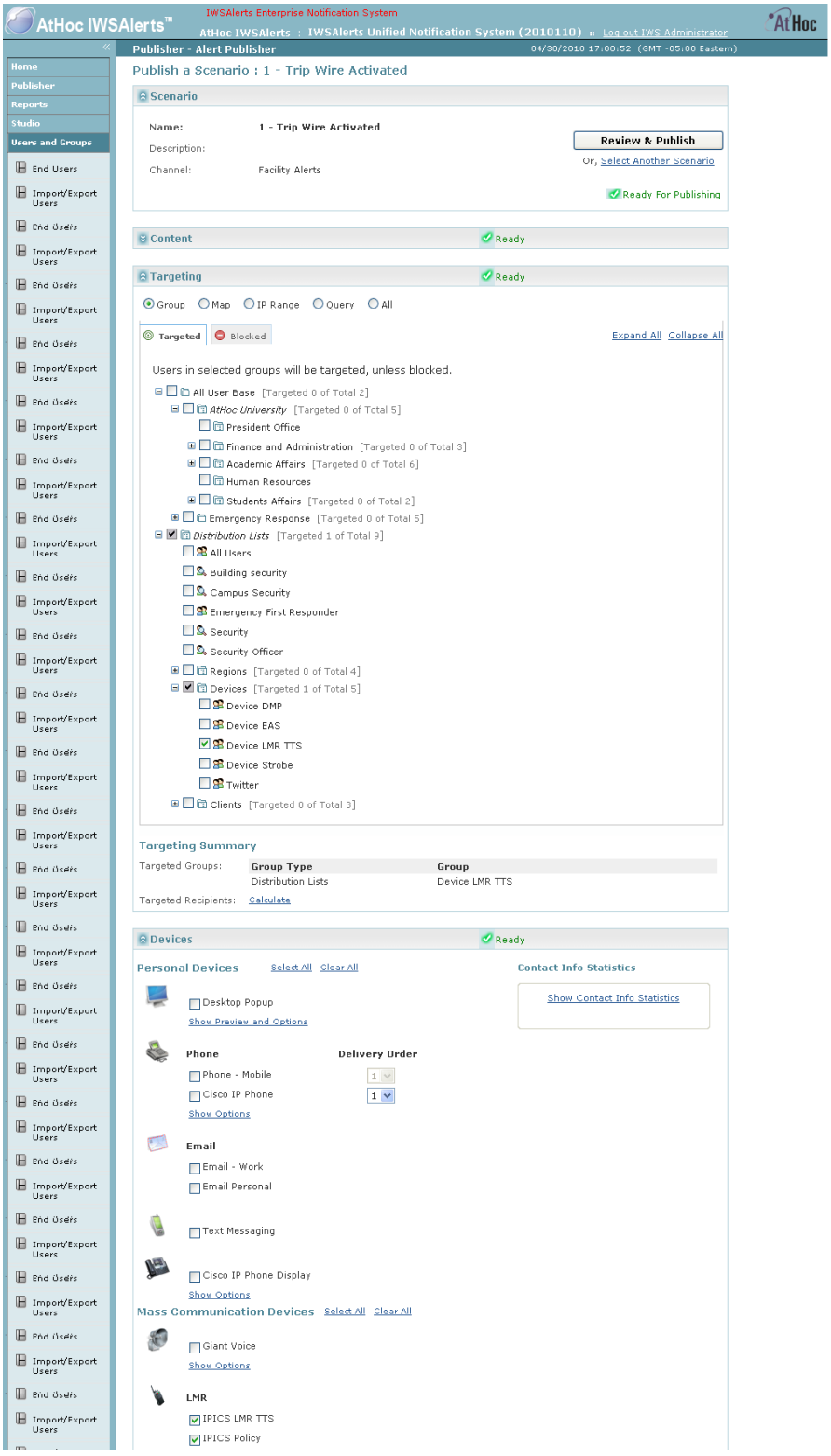
AtHoc has defined the “IPICS LMR TTS” device. Update the “default MetaStore” for this device with the URL for triggering IPICS. See Figure 5-10.

Figure 5-10 Update Default MetaStore for IPICS



Make sure IPICS is enabled on both Targeting and Devices submenus when creating a scenario that triggers IPICS. See Figure 5-11.

Figure 5-11 Enable IPCS for Both Targeting and Devices Submenus



DMP Integration

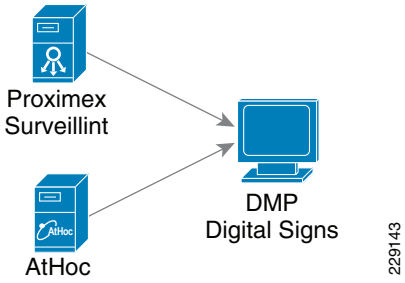
Digital media players are able to decode and display unicast and multicast live video stream as well as Flash content. In large deployments, DMPs are controlled by the Digital Media Manager (DMM), but DMPs can also receive content directly from a web server or other applications.

Typically, a web server holds the content to be displayed on the DMP, and content can be triggered by external programs using HTTP URLs to invoke configured policies. The following steps are required to display content on the DMP:

1. Create a policy in the external program, such as Cisco IPICS or AtHoc IWSAlerts.
2. Create the content to be displayed by the DMP.
3. Configure an event to trigger the policy. The DMP display changes to display the appropriate content.

Figure 5-12 shows the interaction between the DMP and other external programs. In Figure 5-12, Surveillint and AtHoc send alerts to DMP. The integration between DMP and other applications can be done through HTTP or through DMP's Application Programming Interface (API).

Figure 5-12 DMP Receiving Alerts



Creating HTML Content for the DMP

A basic HTML page can be configured to display an alert message or any message specific to the security incident. The following example displays a message on the DMP and retrieves a snapshot (via the Media Server) of the camera involved in the incident. Figure 5-13 shows a message notifying DMP viewers to avoid specific building exits.

Figure 5-13 Sample DMP Alert

The HTML code to produce the previous image is simple and relies on the Cisco Media Server to retrieve a jpg snapshot. More detailed pages can be created to display complex messages.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
   <meta http-equiv="Content-Type"
 content="text/html; charset=iso-8859-1">
  <title>Active Log</title>
</head>
<body bgcolor="#ff0000">
 
<p>   </p>
<p align="center"><b><font color="#ffffff" size="7">!ALERT!</font></b> </p>
<p align="center"><b><font color="#ffffff" size="7">Chemical Leak Reported</font></b><br>
</p>
<p align="center"><b><font color="#ffffff" size="7">Avoid South Building
Exits</font></b><br>
</p>
<table bordercolorlight="#F0F0F0" border="1" bordercolor="#a0a0a0">
  <tbody>
    <tr>
      <td valign="top">
      <blockquote>
        <blockquote>
          <blockquote>
            <blockquote> <br>
              <img
 src="http://10.94.162.201/video.jpg?framerate=0&amp;source=p_s1_Englewood_-_4500-1_1">
              <p align="center"><b><font color="#ffffff" size="5">Still
Snapshot</font></b><br>
```

```
                </p>
              </blockquote>
            </blockquote>
          </blockquote>
        </blockquote>
        </td>
      </tr>
    </tbody>
</table>
</body>
</html>
```

This HTML code can be served by any standard web server, such as IIS on Windows-based servers and Apache on Linux-based servers. In the previous HTML code, the syntax to retrieve a camera snapshot from the Media Server under the img src tag is:

http://<vsm_ip_address>/video.jpg?framerate=0&source=<camera_proxy_name>

In the previous example, the Media Server is 10.94.162.201 and the snapshot is retrieved from a Cisco 4500 IP camera:
http://10.94.162.201/video.jpg?framerate=0&source=p_s1_Englewood_-_4500-1_1

The following URL is used to obtain the proper camera proxy name from the Cisco Media Server:

http://<vsm_ip_address>/info.bwt?type=proxy

Note The snapshot URL will only work with IP Cameras that support MJPEG streams

Invoking Content for the DMP

To trigger the DMP display to change, use the following HTTP syntax:

http://<dmp_user>:<dmp_password>@<dmp_ip_address>:7777/set_param?init.BROWSER_CMD=http://<web_server_ip_address>/<web_page_name>&init.TVZILLA_URL=http://<web_server_ip_address>/<web_page_name>

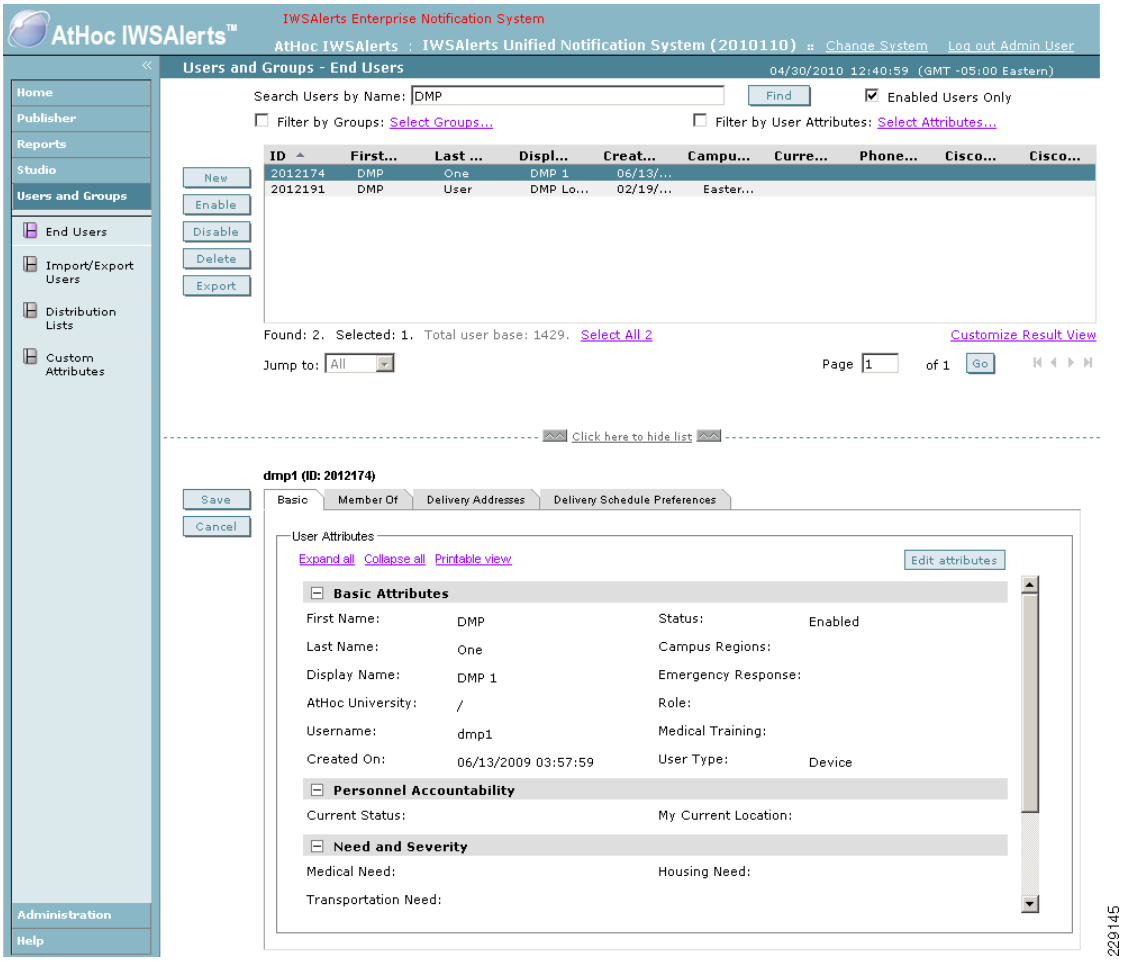
The following example retrieves the chemical.html file from the DMP at IP address 10.94.162.225. The chemical.html page is served by the web server at 10.94.162.233:
http://admin:default@10.94.162.225:7777/set_param?init.BROWSER_CMD=http://10.94.162.233/chemical.html&init.TVZILLA_URL=http://10.94.162.233/chemical.html

Integrating DMP and AtHoc IWSAlerts

To integrate DMP and AtHoc IWSAlerts, perform the following steps:

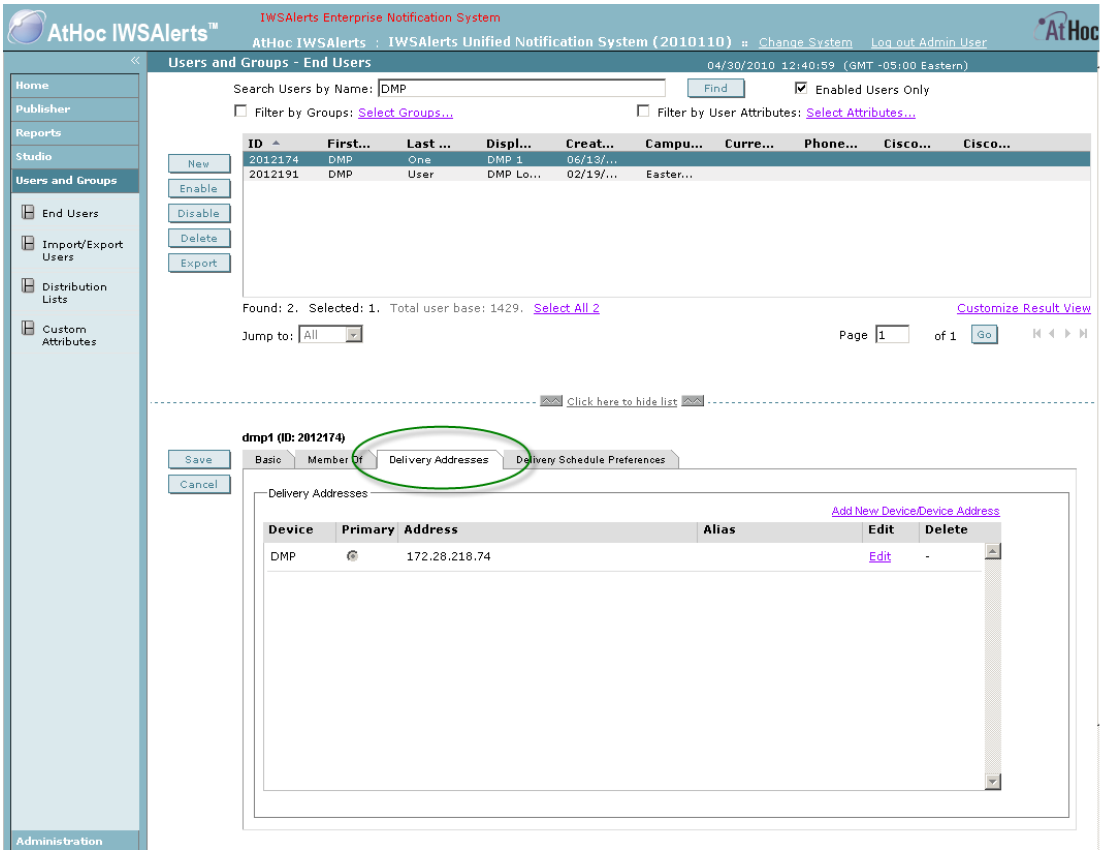
Step 1 The DMP is defined in IWSAlerts under **Users and Groups > End Users**, as shown in Figure 5-14.

Figure 5-14 DMP Definition in IWSAlerts



Step 2 AtHoc has a predefined DMP configuration. Click **Delivery Addresses > Edit** and change the IP address to point to the right DMP, as shown in Figure 5-15.

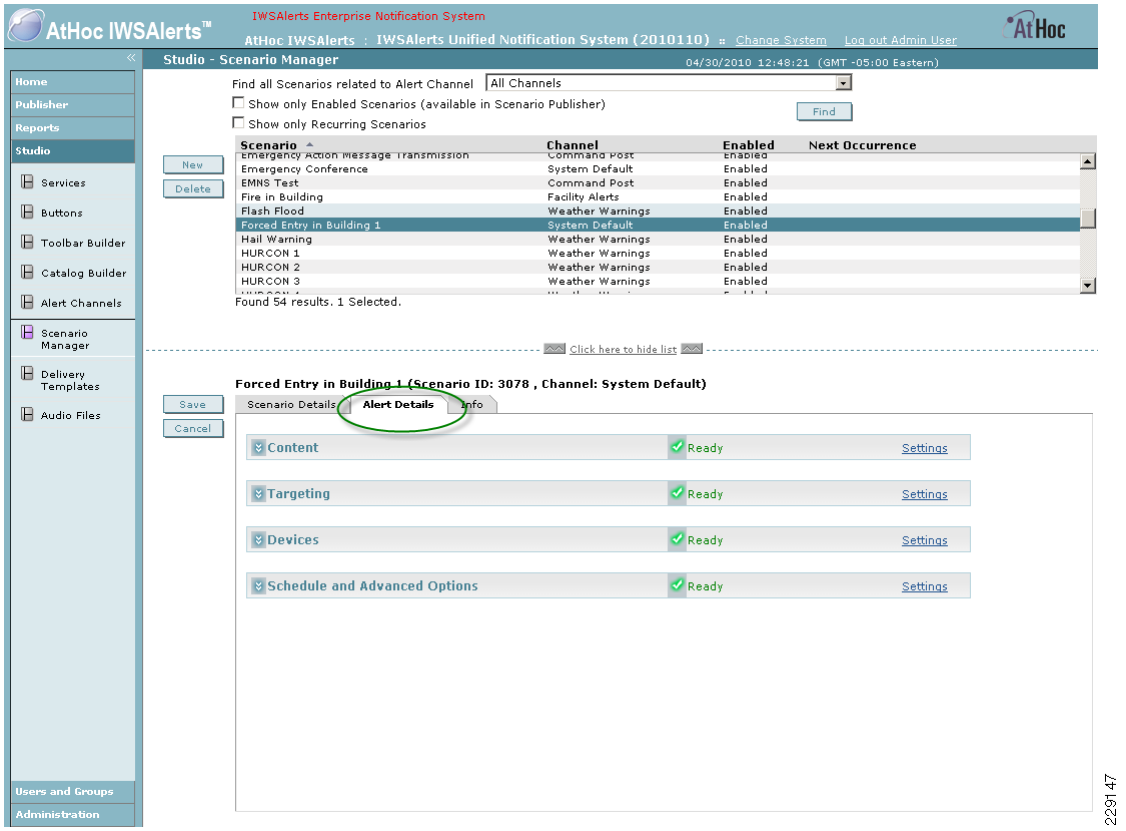
Figure 5-15 DMP IP Address



Step 3 Select the proper scenario to send alerts to the DMP by clicking **Studio > Scenario Manager > Forced Entry in Building 1**.

Step 4 Click **Alert Details**, as shown in Figure 5-16.

Figure 5-16 DMP Scenario



Step 5 Make sure DMP is enabled on both Targeting and Devices submenus, as shown in Figure 5-17 and Figure 5-18.

Figure 5-17 Target Devices

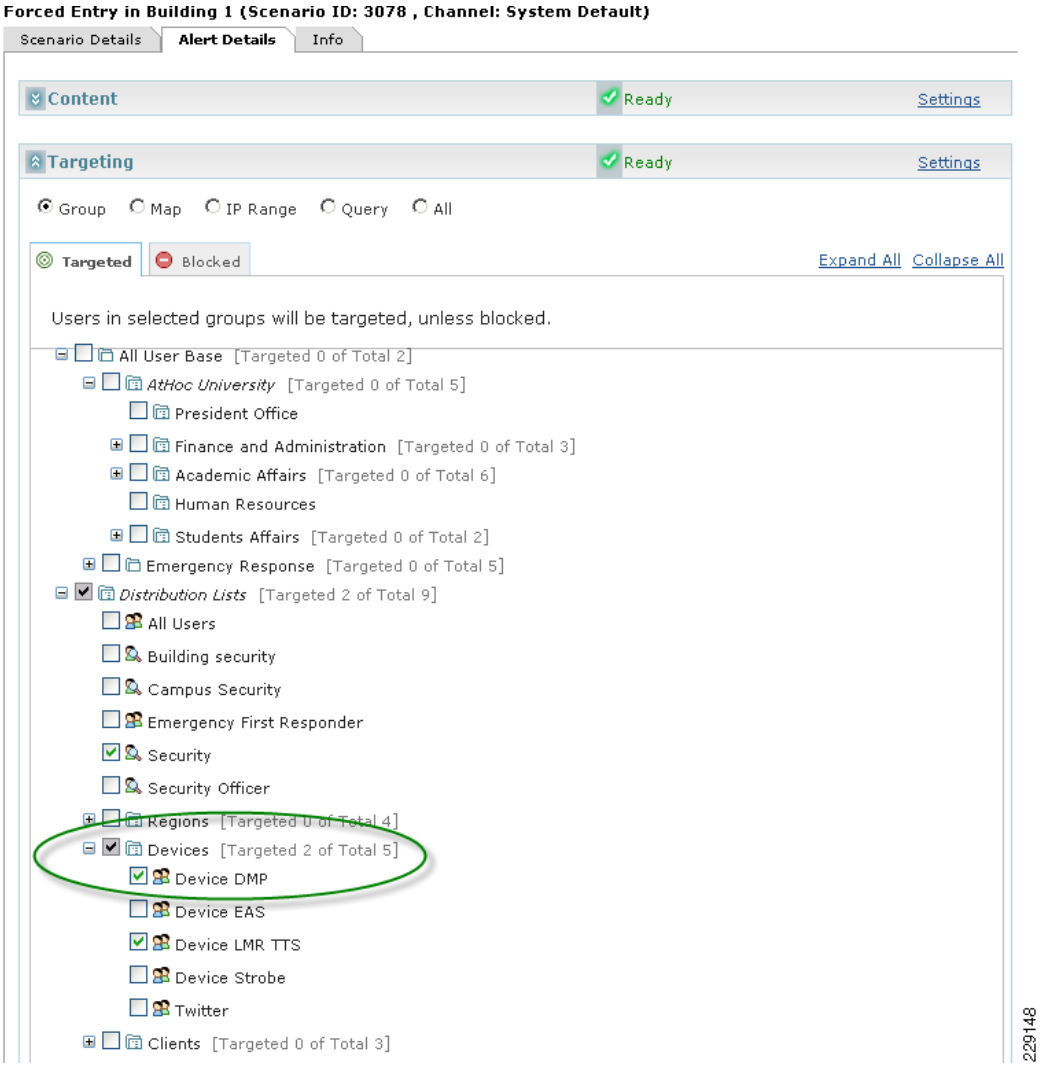
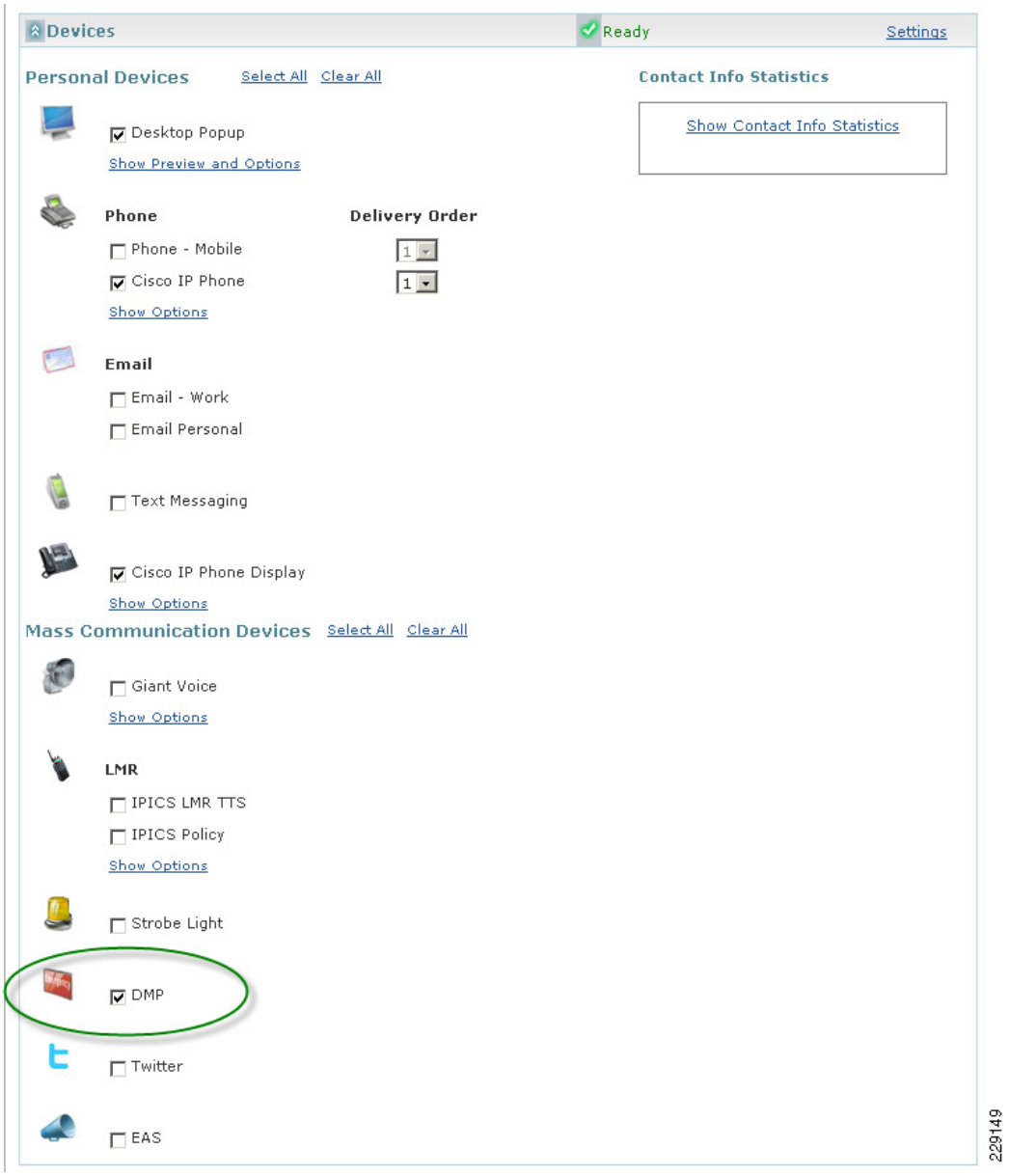


Figure 5-18 Enabled Devices



Step 6 Replace the following URL with a specific camera name:

*http://<vsms_ip_address>/video.jpg?framerate=0;source=<**camera_name**>*

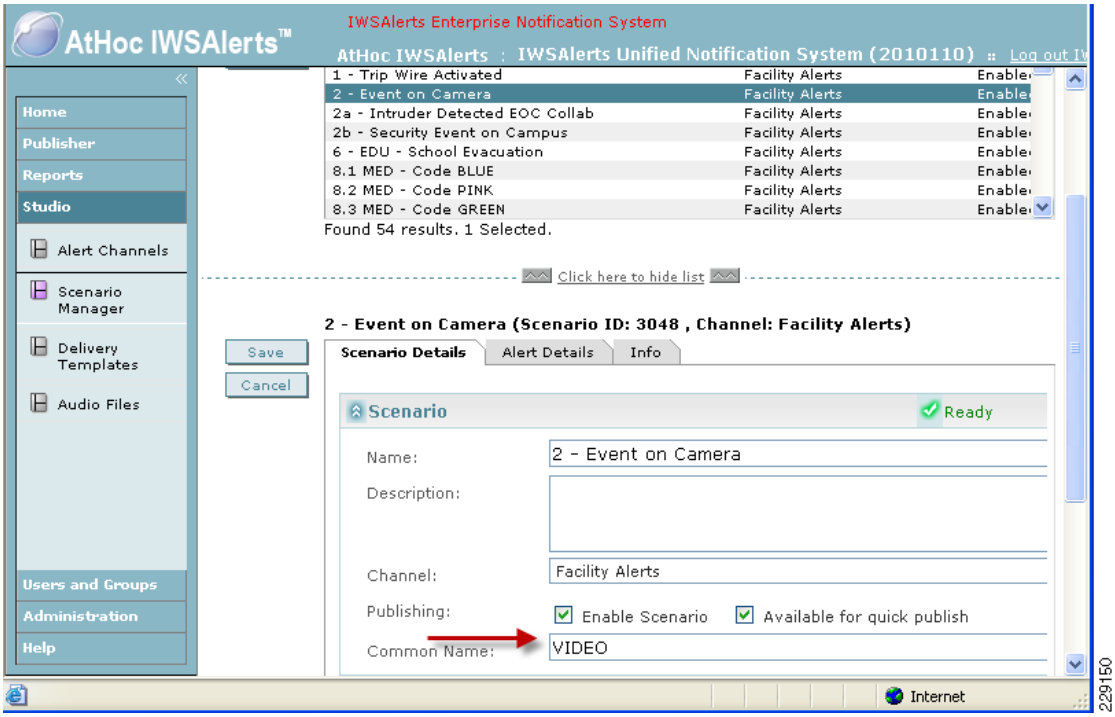
For example, enter the following URL in a browser:

http://172.28.218.82/video.jpg?framerate=0&source=p_s1_San_Jose_-_2521-1_1

It will show a snapshot of a camera.

Step 7 To send the video to DMP, place the URL for the image in scenario metastore in the DMP section. AtHoc has already defined a “event on camera” scenario. Make sure DMP is enabled on both Targeting and Devices submenus. Figure 5-19 shows the common name of the pre-defined “event on camera” scenario.

Figure 5-19 Common Name for a Pre-defined Alert



A user can trigger the notification by specifying common name in the URL:

*http://<AtHoc_ip_address>/corp/gw/gw.asp?scenario=**<common_name>***

For the above scenario, it will be:

http://172.28.218.84/corp/gw/gw.asp?scenario=VIDEO.

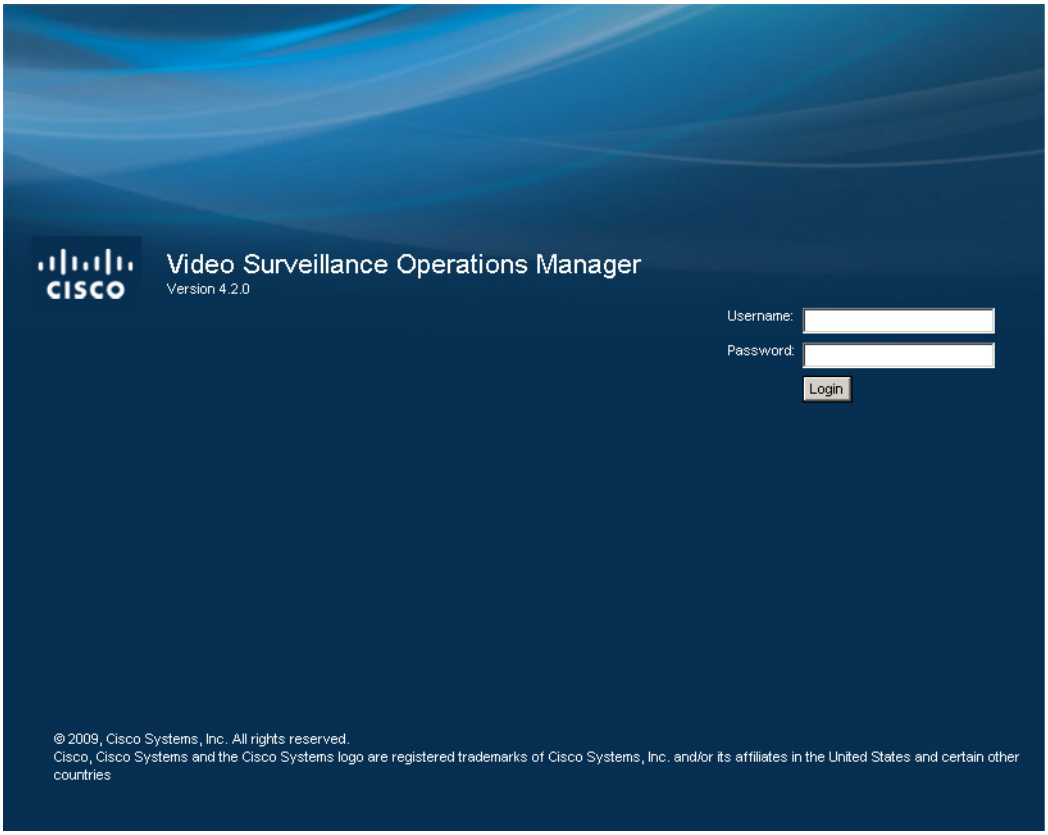
ObjectVideo Integration with Surveillint

Surveillint is able to receive video analytics alerts from ObjectVideo by using the Surveillint Integration Module for ObjectVideo. This integration module allows alerts generated by ObjectVideo to be delivered to the Surveillint Operation Console, where operators can review the incident. The integration provides a more intelligent and efficient way to process video analytics alerts and by integrating with other sensors a richer command and control environment.

Configuring ObjectVideo Sensors

Before defining an ObjectVideo analytic sensor, the ObjectVideo server must have the Cisco Video Surveillance ActiveX client installed. A simple way to do it is to connect to the Video Surveillance Operations Manager (VSOM) and display a video feed. The first time the client connects to VSOM, the proper ActiveX controls are automatically installed. Figure 5-20 shows the VSOM login screen.

Figure 5-20 Cisco Video Surveillance Operations Manager



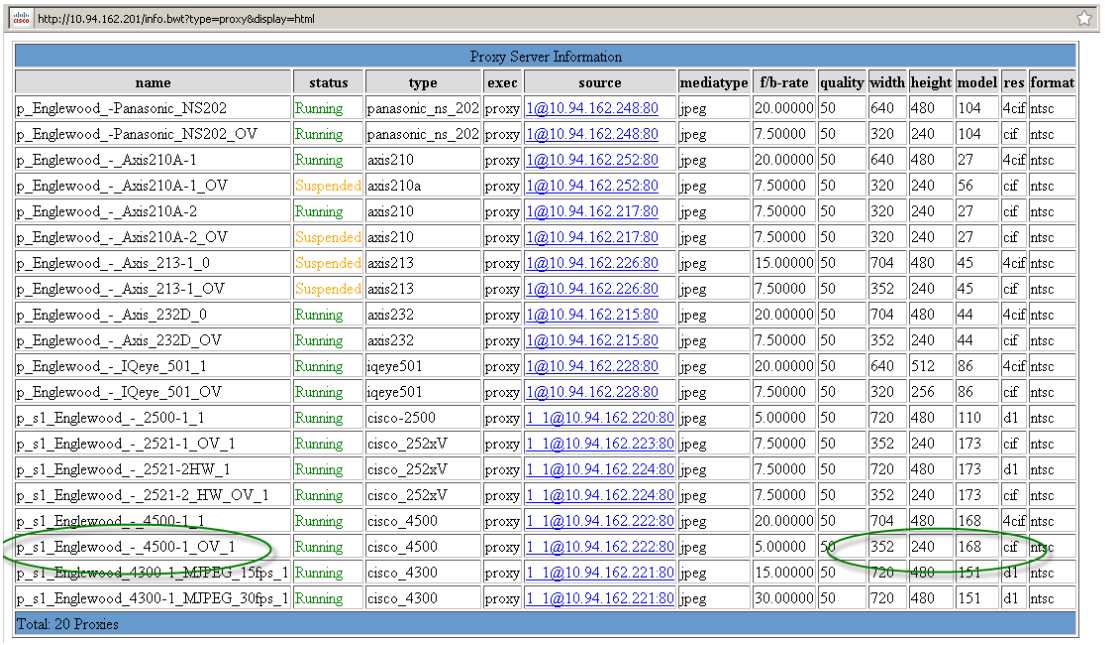
Selecting the Video Source for a Sensor

ObjectVideo is able to connect to video streams from a Video Surveillance Media Server by using the following format: *bwims://<Media Server IP address>/<proxy name>*.

The proper proxy name may be located by pointing a web browser to the Media Server using the following link: *http://<Media Server IP address>/info.bwt?type=proxy&display=html*

The link displays a list of proxies defined in the Media Server. Select the proper proxy name from the list, as shown in Figure 5-21.

Figure 5-21 List of Running Proxies



http://10.94.162.201/info.bwt?type=proxy&display=html

Proxy Server Information

name	status	type	exec	source	mediatype	f/b-rate	quality	width	height	model	res	format
p_Englewood_-Panasonic_NS202	Running	panasonic_ns_202	proxy	1@10.94.162.248:80	jpeg	20.00000	50	640	480	104	4cif	ntsc
p_Englewood_-Panasonic_NS202_OV	Running	panasonic_ns_202	proxy	1@10.94.162.248:80	jpeg	7.50000	50	320	240	104	cif	ntsc
p_Englewood_-_Axis210A-1	Running	axis210	proxy	1@10.94.162.252:80	jpeg	20.00000	50	640	480	27	4cif	ntsc
p_Englewood_-_Axis210A-1_OV	Suspended	axis210a	proxy	1@10.94.162.252:80	jpeg	7.50000	50	320	240	56	cif	ntsc
p_Englewood_-_Axis210A-2	Running	axis210	proxy	1@10.94.162.217:80	jpeg	7.50000	50	320	240	27	cif	ntsc
p_Englewood_-_Axis210A-2_OV	Suspended	axis210	proxy	1@10.94.162.217:80	jpeg	7.50000	50	320	240	27	cif	ntsc
p_Englewood_-_Axis_213-1_0	Suspended	axis213	proxy	1@10.94.162.226:80	jpeg	15.00000	50	704	480	45	4cif	ntsc
p_Englewood_-_Axis_213-1_OV	Suspended	axis213	proxy	1@10.94.162.226:80	jpeg	7.50000	50	352	240	45	cif	ntsc
p_Englewood_-_Axis_232D_0	Running	axis232	proxy	1@10.94.162.215:80	jpeg	20.00000	50	704	480	44	4cif	ntsc
p_Englewood_-_Axis_232D_OV	Running	axis232	proxy	1@10.94.162.215:80	jpeg	7.50000	50	352	240	44	cif	ntsc
p_Englewood_-_IQeye_501_1	Running	iqeye501	proxy	1@10.94.162.228:80	jpeg	20.00000	50	640	512	86	4cif	ntsc
p_Englewood_-_IQeye_501_OV	Running	iqeye501	proxy	1@10.94.162.228:80	jpeg	7.50000	50	320	256	86	cif	ntsc
p_s1_Englewood_-_2500-1_1	Running	cisco-2500	proxy	1_1@10.94.162.220:80	jpeg	5.00000	50	720	480	110	d1	ntsc
p_s1_Englewood_-_2521-1_OV_1	Running	cisco_252xV	proxy	1_1@10.94.162.223:80	jpeg	7.50000	50	352	240	173	cif	ntsc
p_s1_Englewood_-_2521-2HW_1	Running	cisco_252xV	proxy	1_1@10.94.162.224:80	jpeg	7.50000	50	720	480	173	d1	ntsc
p_s1_Englewood_-_2521-2_HW_OV_1	Running	cisco_252xV	proxy	1_1@10.94.162.224:80	jpeg	7.50000	50	352	240	173	cif	ntsc
p_s1_Englewood_-_4500-1_1	Running	cisco_4500	proxy	1_1@10.94.162.222:80	jpeg	20.00000	50	704	480	168	4cif	ntsc
p_s1_Englewood_-_4500-1_OV_1	Running	cisco_4500	proxy	1_1@10.94.162.222:80	jpeg	5.00000	50	352	240	168	cif	ntsc
p_s1_Englewood_4300-1_MJPEG_15fps_1	Running	cisco_4300	proxy	1_1@10.94.162.221:80	jpeg	15.00000	50	720	480	151	d1	ntsc
p_s1_Englewood_4300-1_MJPEG_30fps_1	Running	cisco_4300	proxy	1_1@10.94.162.221:80	jpeg	30.00000	50	720	480	151	d1	ntsc

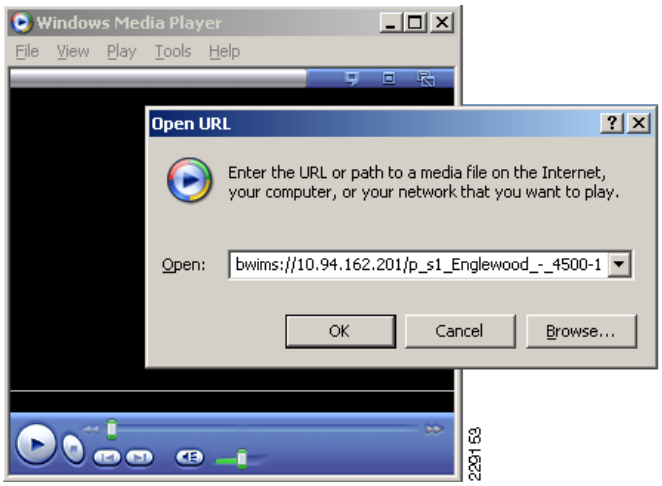
Total: 20 Proxies

229152

Based on List of Running Proxies, the complete Video Source for that camera translates into: *bwims://10.94.162.201/p_s1_Englewood_-_4500-1_OV_1*.

A simple way to verify whether the link is valid is to view it in Windows Media Player. Launch Windows Media Player and click **File > Open URL** and paste the bwims:// URL, as shown in Figure 5-22.

Figure 5-22 Windows Media Player



Windows Media Player should be able to play the video stream directly from the Media Server, as shown in Figure 5-23.

Figure 5-23 Windows Media Player—Streaming

Note A digitized CIF NTSC video feed translates to a resolution of 352x240 pixels. ObjectVideo recommends that video feeds are configured with either 320x240 (QVGA), 352x240 (CIF NTSC), or 352x288 (CIF PAL) pixels of resolution.

Configuring a New Sensor using the ObjectVideo Management Tool

To define a new sensor in ObjectVideo, perform the following steps:

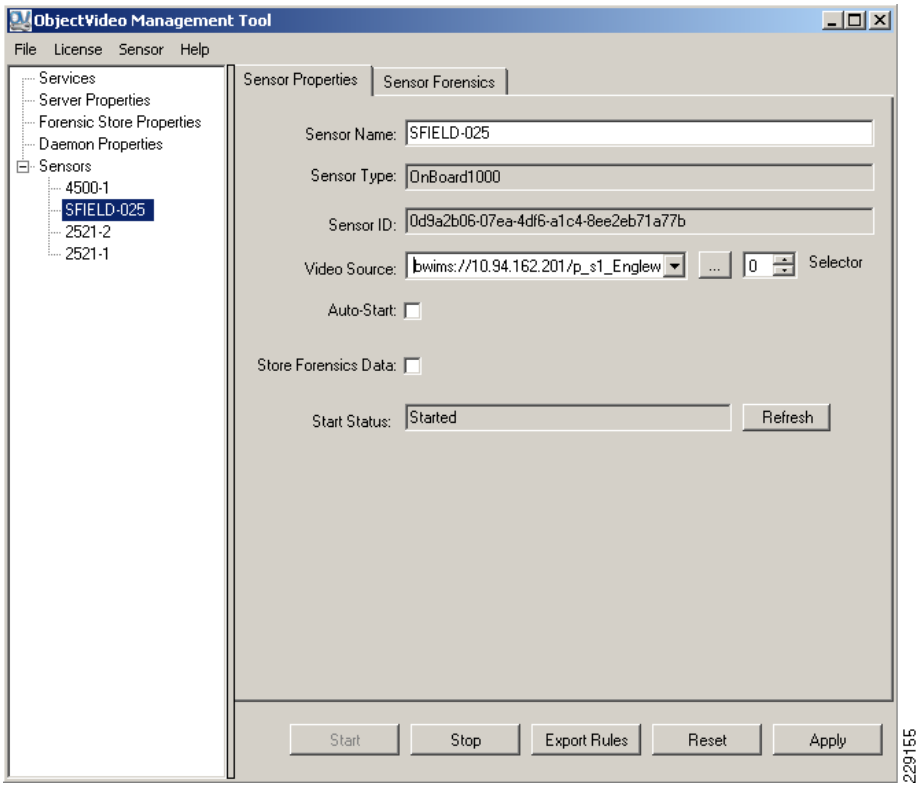
Step 1 Launch the ObjectVideo Management Tool and click on **Sensor > Add.** Specify the sensor type as **OnBoard 1000.**

The ObjectVideo Management Tool creates a new sensor name with default settings. The Sensor name is auto-generated by ObjectVideo.

Step 2 Change the Sensor Name and Video Source to point to the right camera source. In this case, the following video feed from the Media Server is used: *bwims://10.94.162.201/p_s1_Englewood_-_4500-1_OV_1*.

While the name can be assigned by the user, note that the Sensor ID is assigned by ObjectVideo and is unique for each sensor. Figure 5-24 shows the complete sensor configuration. The sensor may be configured to auto-start when ObjectVideo starts by clicking on the Auto-Start option.

Figure 5-24 Sensor Defined



The proper configuration and XML files for the sensor are created in the following directory of the ObjectVideo server: *C:\program files\ObjectVideo\ISE*. The file names are based on the Sensor ID generated by ObjectVideo.

ObjectVideo Rule Management Tool

The Rule Management Tool enables users to configure various video analytics rules defined for each sensor. Rules tell the system which events to look for while monitoring video, and how to respond to those events.

ObjectVideo supports several types of events and object types. Events are activities that occur within a camera's field of view. All ObjectVideo event types are presented to the user in the Rule Management Tool in the following categories. Note that depending on how a particular sensor is licensed, not all of these may be available to the user.

- Video TripWire—An object crosses a line (tripwire) drawn within the camera's field of view.
- Multi-line tripwire—An object crosses two lines (Tripwires) drawn within the field of view within a specified time.
- Partial View—An object performs an action anywhere within an area of interest. An area of interest is a square, rectangle, or other multi-sided shape drawn within the camera's field of view. An area of interest can be a ground plane or an image plane. Actions associated with a Partial View include enters, exits, appears, disappears, loiters, object left behind, and object taken away

- Full View—An object performs an action anywhere within the camera's field of view. Actions associated with a Partial View include *appears*, *disappears*, *object left behind*, and *object taken away.*
- Density—A crowd of low, medium, or high density appears in an area of interest within the camera's field of view consistently over a user-specified period of time.
- Camera Tamper—Camera tamper events are generated for any event that significantly changes the camera's field of view, such as the camera being panned, turned off, unplugged, jostled, or covered, or the lights being turned on or off. For Auto-force view behavior (an ObjectVideo configuration option) in which the system is forced to use the view it sees even if it changes, a Camera Tamper event triggers whenever something occurs to cause the sensor to enter a Bad Signal sensor status.

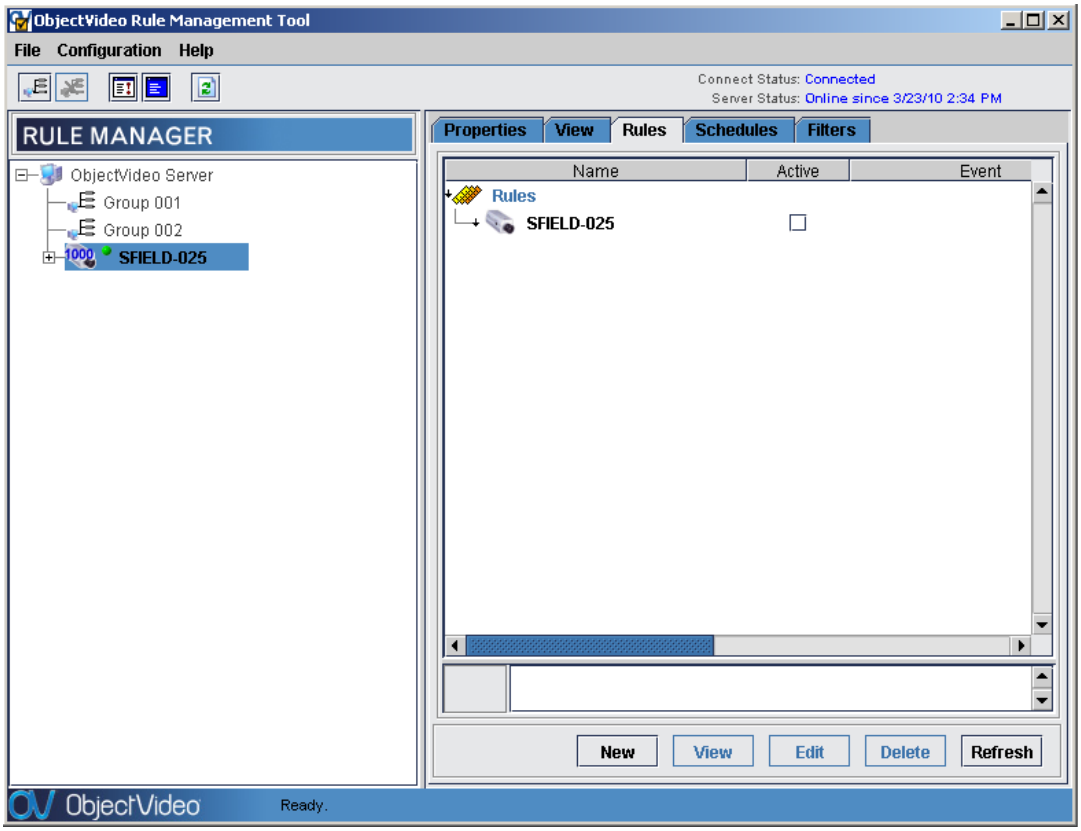
When defining a new event using the Rule Management Tool, one or more objects must be specified for the event. An object is something that either performs an action or is acted upon to trigger a response. The following object types may not be supported by every sensor:

- Anything—Includes all object types (people, vehicles, not categorized). For Taken Away and Left Behind events, anything can include passive objects that do not appear to move on their own.
- Vehicle—A mechanism designed to carry people or other cargo (for example, a car, truck, boat or plane)
- Person—An object with some characteristics of a human being.

To create a new rule, perform the following steps:

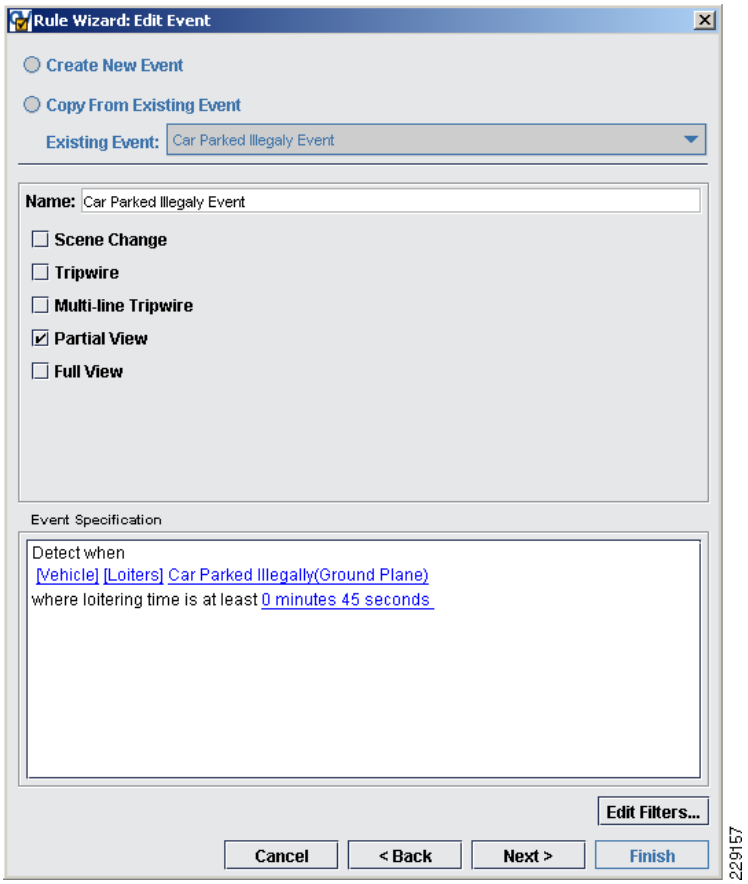
Step 1 Select the newly created sensor and click on **Default View > Rules > New**, as shown in Figure 5-25.

Figure 5-25 New Analytics Rule



Step 2 Give the rule a new name. For this example the rule is named **Car Parked Illegally**. The following event details are defined to identify a vehicle parked in a restricted area for more than 45 seconds, as shown in Figure 5-26.

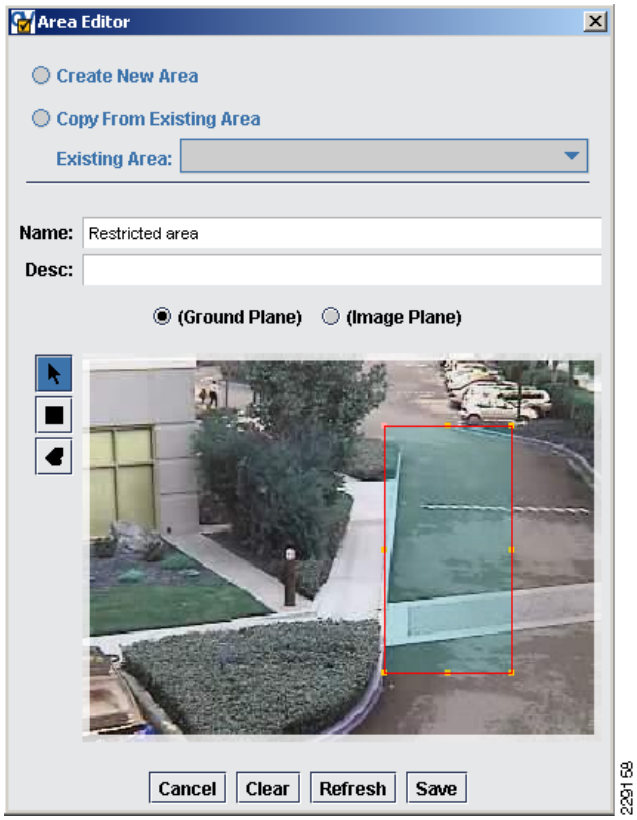
Figure 5-26 Event Details



The event rules include several analytics rules, such as detecting persons, vehicles, tripwire lines, scene changes, and so on. The rules can also be defined in various ways according to the specific field of view or analytics requirements.

Figure 5-27 shows the area that ObjectVideo performs an analysis before generating an alert.

Figure 5-27 Restricted Area



Step 3 Specify when the event will be active in the **Create Schedule** screen and click **Next.**

ObjectVideo is able to send event notifications to different systems, including:

- E-mail recipients
- Surveillint
- Any third-party system able to receive HTTP notifications

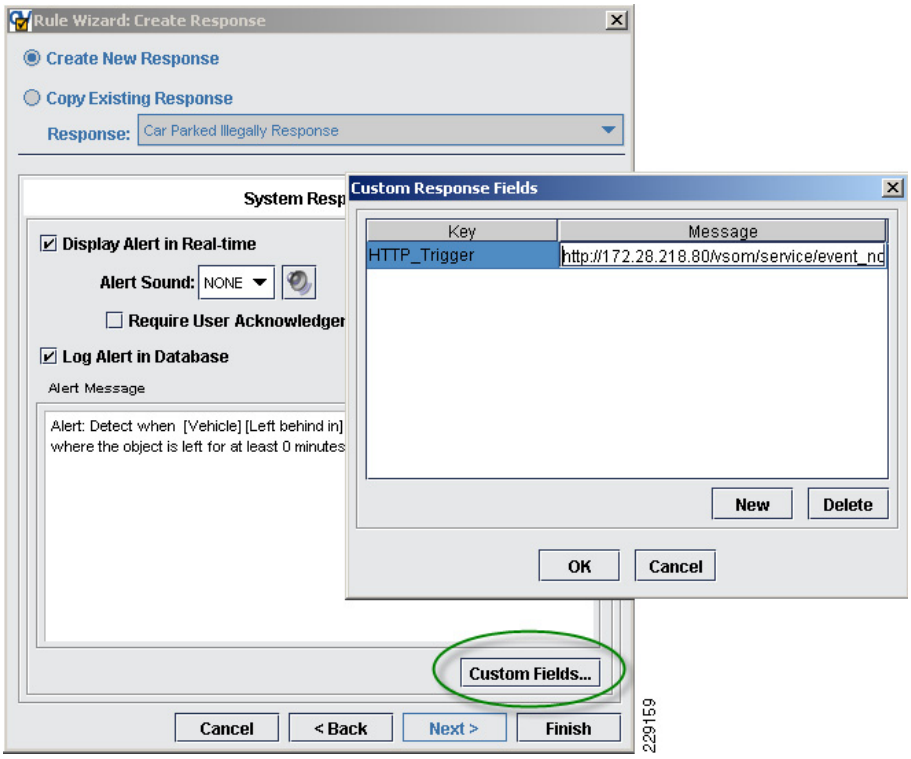
Step 4 To send a specific HTTP message to a third-party system, such as VSOM, define the proper URL in the *Alertbridge.exe.config* file, located in the ObjectVideo server at *C:\Program Files\ObjectVideo\Alert Bridge*.

Step 5 Edit the **URLIdentifier** tag under the UrlHandlerAlertSinkConfig section and enter a keyword used as an identifier. In this example, the keyword **HTTP_Trigger** is used.

```
<UrlHandlerAlertSinkConfig type="ObjectVideo.AlertBridge.Plugin.UrlHandlerAlertSinkConfig,
ObjectVideo.AlertBridge.UrlHandler">
    <UrlIdentifier>HTTP_Trigger</UrlIdentifier>
    <ResponseTimeout>10</ResponseTimeout>
  </UrlHandlerAlertSinkConfig>
```

Step 6 Under the Create Response window, click **Custom Fields > New** to specify the URL that will be used when an alert is generated. An example is shown in Figure 5-28. Notice that the Key value matches the previously defined keyword **HTTP_Trigger**.

Figure 5-28 Custom Response Fields

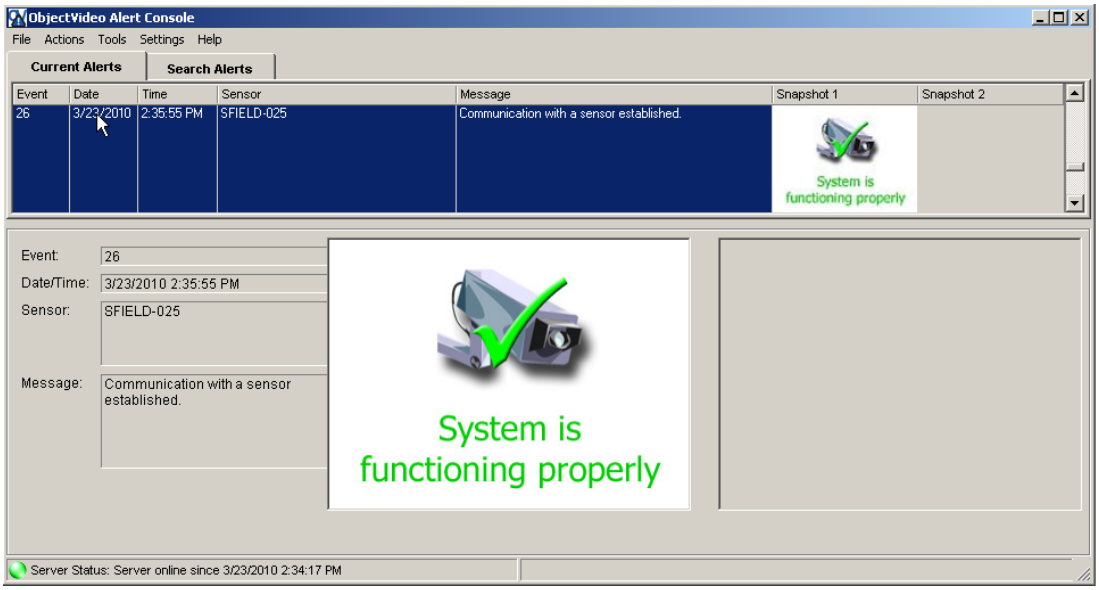


The section Configuring Surveillint to Receive ObjectVideo Alerts, page 5-34 explains how to configure Surveillint to receive alerts from ObjectVideo.

ObjectVideo Alert Console

The Alert Console displays status messages and alerts for each sensor. The Alert Console serves as a way to monitor the connection to all sensors. Figure 5-29 shows an active connection with the new sensor.

Figure 5-29 Communicating with a Sensor

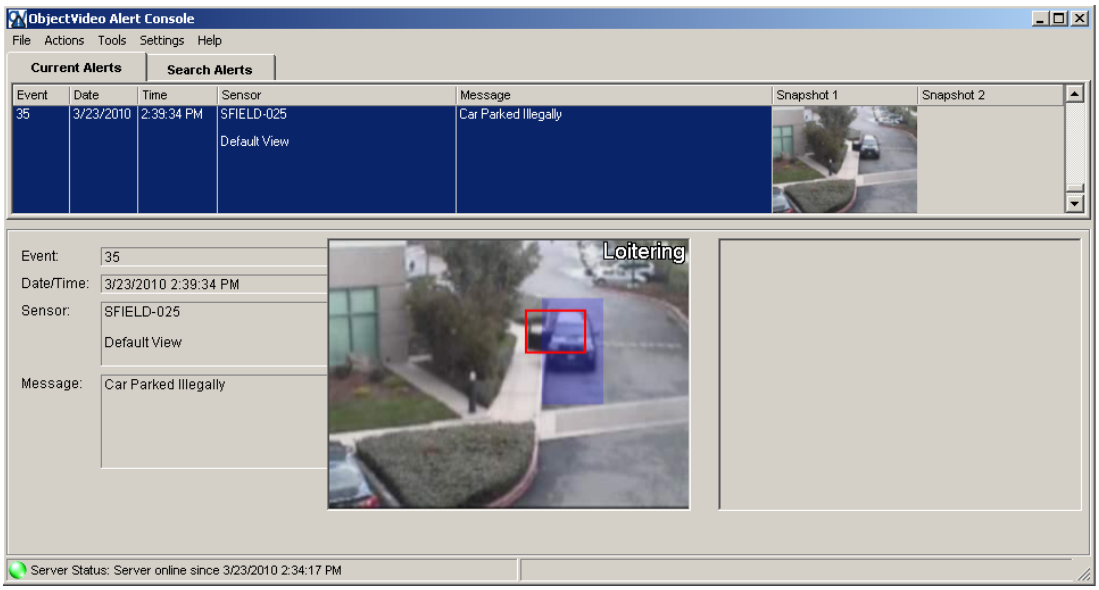


The Alert Console also logs the alerts generated by the video analytics engine. If the system is configured to send an HTTP notification to an external system, an HTTP notification takes place concurrently.

If Surveillint is configured to receive ObjectVideo alerts, the alert is also logged in Surveillint's Operation Console.

Figure 5-30 shows how ObjectVideo detected a car parked illegally for more than 45 seconds and an alert was generated.

Figure 5-30 Car Parked Illegally Alert



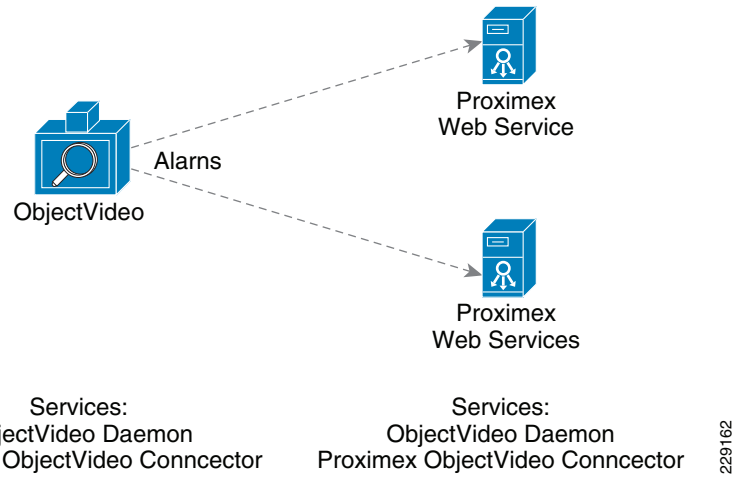
Note A detailed log for each sensor is saved under the *C:\Windows\Temp* directory. The filename is based on the Sensor ID; for example, *Sensor-0d9a2b06-07ea-4df6-a1c4-8ee2eb71a77b.log*.

Configuring Surveillint to Receive ObjectVideo Alerts

By using the ObjectVideo Integration Module, Surveillint is able to receive alerts directly from the ObjectVideo server. This allows Surveillint to receive alerts directly into the Operation Console. By mapping the alerts to the proper sensor, the alerts may be associated to a specific monitoring area.

Figure 5-31 shows the services that must be installed on each server for Surveillint to receive alerts from ObjectVideo.

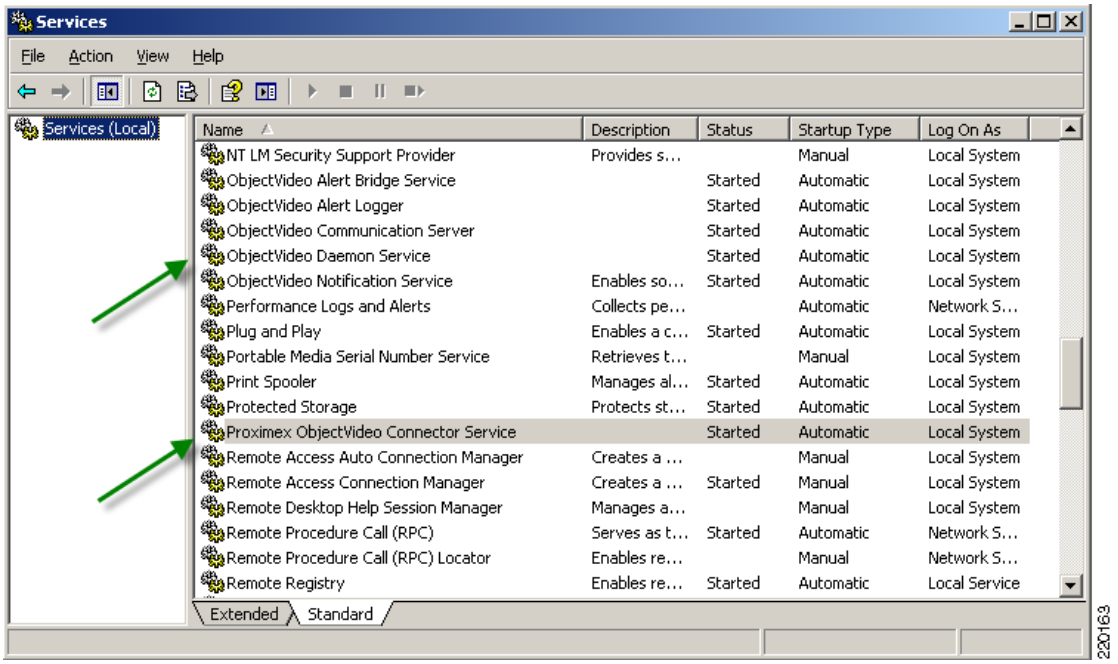
Figure 5-31 Services Required



Perform the following steps:

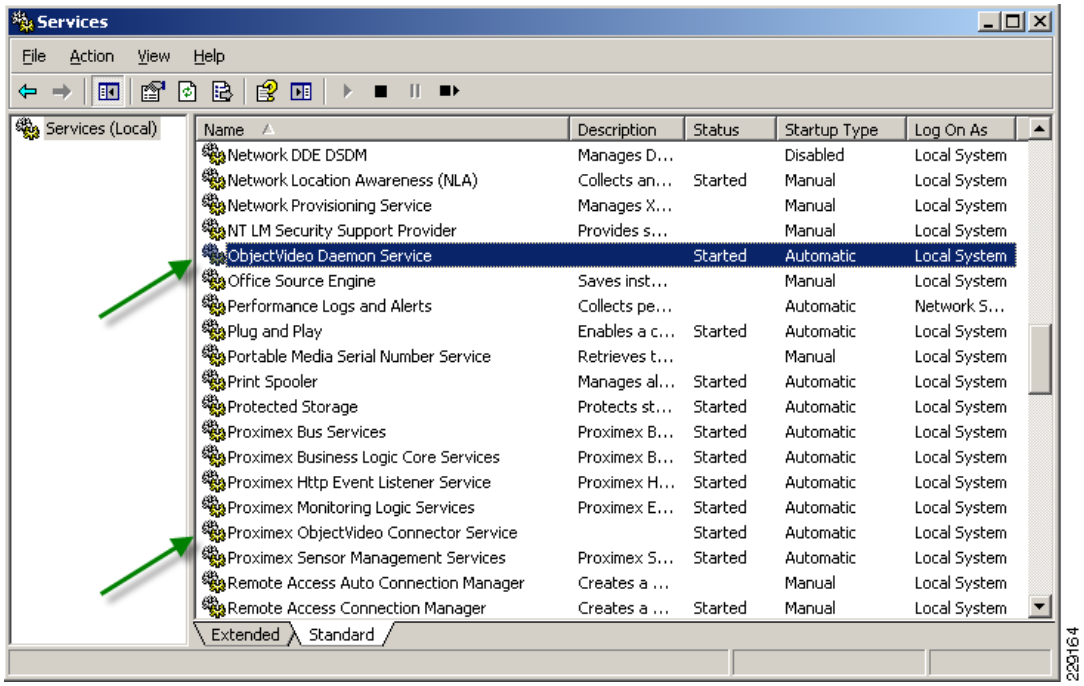
Step 1 On the ObjectVideo server, verify that the ObjectVideo Daemon Service is running and install the Proximex ObjectVideo Integration Module on the same server. The Integration Module is provided by Proximex as a **ProximexOVSetup.msi** installation file. Figure 5-32 shows the services running on the ObjectVideo server.

Figure 5-32 ObjectVideo Services



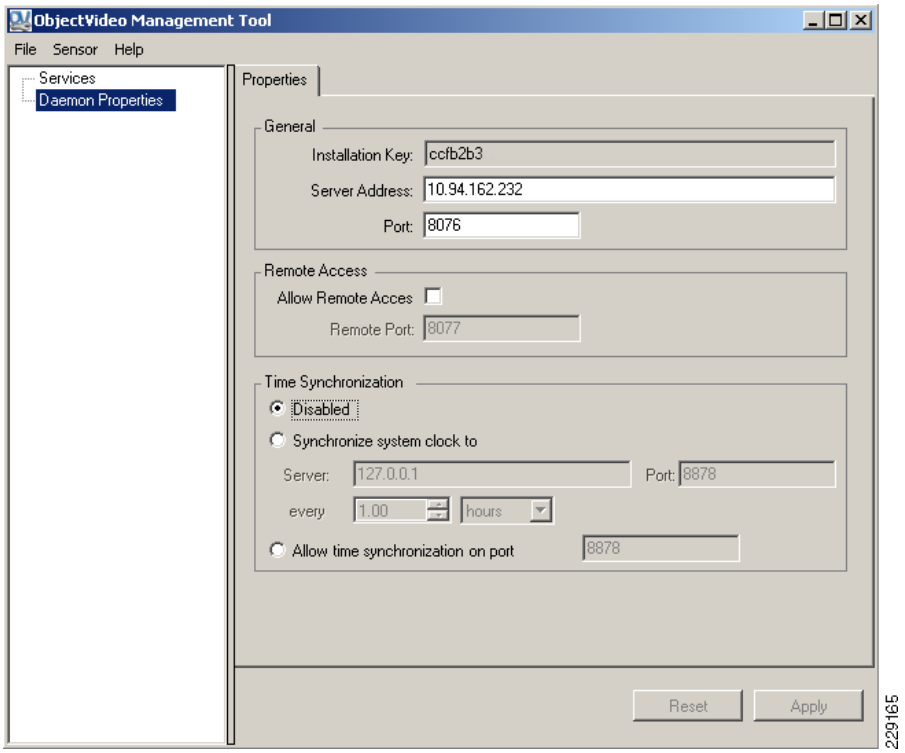
Step 2 On the Surveillint server, install the ObjectVideo Management Tool to receive alerts from ObjectVideo. A new service, *ObjectVideo Daemon Service* is installed in the Surveillint server, as shown in Figure 5-33.

Figure 5-33 Surveillint Services



Step 3 On the Surveillint Server configure the daemon properties by launching the ObjectVideo Management Tool, as shown in Figure 5-34.

Figure 5-34 Daemon Properties



Step 4 Enter the installation key that was used to install the ObjectVideo server.

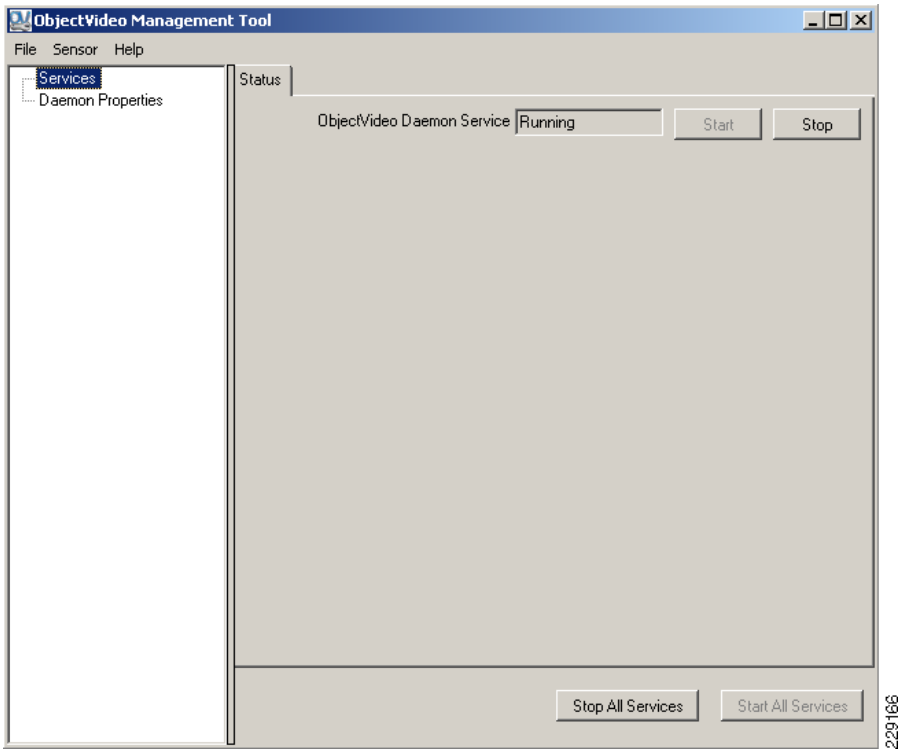
Step 5 Enter the IP address of the ObjectVideo server.

Step 6 Enter the Port number for the ObjectVideo server. The default port number is 8076.

Step 7 Restart the **ObjectVideo Daemon Service** to activate these changes.

Step 8 Click on **Services** to start and stop the service, as shown in Figure 5-35.

Figure 5-35 Restart the Daemon Service



Step 9 If the Surveillint Web Service is installed on a different machine, modify the connector's configuration file *C:\Program Files\Proximex\Services\Config\PxConnectorConfig.xml*.

Note For detailed installation instructions, follow the **Configure ObjectVideo Integration Module** provided by Proximex.

Receiving Alerts from ObjectVideo

For ObjectVideo alerts to be linked to the proper sensor in Surveillint, a sensor map should be configured. Sensor mapping within Surveillint refers to a two-way event connector that synchronizes information in Surveillint with information from ObjectVideo or other external systems.

Sensor mapping works by correlating the sensor name in Surveillint with the name of the same device in ObjectVideo. Sensor mapping enables Surveillint to raise alerts in the appropriate sensor when an alert occurs with the actual sensor device. To obtain video for an alert, Surveillint uses the camera sensor that is a member of the group to which this sensor belongs.

To create a sensor mapping for the ObjectVideo sensor, perform the following steps:

Step 1 Click on **Event Integration > Sensor Mapping** in the Administration Console.

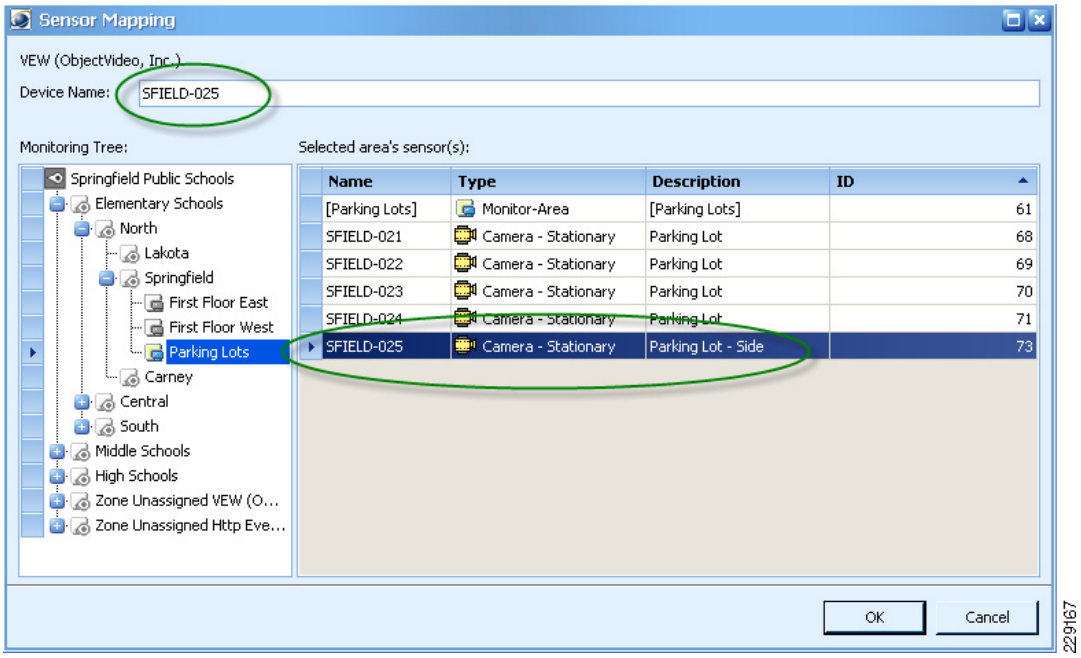
Step 2 Under Application Name, select **VEW (ObjectVideo, Inc.)**

Step 3 Click **Add…**

Step 4 Under Device Name, enter the device name used by ObjectVideo (*SFIELD-025*).

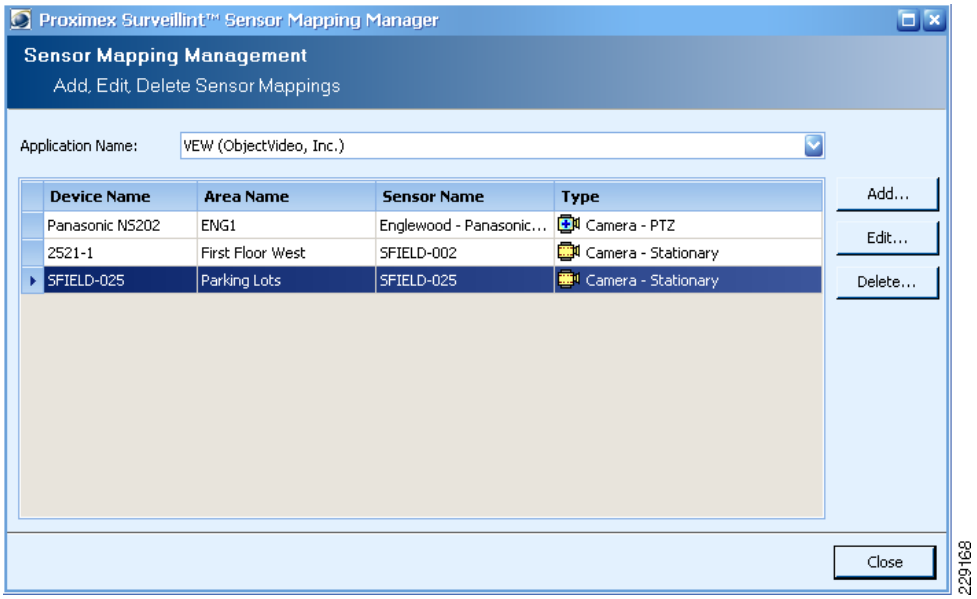
Step 5 Select the monitoring area and sensor to which SFIELD-025 will be mapped (see Figure 5-36).

Figure 5-36 Selecting the Monitoring Area and Sensor



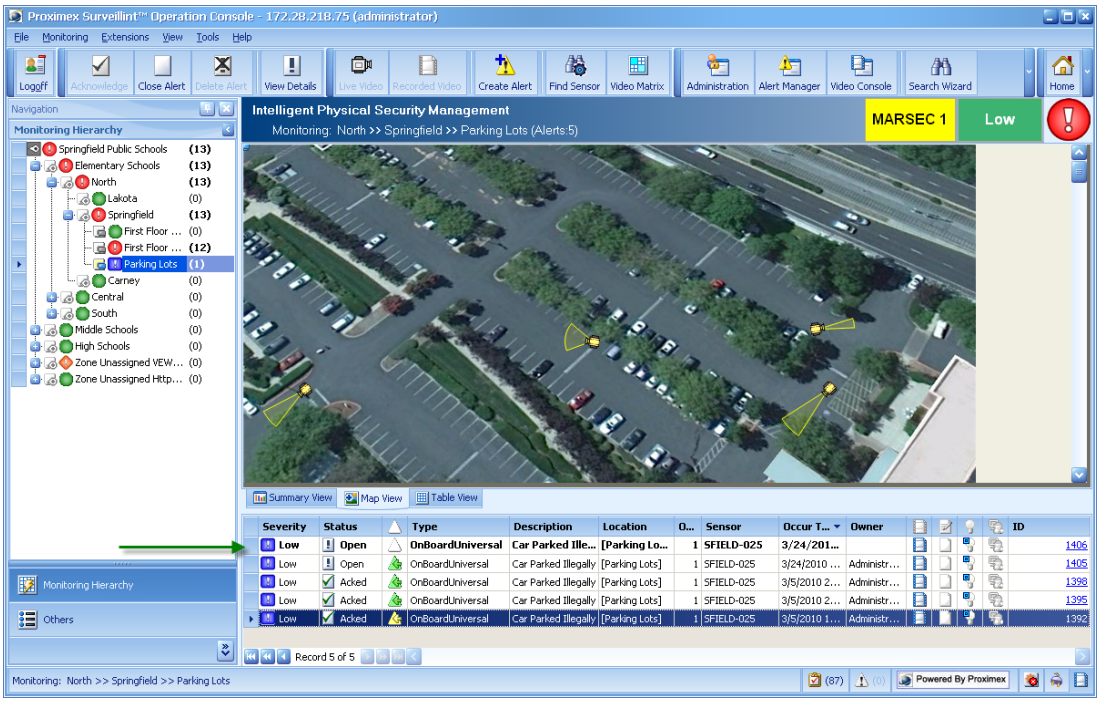
This defines a mapping between ObjectVideo's SFIELD-025 sensor and Surveillint's SFIELD-025 sensor in the Parking Lots area, as shown in Figure 5-37.

Figure 5-37 Sensor Mapping



When a video analytics alert is generated by ObjectVideo on SFIELD-025 sensor, it is simultaneously displayed in the Parking Lots monitoring area of Surveillint, as shown in Figure 5-38.

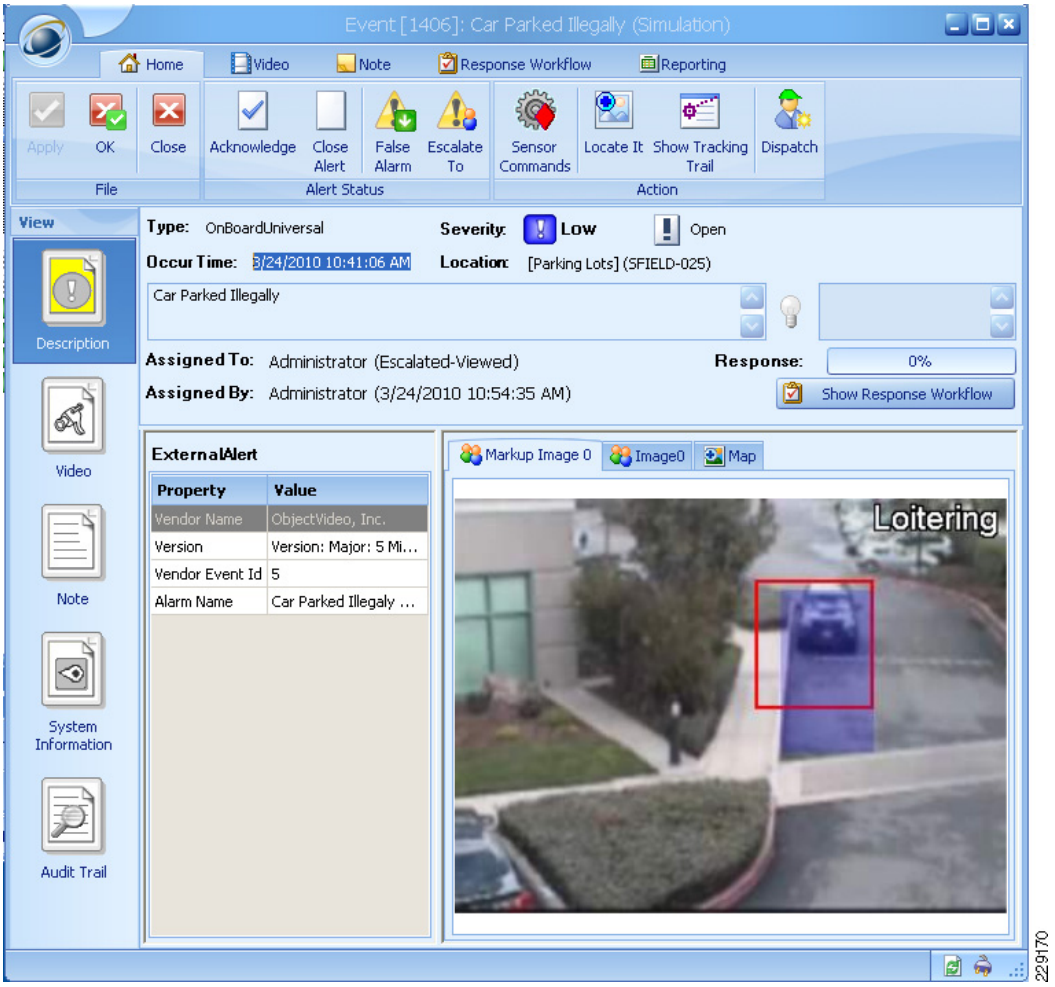
Figure 5-38 ObjectVideo Alert in Surveillint



The ObjectVideo Integration Module allows the operator to analyze alerts using a single command and control environment and to follow a pre-defined response workflow or checklist of actions to take during certain types of alerts.

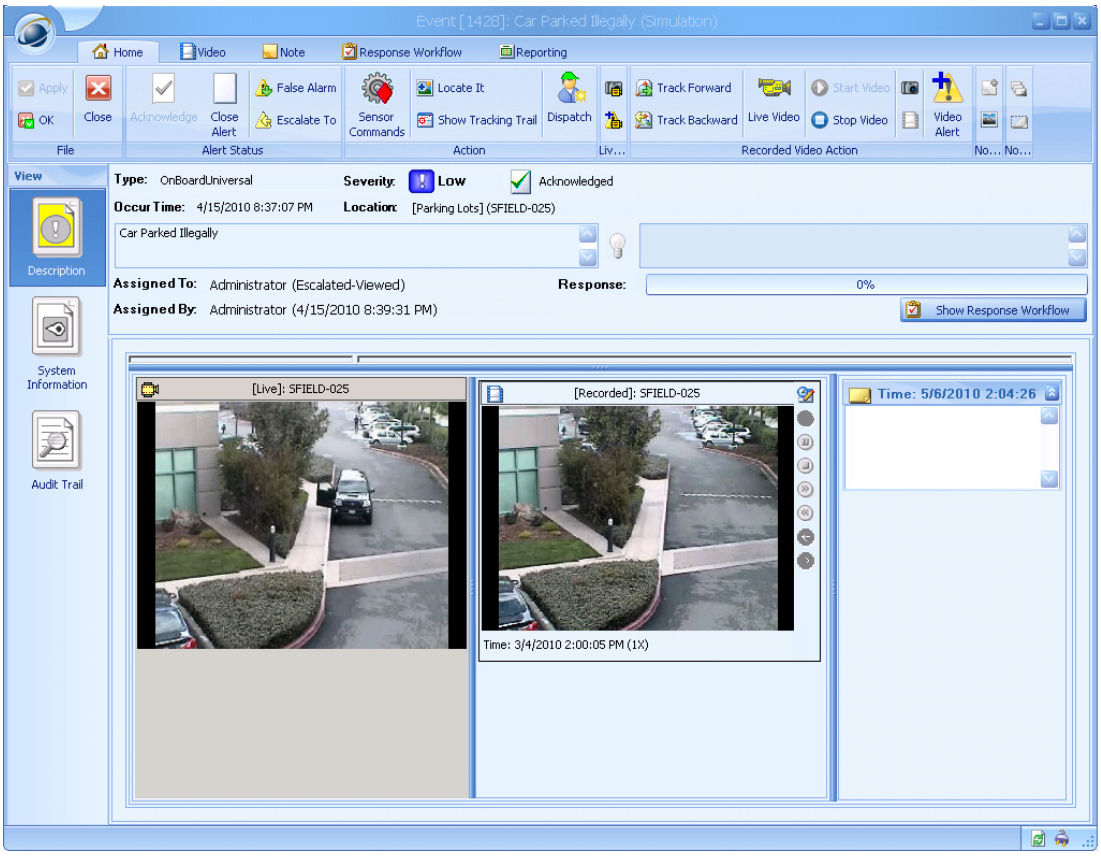
By double-clicking on the new alert, the operator can review the event details. Figure 5-39 shows an alert in Surveillint originated by ObjectVideo.

Figure 5-39 Video Analytics Alert



The sensor mapping also links the alert to a specific sensor in Surveillint, allowing the operator to view live and recorded video from the same event window, as shown in Figure 5-40.

Figure 5-40 Live and Recorded Video



The single event window also allows the operator to review the event and provide features such as the following:

- Finding the location of an alert
- Viewing sensor activities
- Viewing live and recorded video
- Response workflow
- Miniature map
- Follow suspects with EZ-Track
- Export video to a file
- Escalate alerts and add notes to the alert
- Create administrative reports

These and other Surveillint features allow the operator to have a single command and control console to quickly address security breaches. Some of these features are shown in more detail in Chapter 6 - scenarios.

Integrating Surveillint with other Systems

Video Integration with Cisco Video Surveillance Operations Manager

Surveillint provides video integration with a large number of video servers and matrix systems, allowing operators to manage diverse systems using a single console. The source or system manufacturer becomes irrelevant to the operator, because all camera feeds are aggregated to view live and recorded video on a single application.

To integrate video cameras from the Cisco Video Surveillance Operations Manager (VSOM), the ActiveX client must be installed on every machine running Surveillint's Administration Console or the Operation Console. A simple way to do install the ActiveX client is to connect to the Video Surveillance Operations Manager (VSOM) and display a video feed. The first time the client connects to VSOM, the proper ActiveX controls are automatically installed.

Before integrating with third-party systems, a video adaptor provided by Proximex must be installed for the proper system. The proper recording system's SDK must also be installed. For integration with VSOM or VSMS, the file name should be similar to: *PxVideoAdaptorSetup-Cisco6.2.msi*.

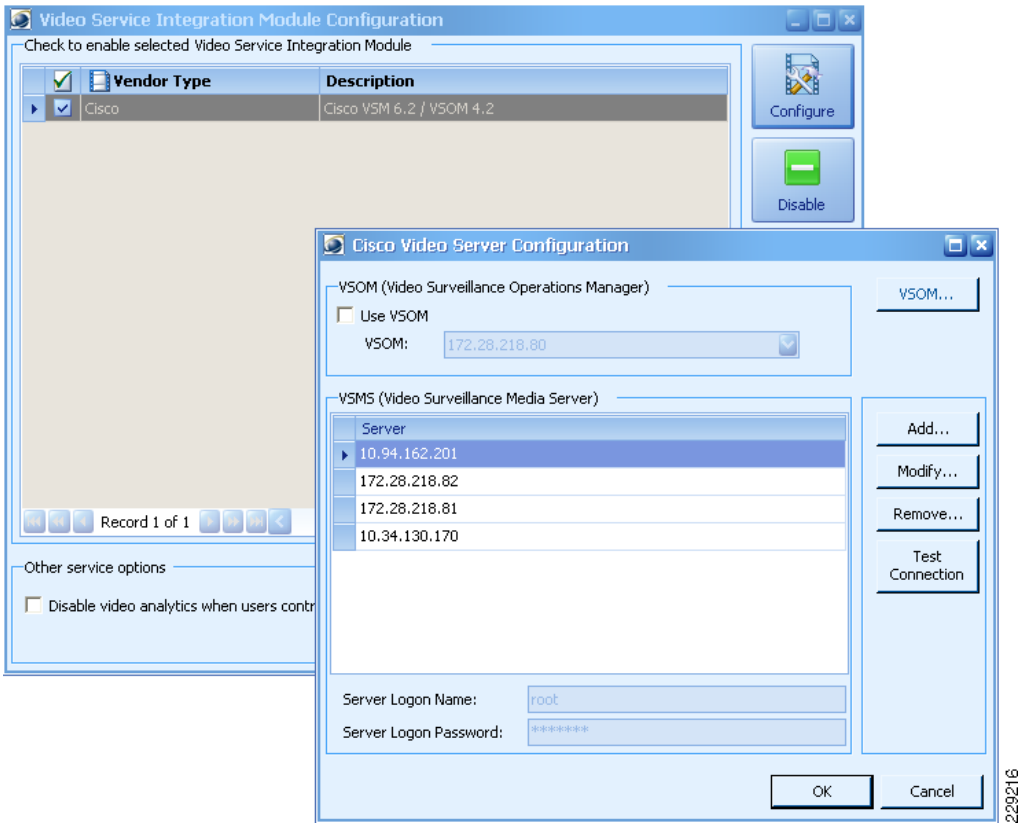
Note Contact Proximex for an updated list of video servers that have been integrated with Surveillint.

To configure a video integration with VSOM, perform the following steps:

Step 1 Select **Video Integration > Video Services** from the Administration Console.

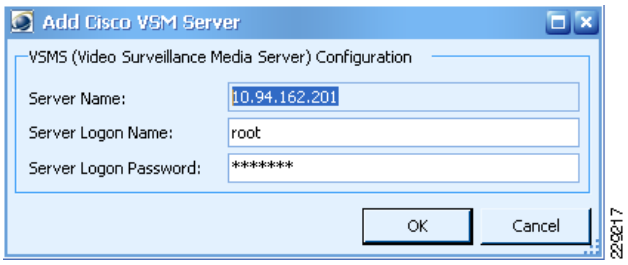
Step 2 Select Cisco VSM6.2 /VSOM 4.2 and click **Configure** (see Figure 5-41).

Figure 5-41 Configuring Video Server



Step 3 Enter the IP address and logon information for the selected server and click **Test Connection** to verify the settings (see Figure 5-41).

Figure 5-42 Verifying the Settings



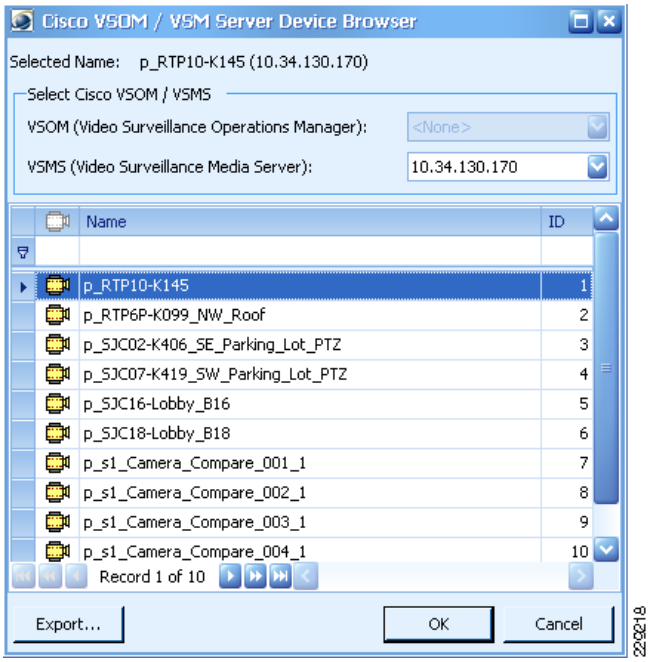
After the integration with VSOM has been defined, the IP Cameras may be added as sensors using the Administration Console.

Step 4 From the Administration Console, click **Environment > Sensors > Add.** The **Add New Sensor** appears.

Step 5 Enter a new Sensor Name and select **Sensor Type** from the pull-down menu.

Step 6 Click **Device ID > Value** and select the Cisco VSMS server from the pull down menu. The cameras available to that server appear, as shown in Figure 5-43.

Figure 5-43 Available Cameras



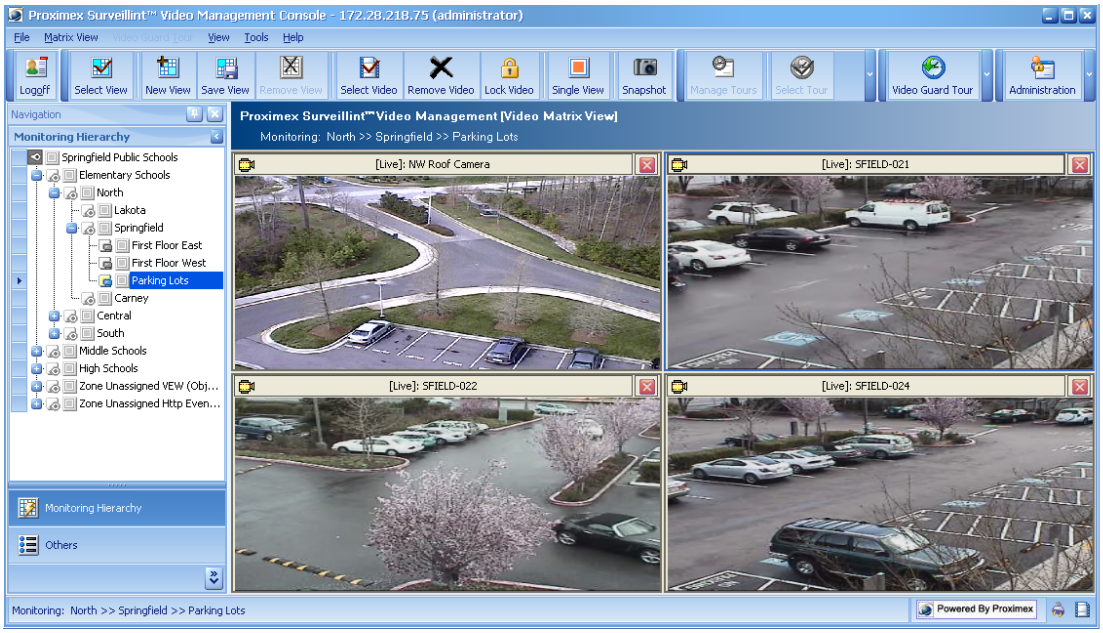
Step 7 A location must be specified for the sensor. The final sensor configuration should include the Location Name. Select a value for the sensor's location and click **OK**.

Step 8 The new sensor should be listed in the **Sensor Management** screen. To test the video stream, click on **View** to launch the Live Video Viewer for that camera.

After the sensor is added to the appropriate Monitoring Area, it can be displayed using the Video Management Console, along with other cameras. The Surveillint system automatically links to the recorded video for that camera.

The Surveillint Video Management Console allows operators to view video streams side-by-side in a matrix format and configure the new guard tours that rotate camera views at predefined intervals. The Video Management Console may be launched from the Windows Start menu or by clicking the Video Console icon on the Operation Console. Figure 5-44 shows the newly defined sensor along with other cameras in the Parking Lots Monitoring Area.

Figure 5-44 Video Management Console



Note For more details on placing sensors in the proper area of the Monitoring Environment, review Surveillint's Administration Guide.

Exporting and Importing Sensors

Surveillint offers the option to import and export sensors using XML files. These XML files may be edited using Microsoft Excel. This feature provides a flexible way to manage the sensor environment in deployments with a large number of sensors.

To use this capability, see the Proximex Administering Surveillint Guide.

Sensor Integration and Grouping

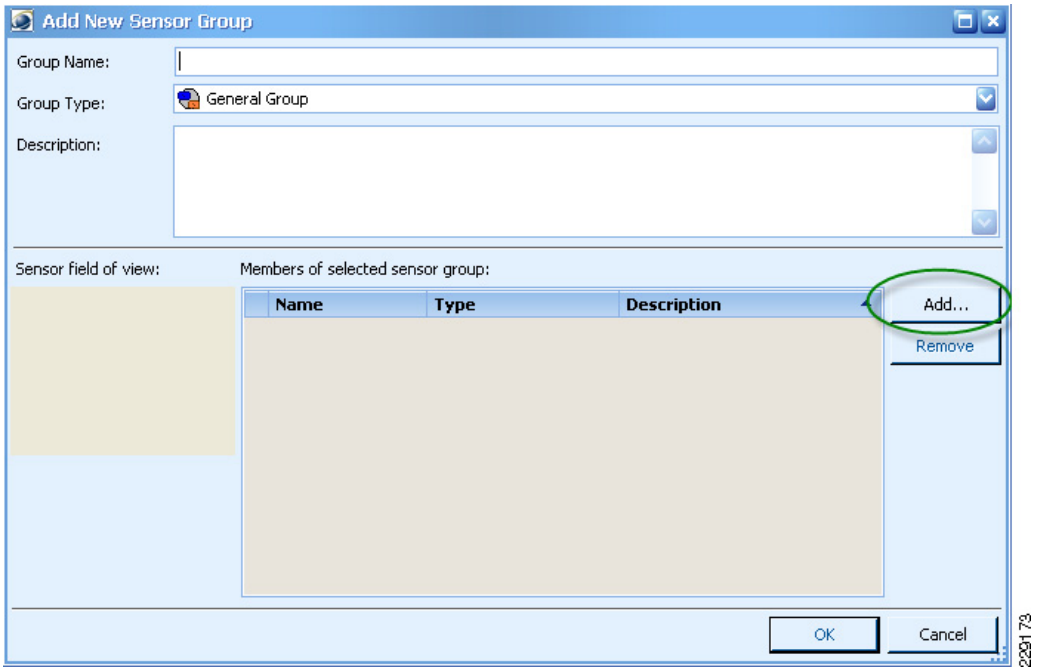
In Surveillint, every physical sensor in the environment, such as video cameras and access control devices, needs to be very presented with a sensor definition. Surveillint integrates with a wide variety of sensors.

A sensor group associates sensors designed to collect information about incidents occurring in a certain location. For example, a video camera sensor may be associated with an access control door so when an alarm occurs at the door video from the incident is linked to the right video camera.

To associate an access control door with a video camera sensor, perform the following steps:

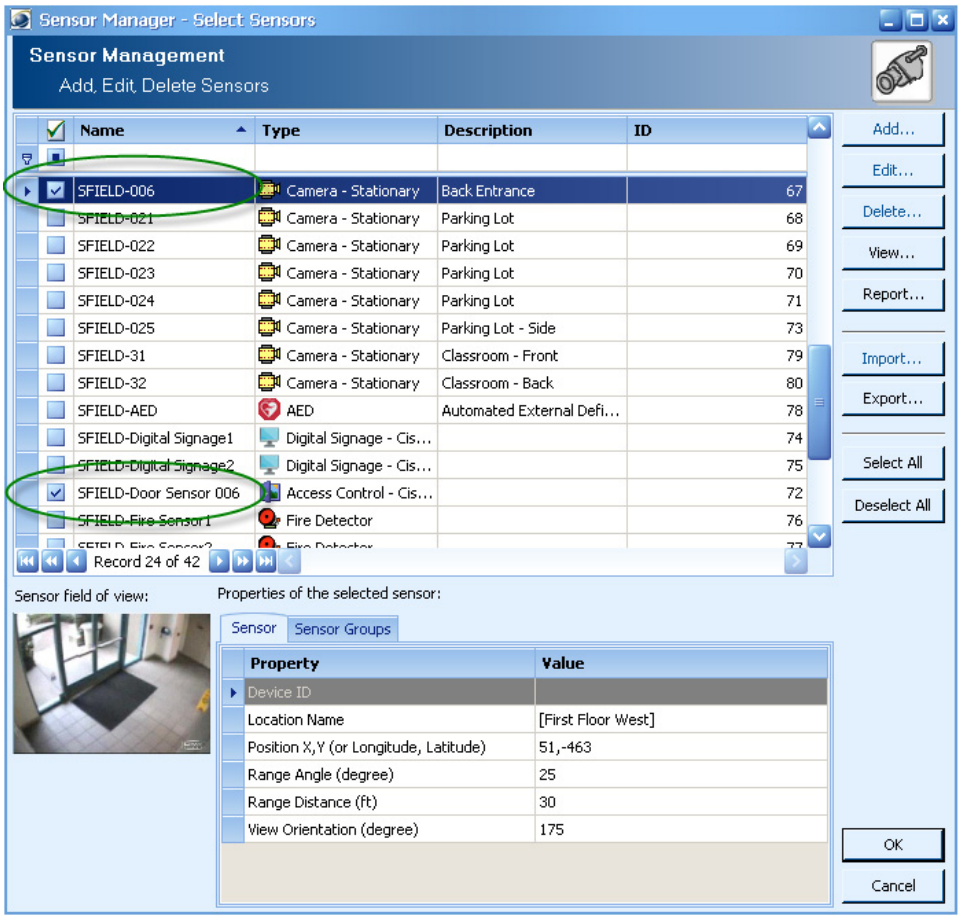
Step 1 Launch the Administration Console and click on **Environment > Sensors > Sensor Group > Add,** as shown in Figure 5-45.

Figure 5-45 New Sensor Group



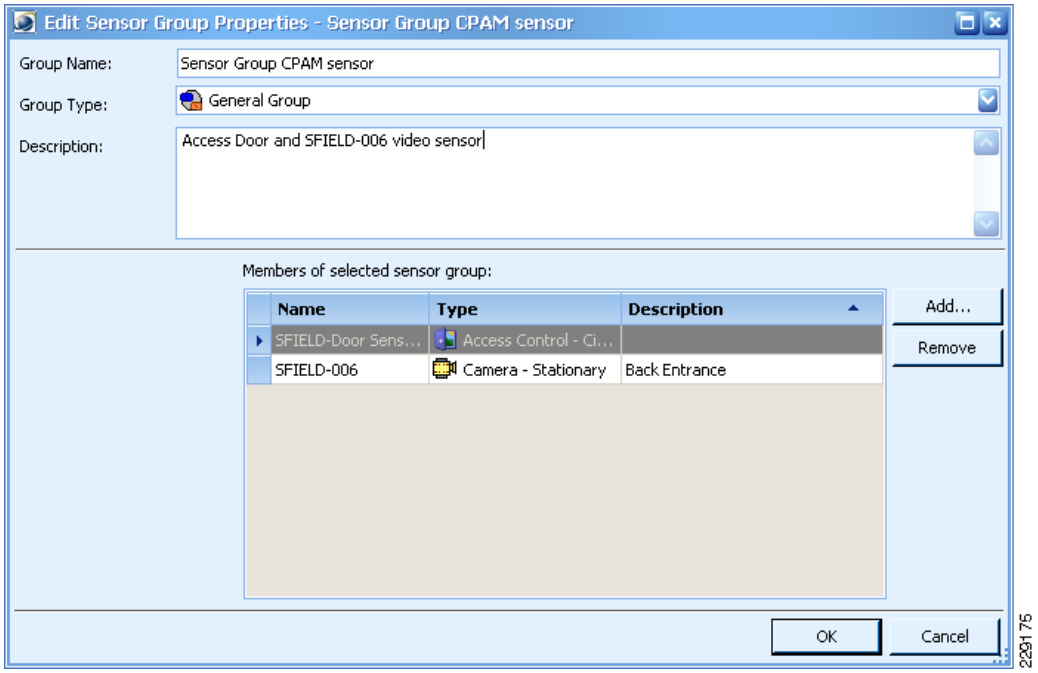
Step 2 To add members to the new group, click **Add** and select the new members by clicking the check box for each sensor, as shown in Figure 5-46.

Figure 5-46 Group Members



Step 3 Give the sensor group a name and description. The new sensor group is shown in Figure 5-47 and includes an access control door and a video camera sensor, both located in the same general location.

Figure 5-47 Sensor Group Properties



Simulating Alerts with Business Logic Policies

Surveillint provides a flexible and powerful way to customize default business logic policies that determine pre- and post-alert processing and response management actions that should be taken when certain alerts are raised. These business logic policies capture processes and requirements for alert response based on the alerts status, schedule, monitoring area, and threat level. These policies allow security personnel to concentrate on execution of planned responses instead of reassessing unfolding situations.

Surveillint's Business Logic engine uses the advanced Business Logic engine embedded in Microsoft's .NET Framework. The following section provides a high level configuration guide. For more detailed screenshots and steps, please refer to the Proximex Administering Surveillint Guide.

For testing purposes, Business Logic may be used to simulate alarms and to test different alert conditions. Perform the following steps:

Step 1 From the Administration Console, click **Business Logic > Business Logic Designer**. A blank business logic rule should be loaded.

Step 2 Surveillint has several business logic policies already defined as templates. Copying an existing policy is a simple way to get started. Click on **Templates > Open Business Logic Template** and select the existing **Simulated alert** template.

This open a template with basic shapes used to simulate an existing alert. A large number of additional actions, decisions and commands may be added to a policy.

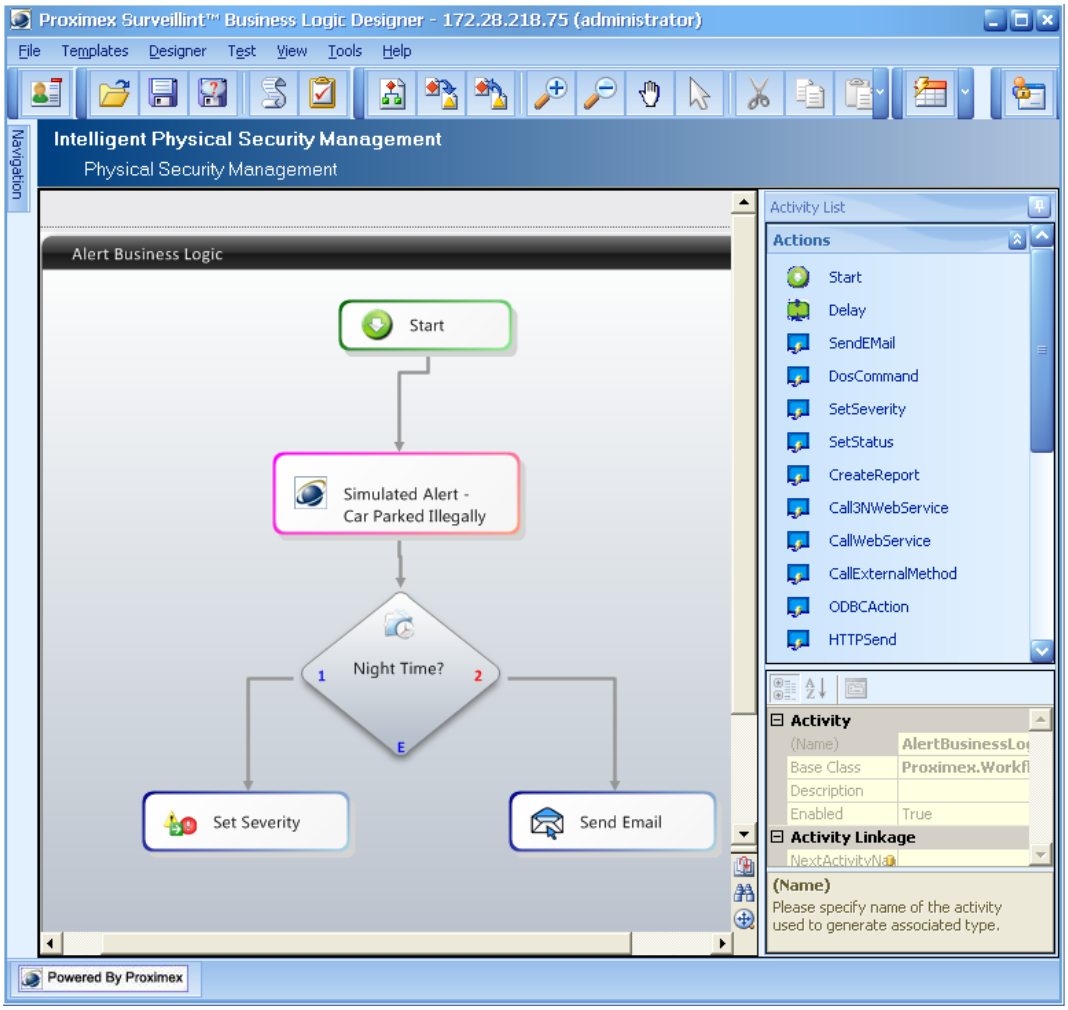
Step 3 To simulate an existing alert for testing purposes, edit the Simulate Alert component by double-clicking the **Simulate Alert** activity.

Step 4 Click **Select Alert** and locate an existing alarm that will be used for testing purposes. Give the component a name, description and severity.

A real alarm was previously generated by ObjectVideo, and a copy of that alarm may be used for simulation purposes or for testing additional configuration options, such as response work flow, sending E-mail notifications, create reports, and so on.

The simulated alert may have more relevance if a car is parked in a restricted area (parking too close to the building) during certain times. The Schedule activity can also be used to define different policies to be enforced during different times of day. For example, based on the time of the day, the alarm's severity could be automatically raised to High, or an automatic e-mail could be generated to certain security personnel members, letting them know about the incident. Any combinations of security workflow can be created with the Business Logic Designer and Surveillint's predefined list of decision and action activities. (See Figure 5-48.)

Figure 5-48 Business Logic



It is recommended to test the business logic rule to make sure that the policy flow works as expected before applying it to the security environment. Testing and debugging of business logic rules in a production environment is not recommended, because false information would appear on the security operator's console.

To test the business logic rule, perform the following steps:

Step 1 Click on **Test > Test – Start**.

Step 2 To pause the execution at certain activities, select the appropriate component in the business logic rule and click **Test > Test – Set Breakpoint.** A red dot appears on the icon where the execution will be paused.

The Operations Console should display the new alert generated by Business Logic.

The previous example offers just a glimpse into the power of Surveillint's Business Logic rules. Other business logic activities include:

- Action Activities—These activities define what should happen when conditions are met. They have a single output point. An example of some of the action rules include:
  - Send e-mail messages
  - Launch a DOS command
  - Set the alert's severity
  - Create reports
  - Call a Web Service, including a service URL or WSDL URL
  - Send an HTTP notification to an external system, including User Name and Password
  - Run a custom ODBC SQL script against a data source
  - Call a Child Business Logic rule
- Decision Activities—These activities specify conditions under which certain actions should occur. They have multiple output points. The component decides which branch of the rule to execute based on. A few examples of the decision activities include:
  - The alert's severity or status
  - A pre-defined schedule
  - The monitoring zone or area issuing the alert
  - The Homeland Security or MARSEC threat level
  - GPS location
- Decision + Action Activities—These activities specify conditions under which specific actions should occur. They have multiple output points. A few examples of the Decision + Action activities include
  - PowerShell scripts. Microsoft's PowerShell must be installed on the system.
  - Escalate an alert to a specific user or group based on certain criteria
  - Correlate multiple alarms across multiple systems. See the following section for an example.
  - Run custom ODBC SQL scripts and make decisions based on the data returned

- Sensor Command Rules—These activities enable specific actions to be taken on particular sensors such as doors, cameras and other sensors. A few examples of the Sensor Command Rules activities include:
  - Open a door
  - Lock a door
  - Open a door momentarily

Note To obtain a full list of these Business Logic Activities, learn more about the properties of each component and to fully understand the power of Business Logic Rules, review Proximex's Administering Surveillint Guide.

HTTP URL Notification with Surveillint

Surveillint is not only able to provide integration with third-party systems, but is also able to receive HTTP URL notifications to create events. By listening to events from other systems, Surveillint provides a rich environment to manage alarms from many diverse systems. A good example is to use VSOM to send a URL notification to Surveillint when motion is detected by an IP camera.

Surveillint provides an integration module that listens to alerts on a specific port. The default TCP port is 9001, but may be modified as necessary. To get more detailed information on how to set up this capability, install Surveillint HTTP Event Listener and refer to the included documentation.

As an example, the following URLs were launched from one of the allowed hosts and generated events in Surveillint.

- http://172.28.218.75:9100/motion?SensorID=Englewood%20-%202500-1&AlertSeverity=2&AlertDescription=Smoke+Alert&AlertText=Smoke+Detected&AlertType=Smoke%20Alarm&AlertName=Smoke+Detected
- http://172.28.218.75:9100/motion?SensorID=Englewood%20-%204300-1&AlertSeverity=2&AlertDescription=Forced+Entry&AlertText=Forced+Entry&AlertType=Forced&AlertName=Forced+Entry
- http://172.28.218.75:9100/motion?SensorID=Englewood%20-%204500-1&AlertSeverity=2&AlertDescription=Fire+Alert&AlertText=Fire+Detected&AlertType=Fire+Alarms&AlertName=Fire+Detected

Figure 5-49 shows Surveillint's Alert Console, displaying the three new alerts.

Figure 5-49 URL Event Notifications

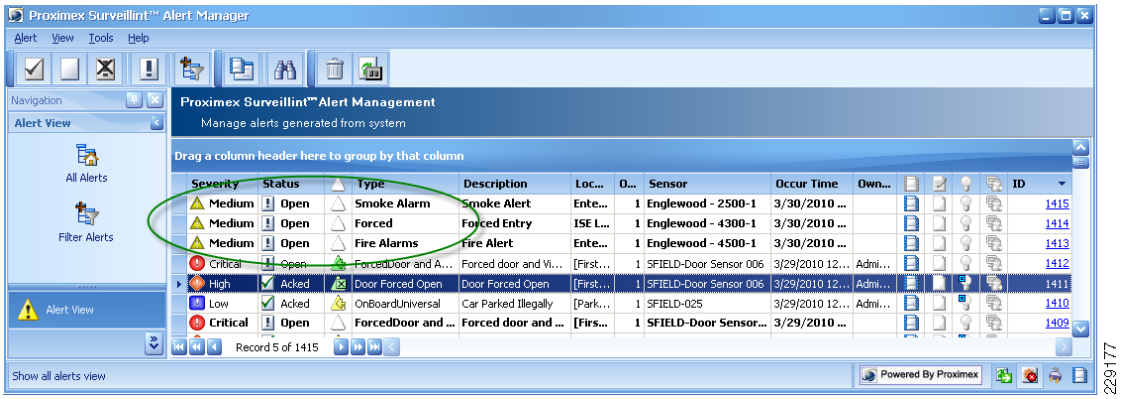
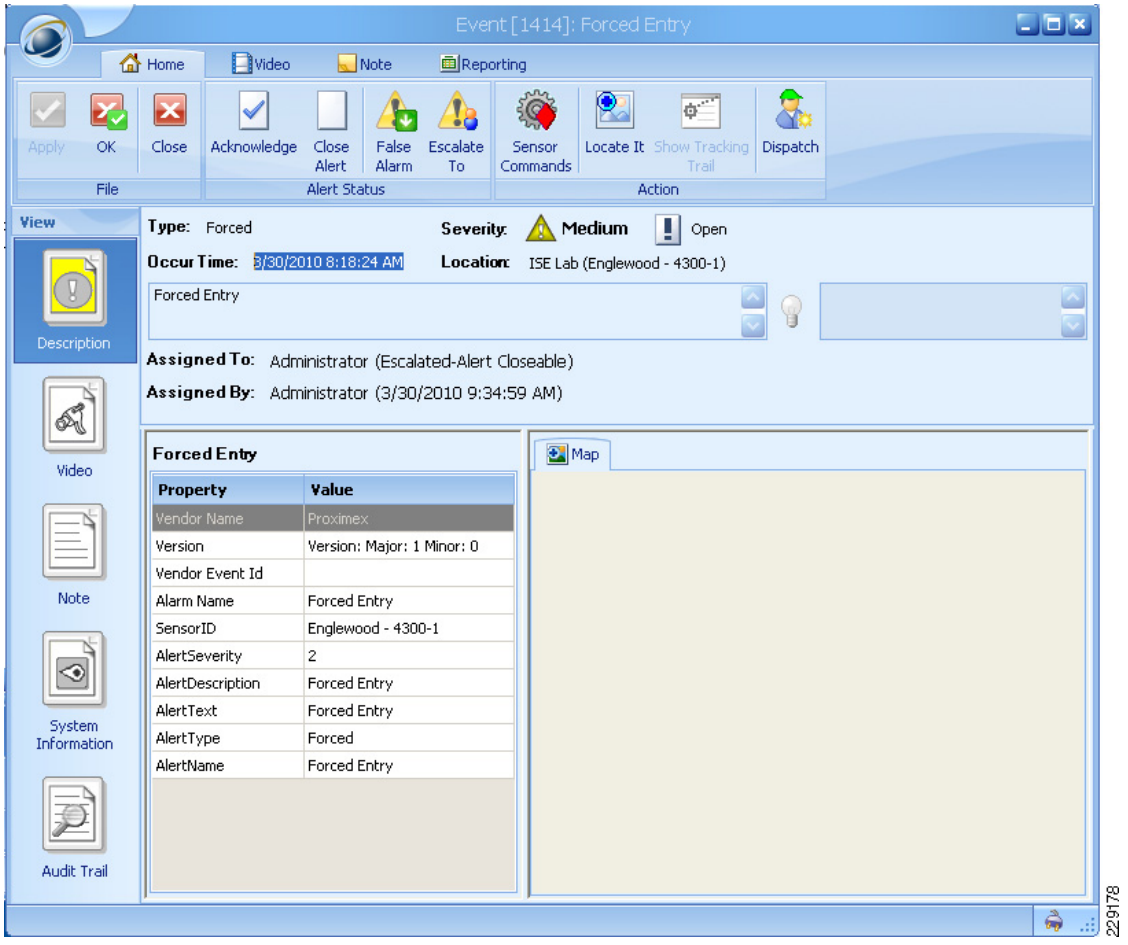


Figure 5-50 shows the new event and the parameters that were passed by the URL notification. The event is created and located in the monitoring area according to the sensor used in the URL.

Figure 5-50 New HTTP URL Notification



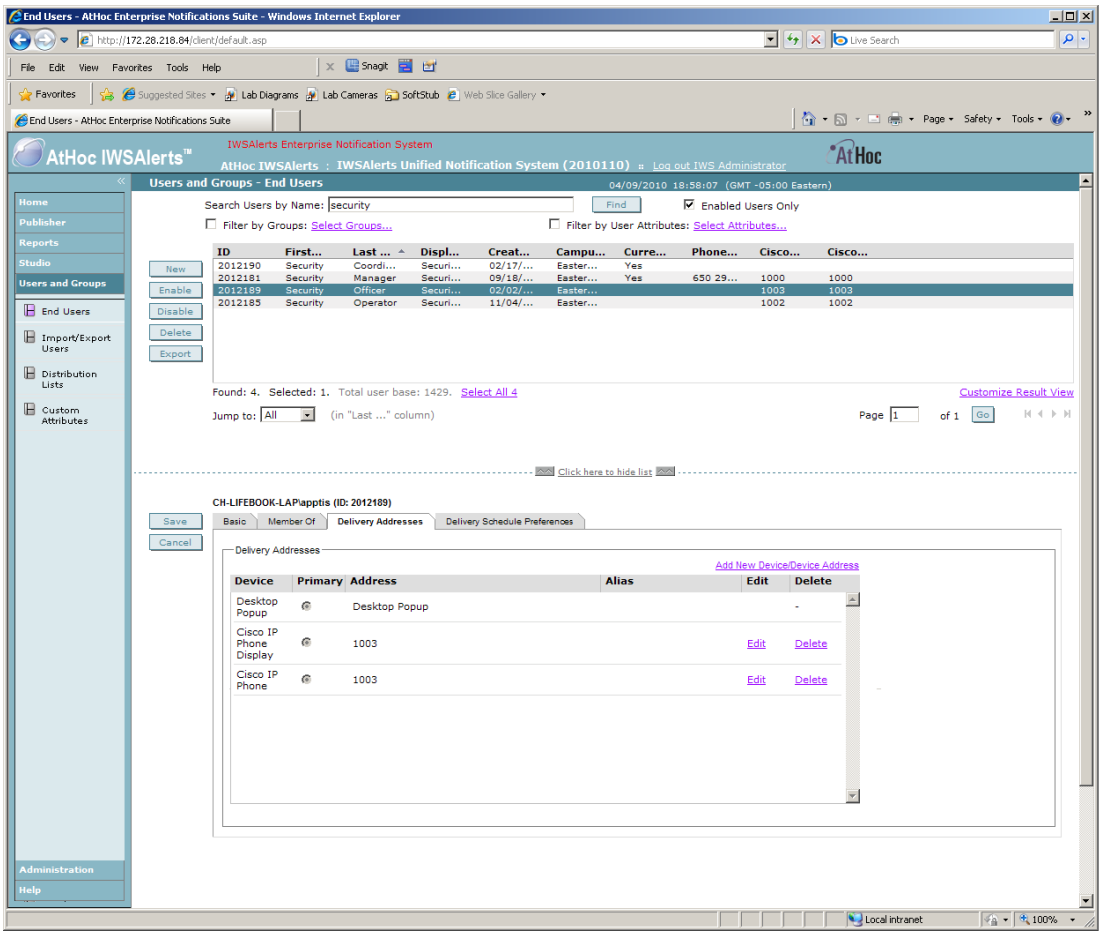
AtHoc Integration

AtHoc typically integrates with other applications or hardware through its API.

Before integrating with another application, test whether AtHoc can be triggered from a URL. For example, in case of a forced entry incident, notification should be sent to security. The following steps trigger this notification from a URL:

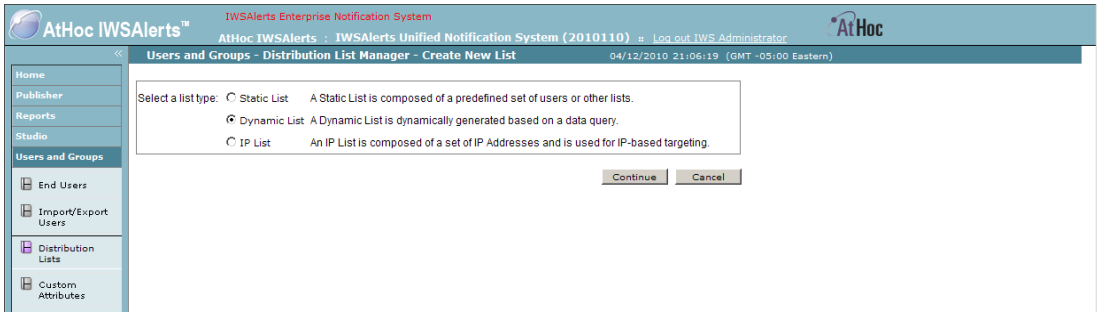
Step 1 Figure 5-51 shows how to create end users. In this example several end users are created. They have extension number 1000, 1002, 1003 respectively.

Figure 5-51 Create End Users



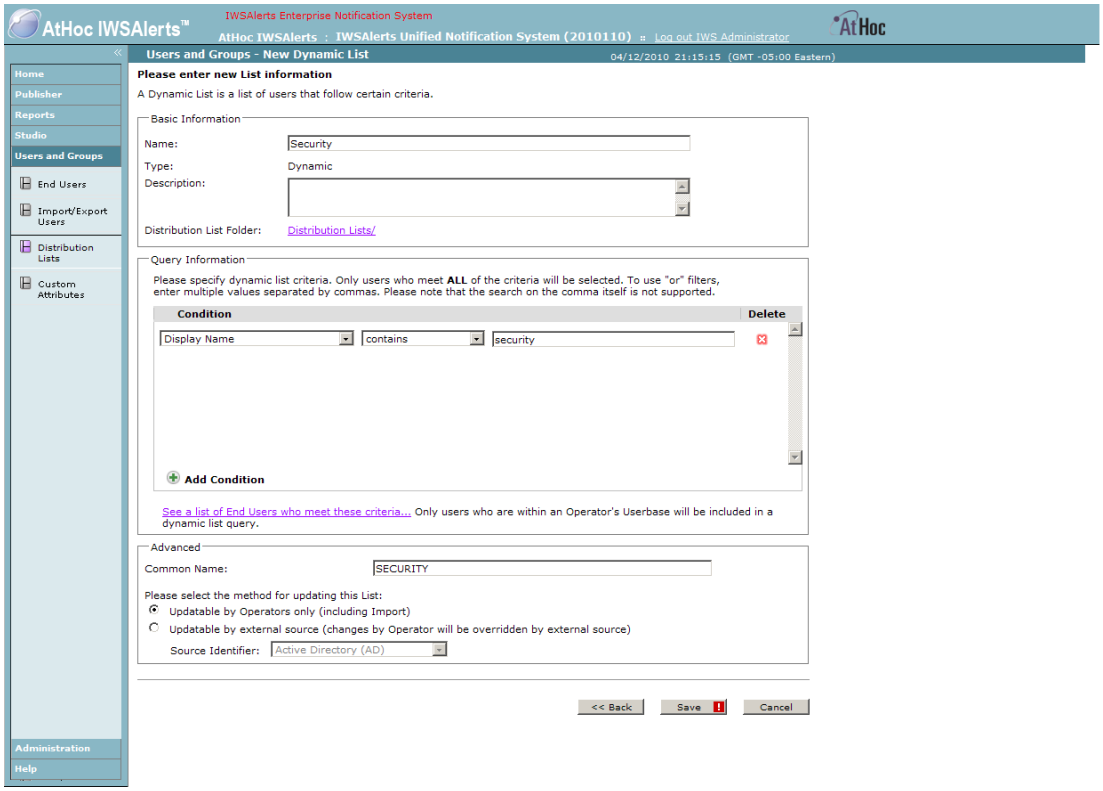
Step 2 Create a distribution list, as shown in Figure 5-52.

Figure 5-52 Specify a Dynamic List



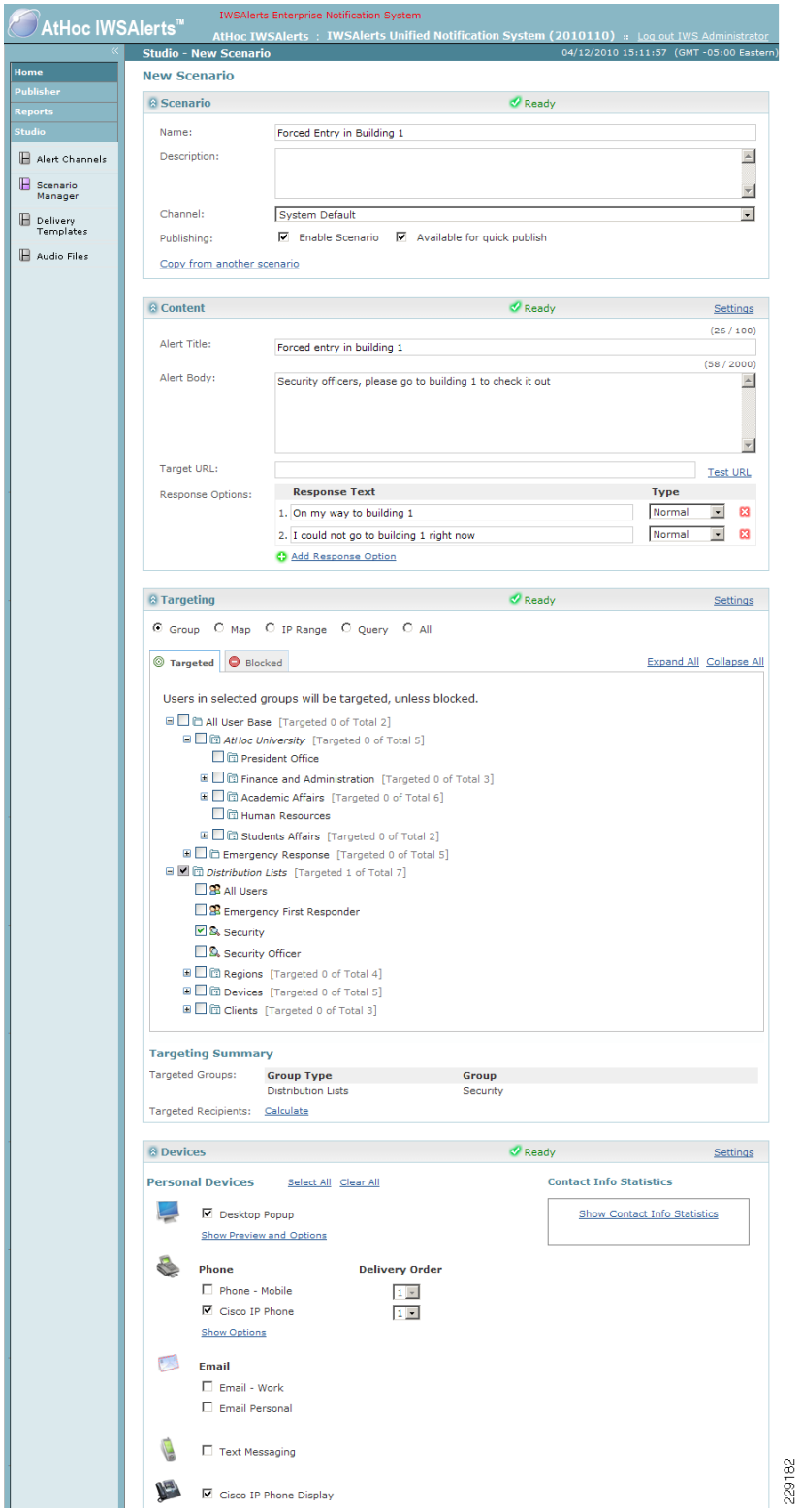
Step 3 Specify conditions for the list, as shown in Figure 5-53.

Figure 5-53 Specify Conditions for the List



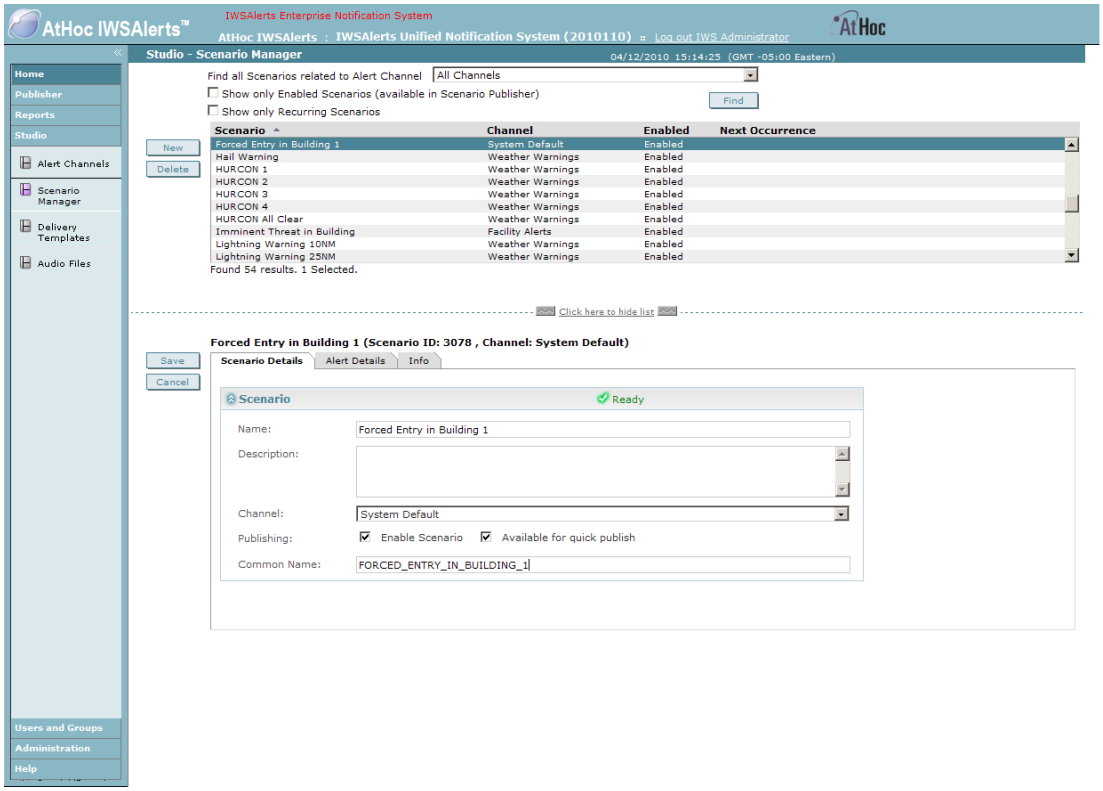
Step 4 Create a scenario, as shown in Figure 5-54. Here a scenario called “forced entry” is created.

Figure 5-54 Create a Scenario—Forced Entry



Step 5 Specify **Common Name** and click the **Save** button. Figure 5-55 shows "FORCED_ENTRY_IN_BUILDING_1" is entered as common name.

Figure 5-55 Specify "Common Name" for Newly Created Scenario



Step 6 Open Internet Explorer and enter the following URL:
http://172.28.218.84/corp/gw/gw.asp?scenario=FORCED_ENTRY_IN_BUILDING_1

Note that "Common Name" specified in previous step is included in the URL.

Phones will ring to notify about the forced entry incident.

This URL gateway is a sample wrapper around AtHoc IWSAlerts APIs, which are used for the actual activation of the scenario. Production level integration would leverage the embedded authentication of the activation flow to ensure only authorized sources can activate scenarios.

Integrating AtHoc and Surveillint

Integration between AtHoc and Surveillint can be configured in multiple ways. One way is to use the business logic of Surveillint, where notifications are sent to AtHoc based on certain criteria such as severity, alert type, location of event, and so on. See chapter 5.1 for an example of triggering AtHoc based on business logic.

Additionally, notification to Athoc can occur as a manual action from the operation console, which is detailed below.

Incidents are reported to physical security information management software, which trigger actions according to user configuration. For example, when a forced entry occurs, notification should be sent to security officers.

A user can set up actions for an alert through Surveillint's "Extension" or "Dispatch Button", where one URL or multiple URLs can be specified.

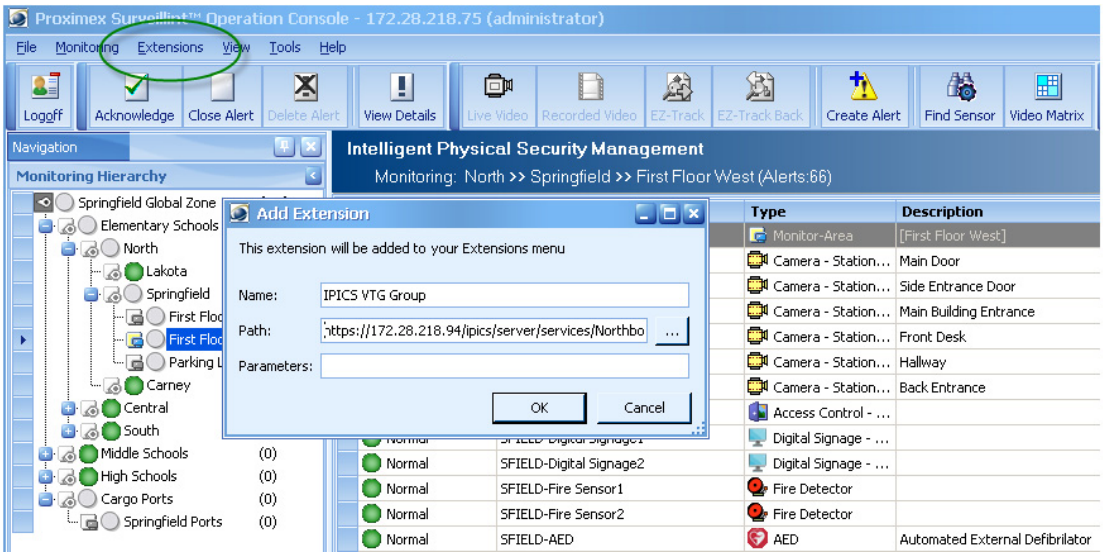
Configure Acting on Alerts through "Extensions"

To define an Extension to originate the IPICS VTG (or any other URL), perform the following steps:

Step 1 Click **on Extensions > Add Extension**.

Step 2 Enter the appropriate path to reach IPICS VTG, as shown in Figure 5-56.

Figure 5-56 Extensions



For example, to notify security officers when a forced entry occurs, a user could use this URL to trigger AtHoc to do the notification: *http://172.28.218.84/corp/gw/gw.asp?scenario=FORCED_ENTRY_IN_BUILDING_1*.

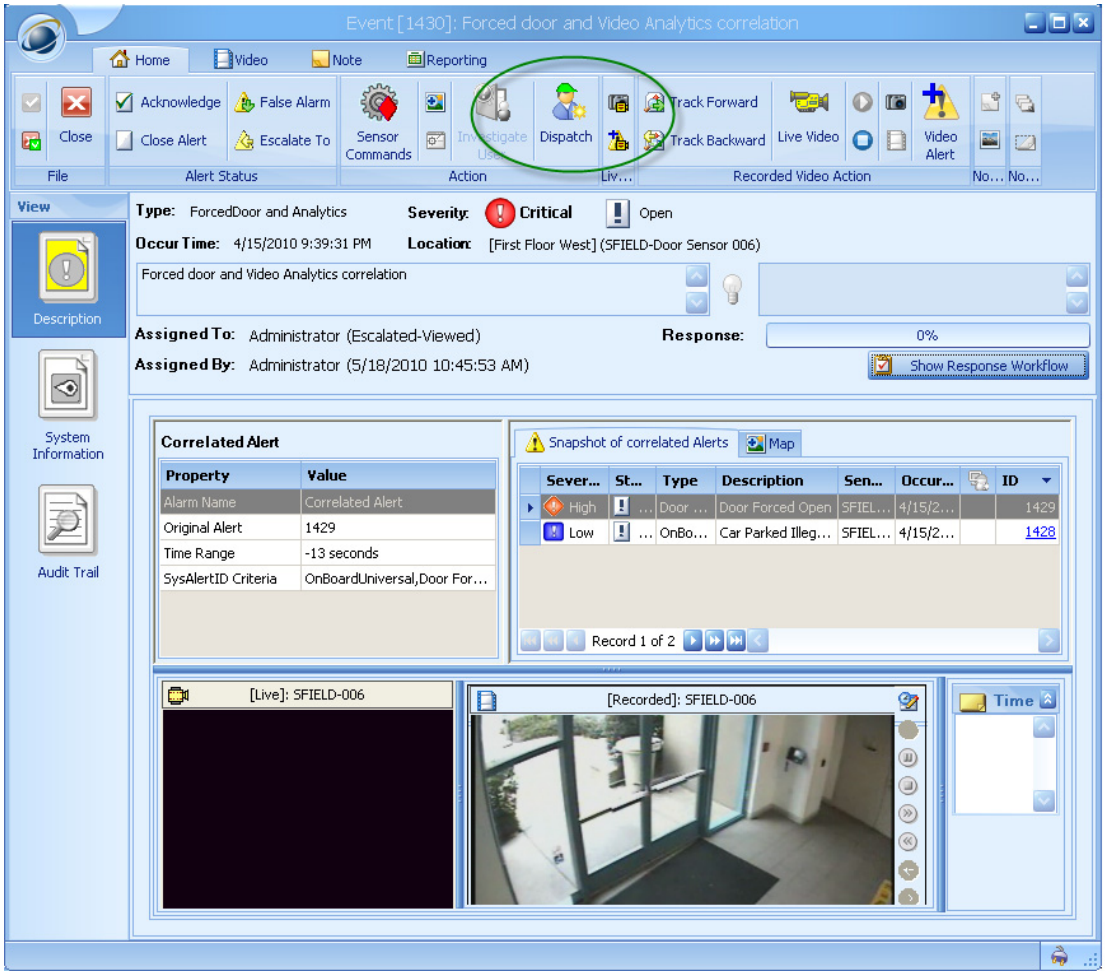
Configure Acting on Alerts through the "Dispatch" Button

To enable the Dispatch Button, perform the following steps:

Step 1 Copy the file *PxConsole.config* provided by Proximex to: *C:\program files\proximex\Surveillint 5.0\Bin*.

Step 2 Edit the file using the appropriate link (links) to execute when the dispatch button is clicked. (See Figure 5-57.)

Figure 5-57 Dispatch Button



Refer to Proximex's *Administering Surveillint Guide* for more details on how to configure this capability.

CHAPTER 6

Sample Scenarios

Protecting an urban environment presents several challenges, where large number of elements need to be protected from crime, natural catastrophes, terrorism, and threats to critical infrastructure.

The following sections present some sample scenarios that integrate the physical security components outlined in this design guide. Based on specific requirements and the environment being monitored, many more scenarios can be imagined and adapted to protect citizens and business by providing a quick resolution of incidents.

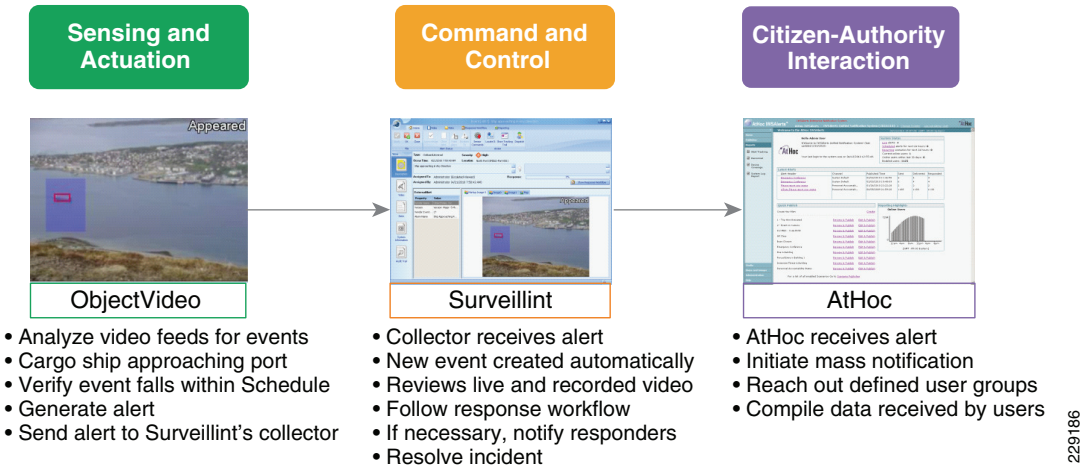
Video TripWire Crossing—Cargo Ports

Video TripWire™ crossing can have different meanings based on the location and type of sensors being used. In a large area such as an airport or oil refinery, it can mean monitoring a virtual fence line monitoring for unexpected movement. In a border situation, it can mean monitoring a state or country line or river for illegal crossings. In a train station, it can be watching for track crossings, but having the need to differentiate between a track crossing and a worker on a catwalk.

Cargo ports represent a vital part of the economy and are used to transport materials such as liquid fuels, chemicals, wood, automobiles, etc. Protecting cargo ports remains a high priority for several regions.

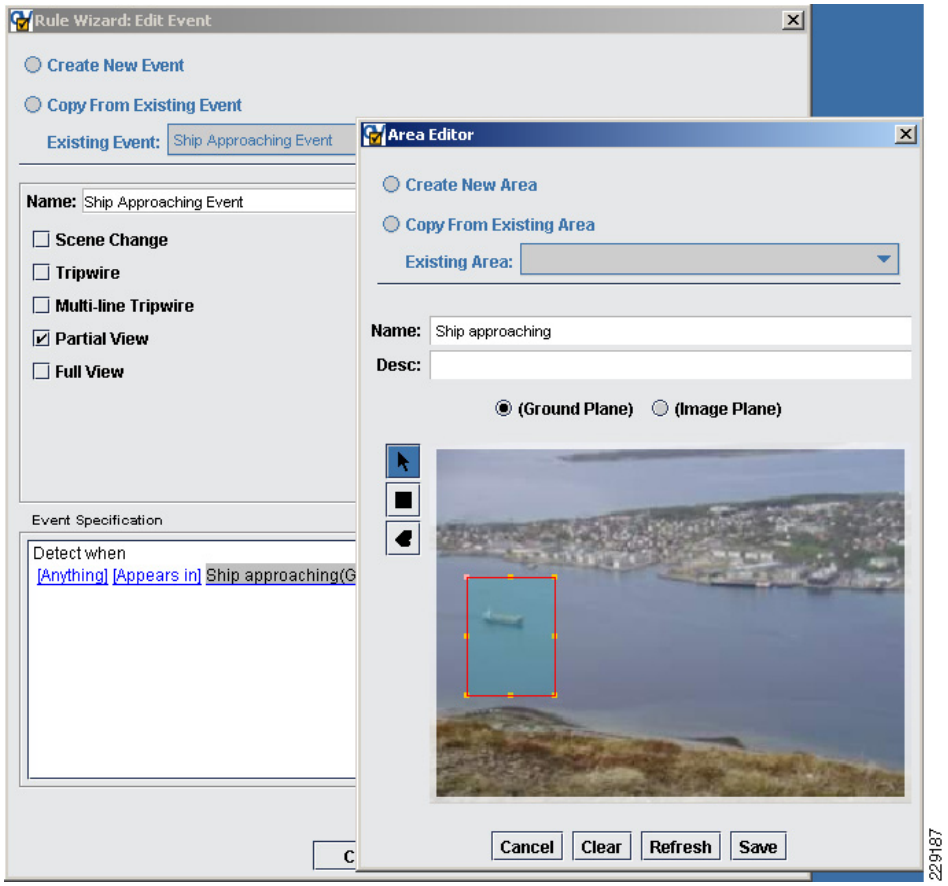
In the following example, video analytics is used to detect cargo ships approaching the port. ObjectVideo is able to detect a ship in the field of view and generates an alert to Surveillint. As shown in Figure 6-1, the alert appears in the Surveillint Operations Console and is addressed by the security operators just like any other alert. The alert may have specific workflow that the operator must follow before closing the event.

Figure 6-1 Scenario Flow



Using the ObjectVideo Rule Management Tool, define the video analytics rules to be observed by the sensor. In the example in Figure 6-2, the rule detects when a cargo ship approaches the defined area. Many other conditions can be defined to identify the ship, such as movement direction, entering or leaving the detection area, detecting time spent in the detection area, and so on.

Figure 6-2 Define Analytics Rule



When the sensor becomes active, the video analytics engine monitors for ships appearing in the field of view. The sensor and rule can also be configured using various size filters to detect only large ships and not for every possible watercraft.

The video analytics engine can be configured to monitor only during specific times, therefore reducing the number of alerts generated. The schedule in Figure 6-3 is configured to monitor for ships during evening or night time.

Figure 6-3 Detection Schedule

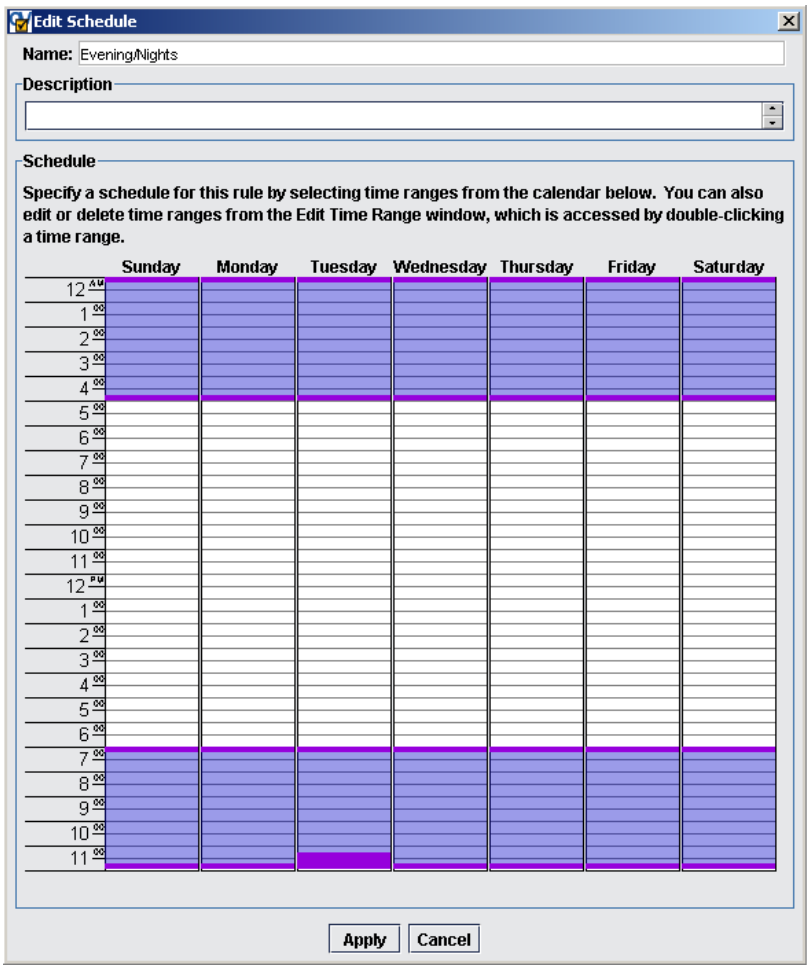
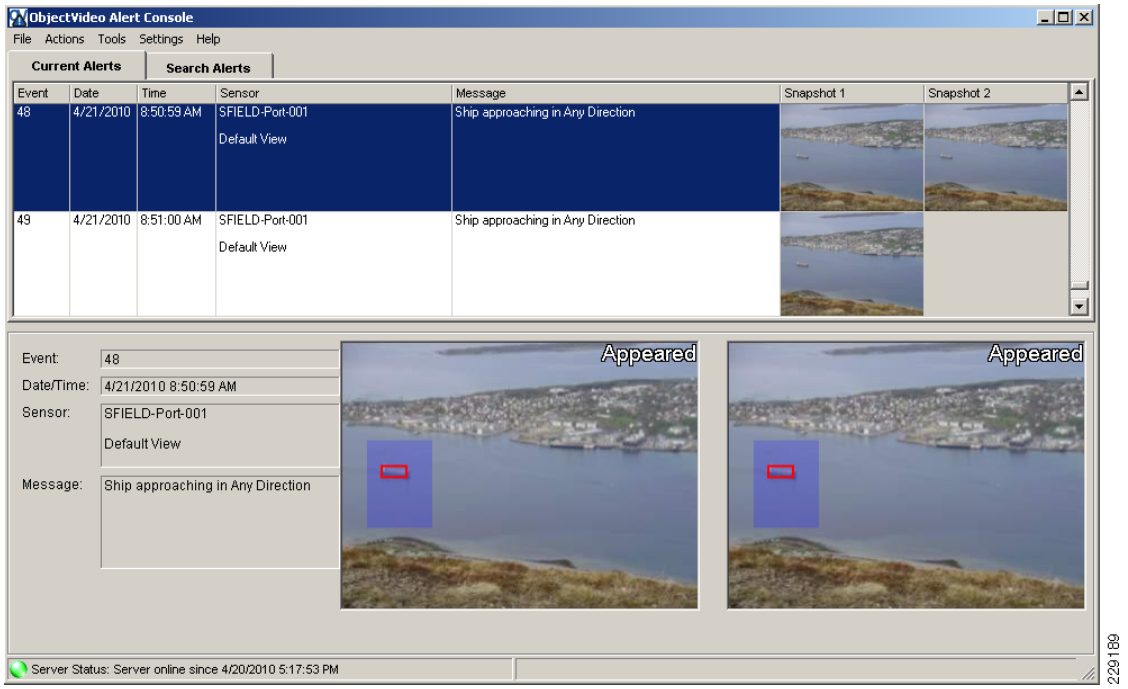


Figure 6-4 shows ObjectVideo's Alert Console detecting a ship approaching the port. The alert is logged in ObjectVideo's console and simultaneously sent to Surveillint for further analysis.

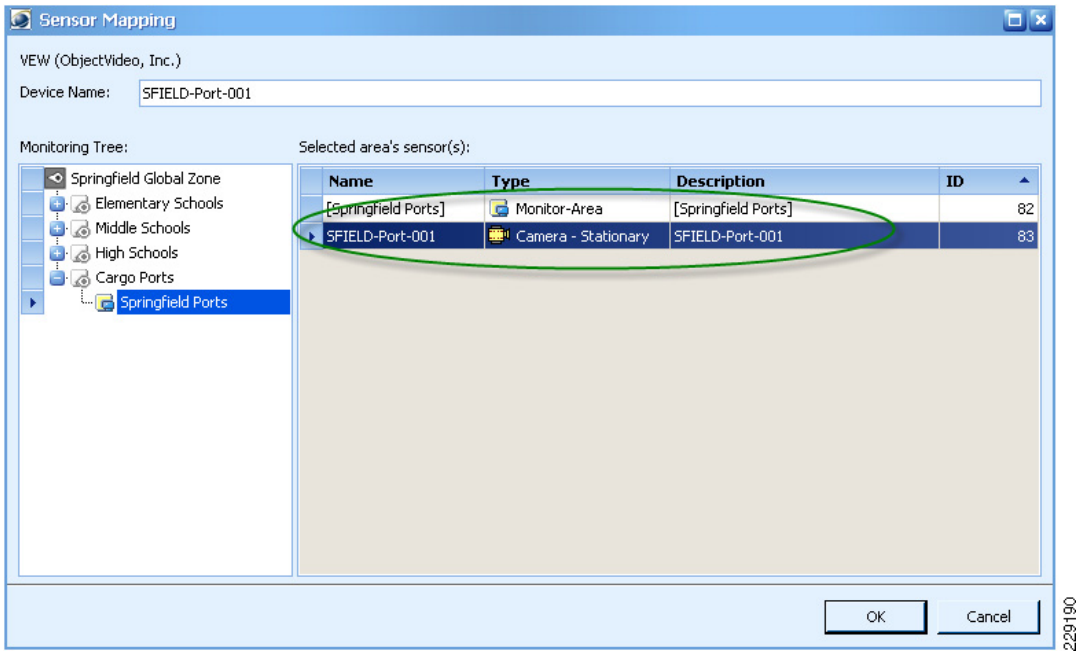
Figure 6-4 Alert Console



Before receiving alerts in Surveillint, you can define a sensor mapping between the ObjectVideo sensor and a camera sensor in Surveillint.

To do this using Surveillint's Administration Console, click on **Event Integration > Sensor Mapping** and define a mapping between SFIELD-Port-001 sensors, as shown in Figure 6-5.

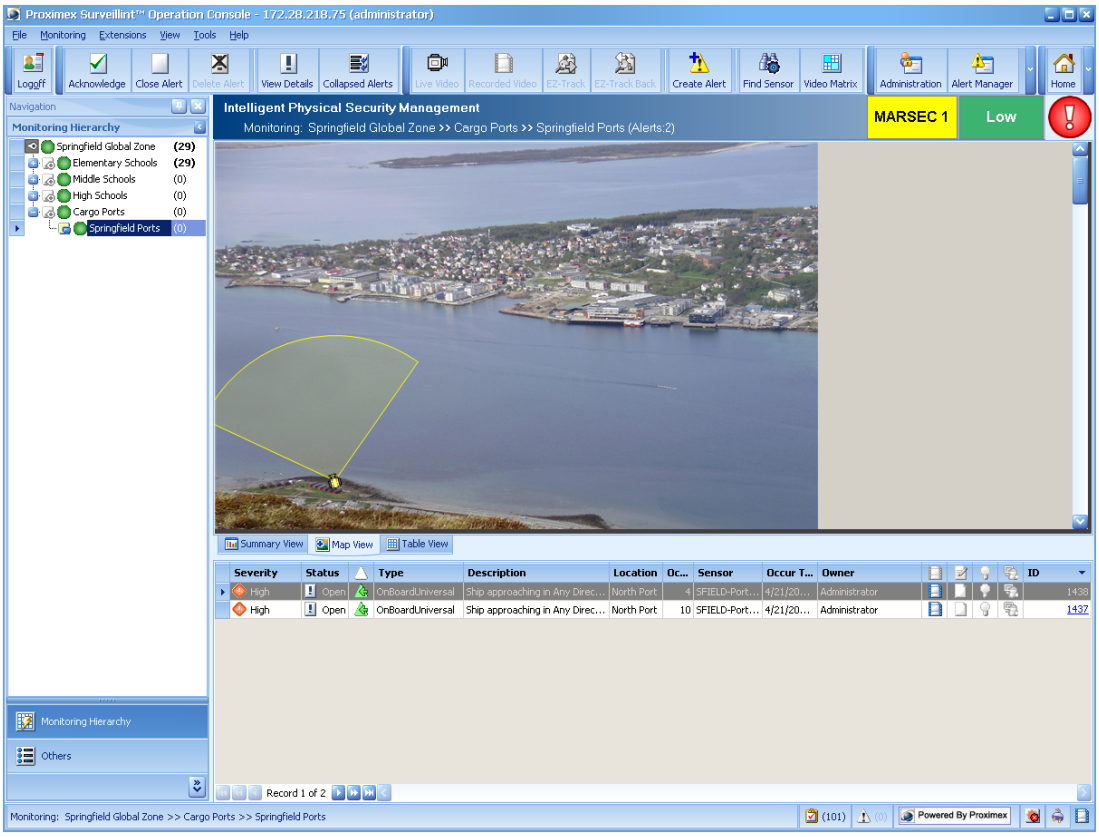
Figure 6-5 Sensor Mapping



The sensor mapping between ObjectVideo and Surveillint ensures that alerts are logged against the right sensor, making event resolution easier for the security operator.

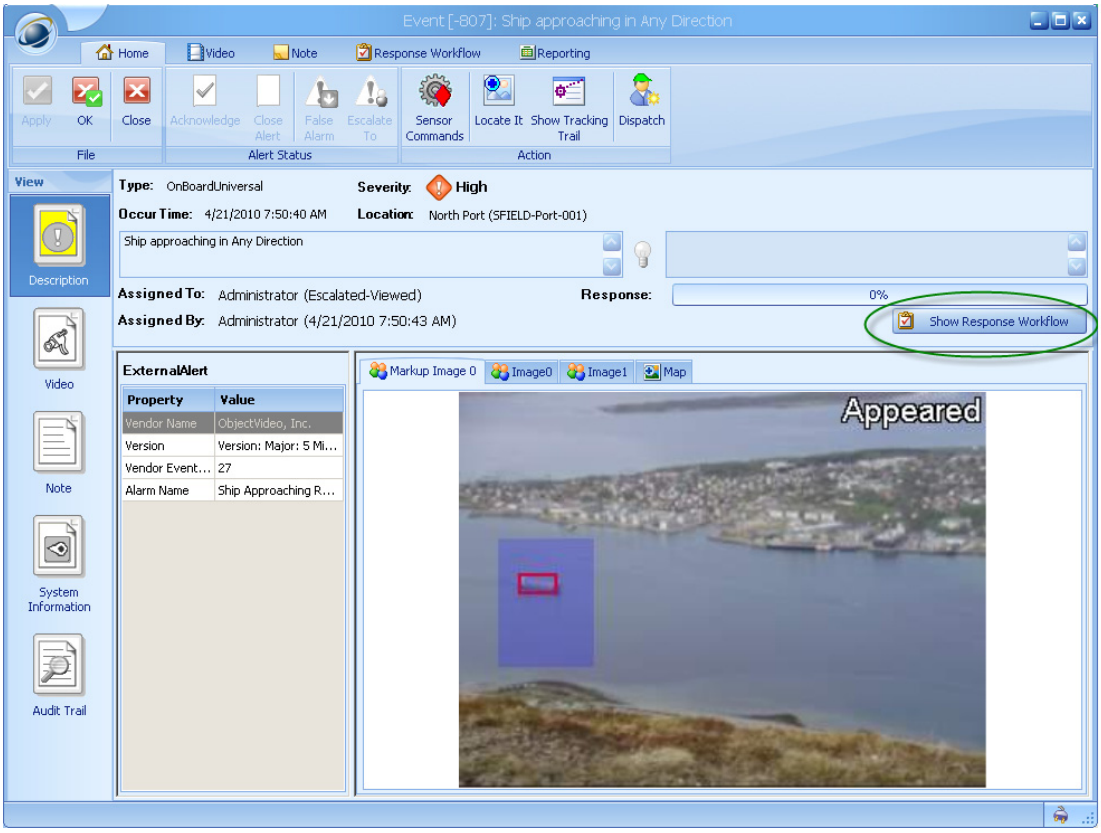
Figure 6-6 shows the monitoring area dedicated to the cargo port and the camera sensor's position in the map. The map can also be defined using actual GPS coordinates to properly identify the location of cameras and sensors.

Figure 6-6 Surveillint Monitoring Area



ObjectVideo sends the alert notification to Surveillint via the connector provided by Proximex. Surveillint logs an event in the Operation Console, as shown in Figure 6-7.

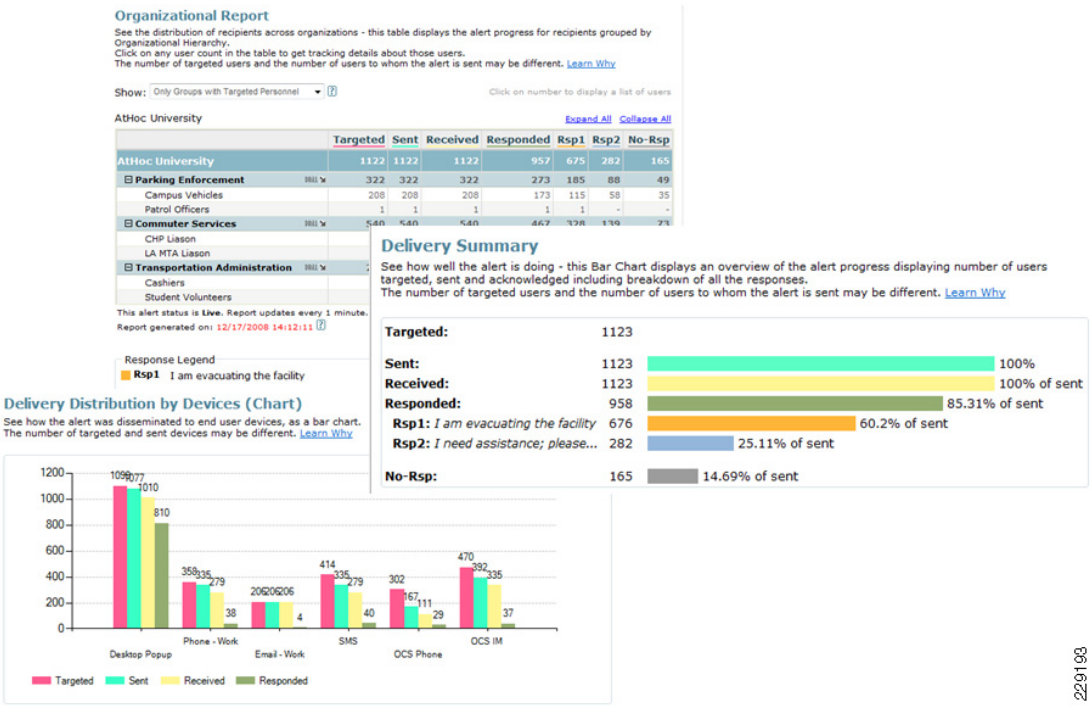
Figure 6-7 Cargo Ship Detected



The event window allows the operator to review the event and determine whether further action is required to resolve it. From the single window, the operator can perform several activities as dictated by the organizations Standard Operating Procedures (SOPs), which can be enforced in Surveillint's response workflow. Surveillint's response workflow provides step-by-step instructions for each alert that empowers the operator to perform the appropriate tasks in the appropriate order to resolve the incident. Other items that are presented to the operator include reviewing live and recorded video, dispatching emergency responders, exporting video files, escalating the alert to another operator/manager, and so on.

When an accountability alert is sent to personnel via AtHoc, all responses are tracked in real-time and compiled to show a personnel accountability graphical report (see Figure 6-8), allowing the operator to drill into the results and see who are the users that had requested help, or that had not responded.

Figure 6-8 AtHoc's Personnel Accountability Graphical Report



Unauthorized Building Access/Forced Entry

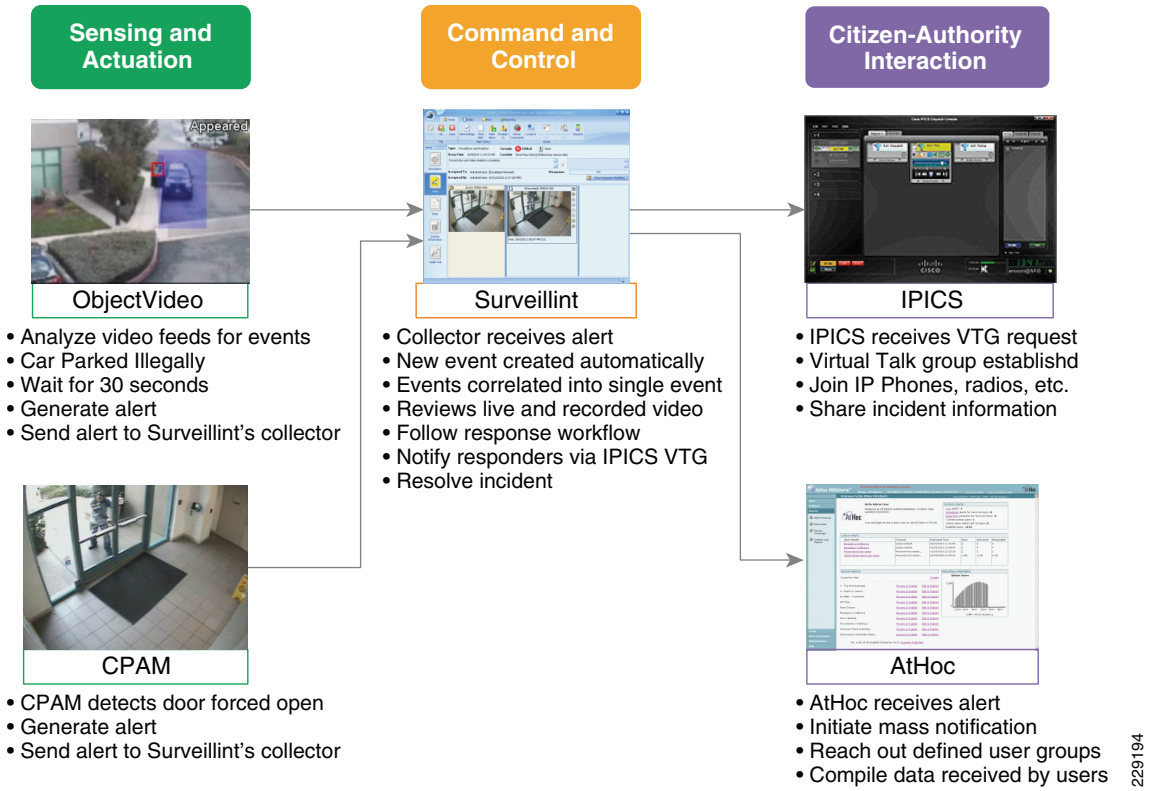
In a more complicated incident, receiving simultaneous alerts may be received from multiple systems in a short period of time. Being able to combine these alerts into a single event greatly improves the time to resolve incidents by allowing the operators to work on a single event window.

A sample scenario where two alerts get combined into a single event can be generated by both ObjectVideo and CPAM.

A car parked illegally in a restricted zone for more than 30 seconds is recognized by ObjectVideo and an alert is sent to Surveillint. By itself, the alert is generated with a low severity and can be quickly resolved by the operator after reviewing live and recorded video.

A second alert arrives from the access control system indicating that a door has been forced open. This alert was received in the general vicinity of the parking lot within a certain number of seconds. Figure 6-9 shows the scenario flow.

Figure 6-9 Scenario Flow



The alerts are combined into a single event window, with a critical severity. From a single event window, the operator is able to work on the incident. By following the response workflow, the operator may view live and recorded video, launch an IPICS Virtual Talk Group, and notify AtHoc's mass notification alerts if appropriate.

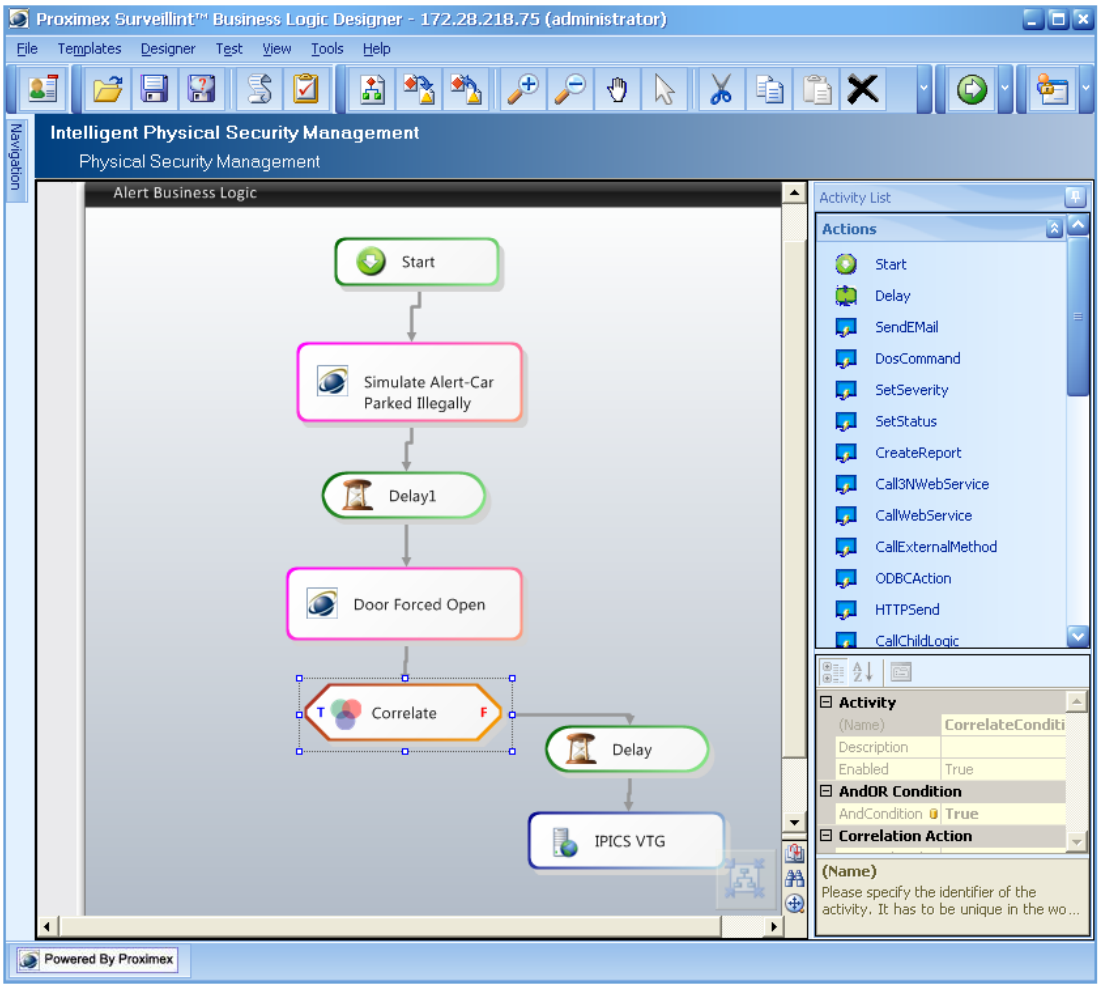
Surveillint's correlated alerts feature allow multiple alerts to be correlated across multiple systems to raise additional alerts, raise the severity of alerts, close or acknowledge existing alerts.

Correlated alerts allow alerts of a certain type across all sensors in an area to be grouped. When the area has multiple sensors (doors, cameras, and so on) and alerts on the sensors trigger within a short span of time, it's useful to gather these alerts together for further analysis.

Alerts can be correlated by time range, proximity by monitoring area or sensor group, severity level, alert description, or alert type. When the correlation criteria are met, the CorrelatedCondition icon in Business Logic can generate a new alert and update the status for severity of the existing correlated alerts.

The Business Logic in Figure 6-10 is used to correlate two alerts and to initiate a Virtual Talk Group with IPICS.

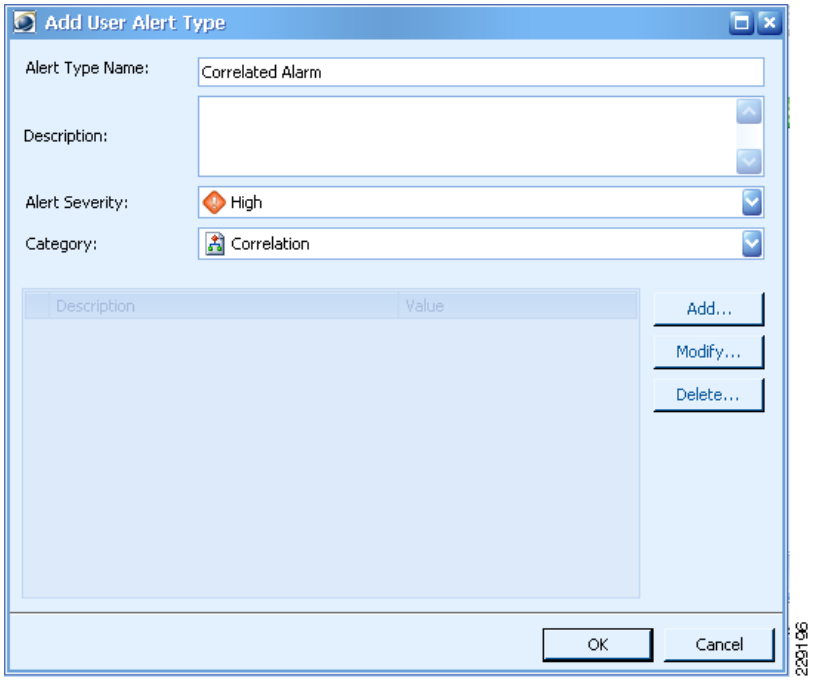
Figure 6-10 Correlated Alert



The first simulated alert is triggered by ObjectVideo after detecting a car parked illegally for more than 30 seconds. The second alert comes from Cisco Physical Access Manager and was triggered by a suspect forcing the door open.

To create the Correlated Alert under the Administration Console, select **Event Integration > User Alert Type > Add**. Define the proper alert severity and set the category to **Correlation**, as shown in Figure 6-11.

Figure 6-11 User Alert Type



From the Business Logic designer, the Correlate activity can be configured to match alerts created within 60 seconds matching two alert types: Door Forced Open and OnBoardUniversal (ObjectVideo). The severity of the correlated alert can also be set to Critical, because the incident has detected a car parked illegally and later on a door forced open. All these parameters can be easily selected and configured through the predefined correlate activity.

To define the two alerts being correlated, from the correlate activity, click the **Alert Type(s) matching** menu and select the relevant alert types.

Under **Alert Type**, select the alert defined in the previous step, ForcedDoor and Analytics.

Because the two events happened in the same area and took place within a certain time, the security operator is able to work on a single event, making the workflow operations and documentation more efficient.

Figure 6-12 shows the results of a correlated alert presented to the security operator, including both alerts: Door Forced Open from CPAM and Car Parked Illegally from ObjectVideo. The operator is also presented with the Response Workflow, or the SOP that should be followed to resolve the alert.

Figure 6-12 Alerts and Response Workflow

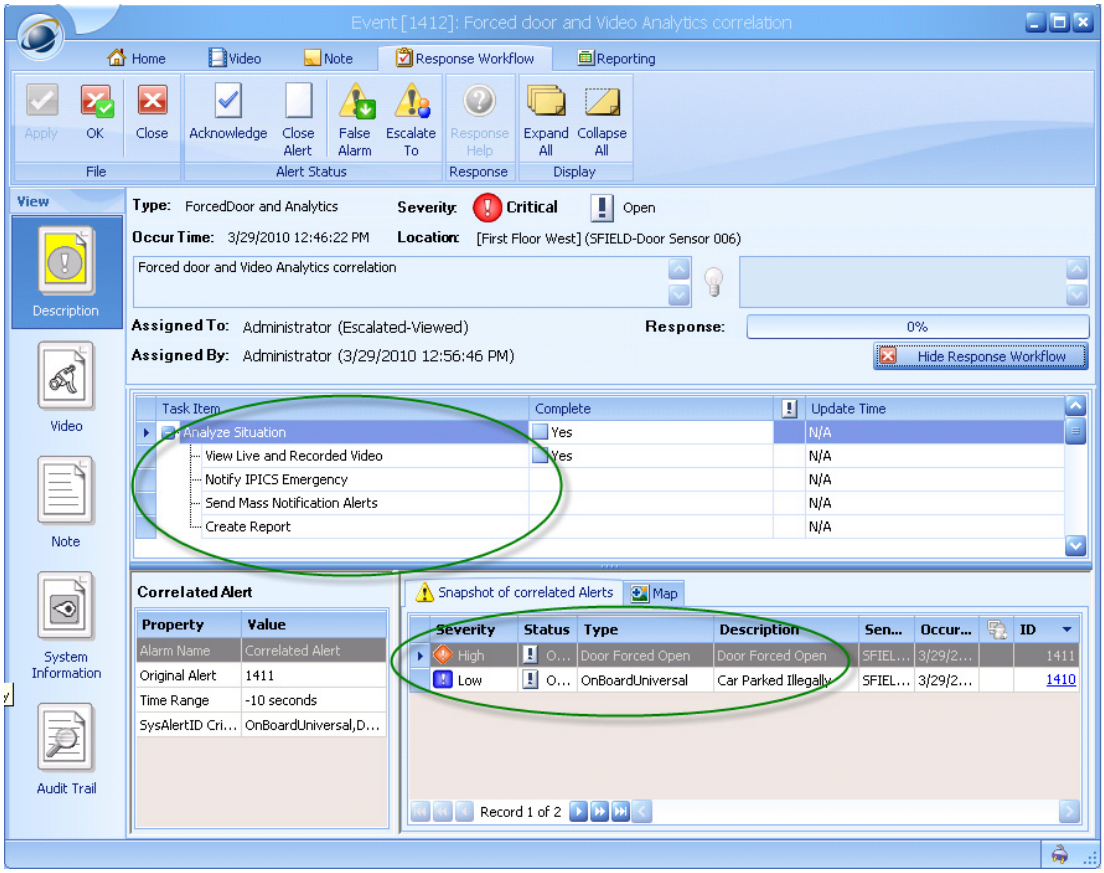
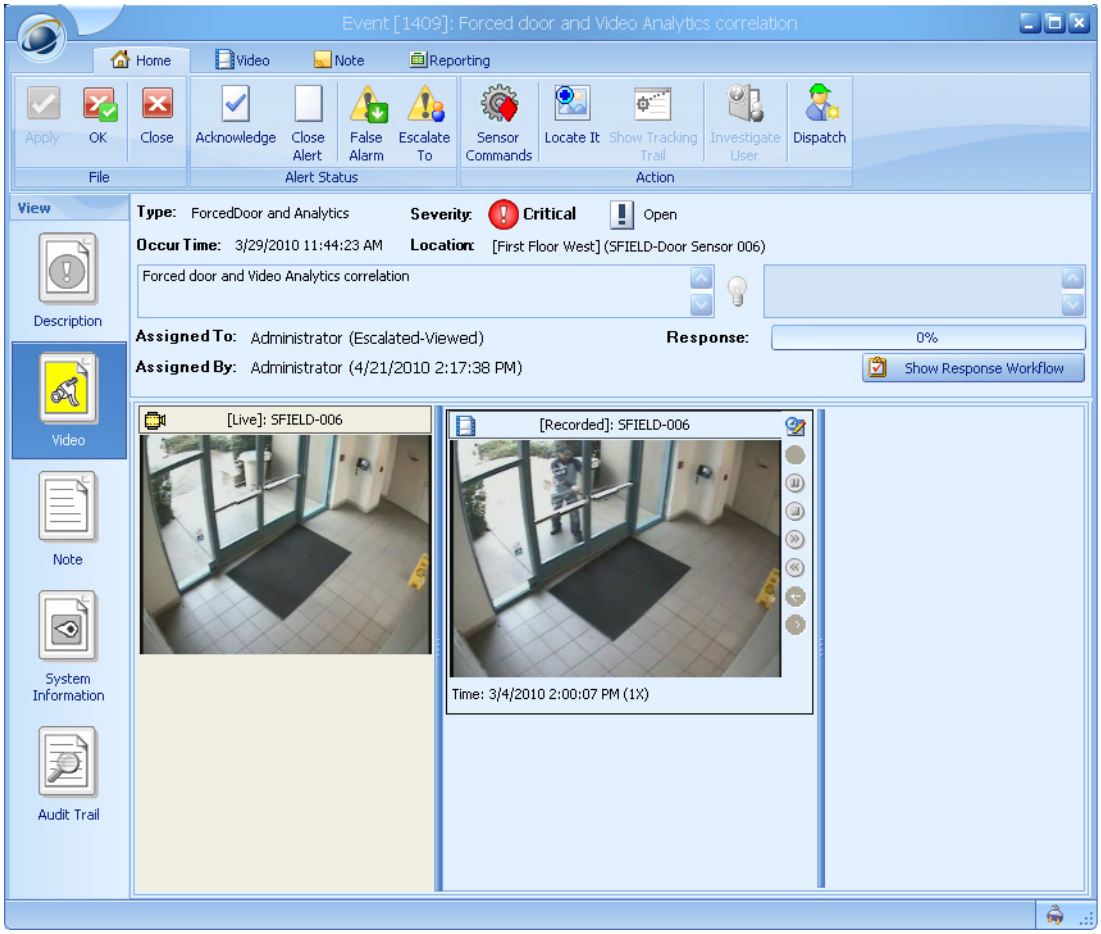


Figure 6-13 shows how the security operator is able to review live and recorded video from the same event window, reducing the number of errors and improving the time to resolve an incident.

Figure 6-13 Live and Recorded Video



From the same event window, the security operator is also able to perform other tasks, such as acknowledging or closing the alert, escalate it to another operator, locate it in a map, write notes, and so on.

CHAPTER 7

Remote Operation Services

Cisco Management Appliance

Urban Security solutions require a mission-critical IP-centric network to be in place and functioning properly at all times. The network is made up of multiple pieces of equipment (video surveillance, access control, incident response, and core network components) as well as middleware software components to correlate and dispatch situational events as they occur. All network components must be in good health for the PSS system to be effective. As a result, remote management of these devices and middleware components is essential to the successful deployment of any physical safety and security (PSS) solution.

Using the Cisco Management Appliance (MAP) to manage the PSS network enables an IT or any other monitoring organization to proactively monitor the health of the network and maintain a healthy network ready to perform its primary purpose of keeping citizens safe.

Cisco Management Appliance Description

The MAP approach to managing PSS systems requires deploying one or more management appliances in the network and leveraging standard management capabilities inherent in the PSS IP devices and gateways (for example, SNMP, ICMP, Syslog, and so on) to discover and place them under management. After each of the components is placed under management, industry standard management functionality and custom Cisco intellectual property integrated into the MAP are used to monitor the health of the entire system.

The same appliance used to manage the PSS components for this effort is already in use to manage advanced and emerging technologies from Cisco such as Telepresence, DataCenter, and IronPort solutions. The appliance is field tested and proven as a management system with Cisco equipment and Cisco applications.

The Cisco MAP is able to monitor all devices in the PSS environment and generate detailed reports on their performance and availability. In addition, Cisco MAP is able to send alerts to Surveillint, allowing the operator to work through a consolidated interface. Figure 7-1 shows how the Cisco MAP is deployed in a typical PSS environment

Figure 7-1 Typical PSS MAP Deployment

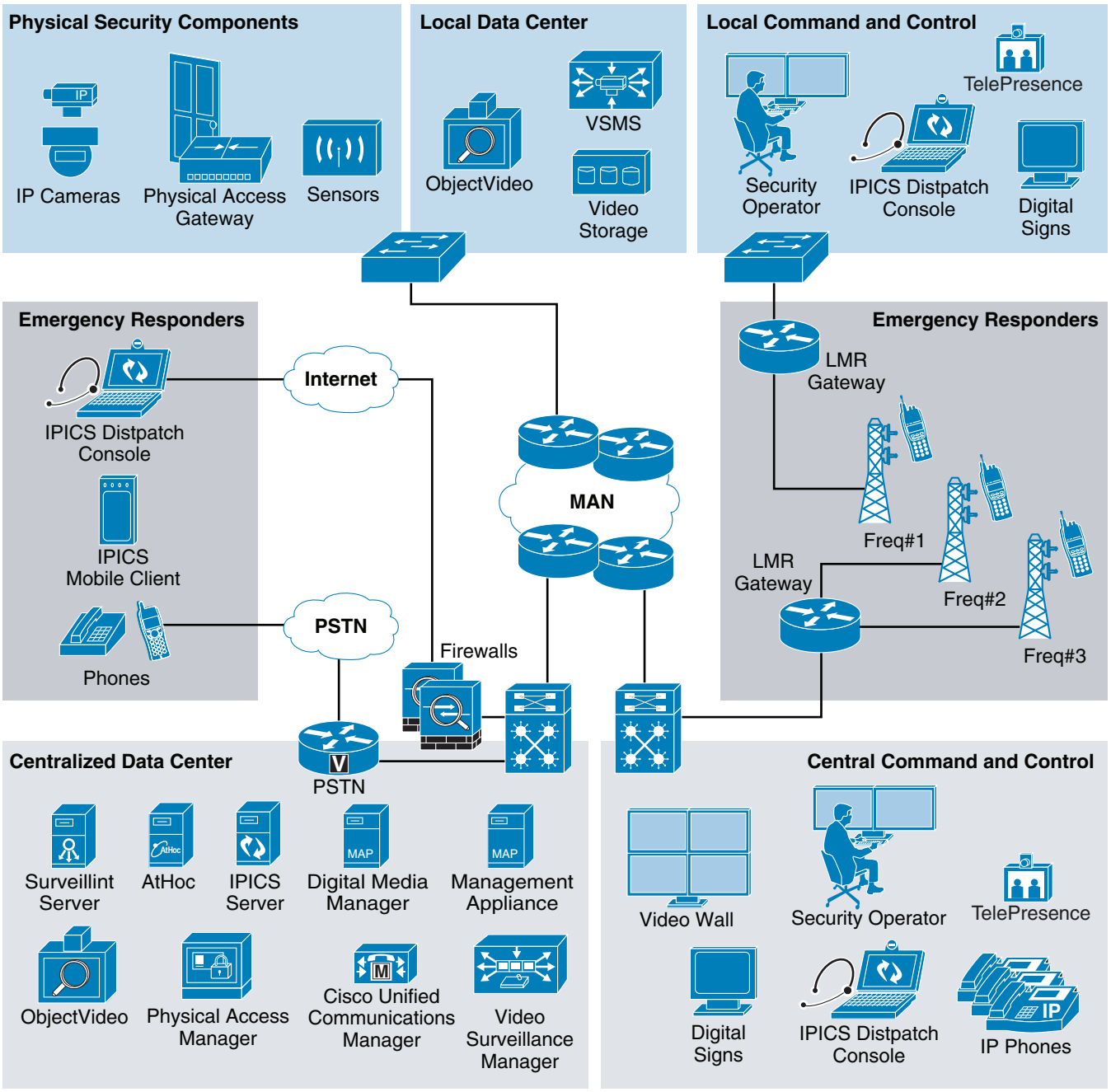
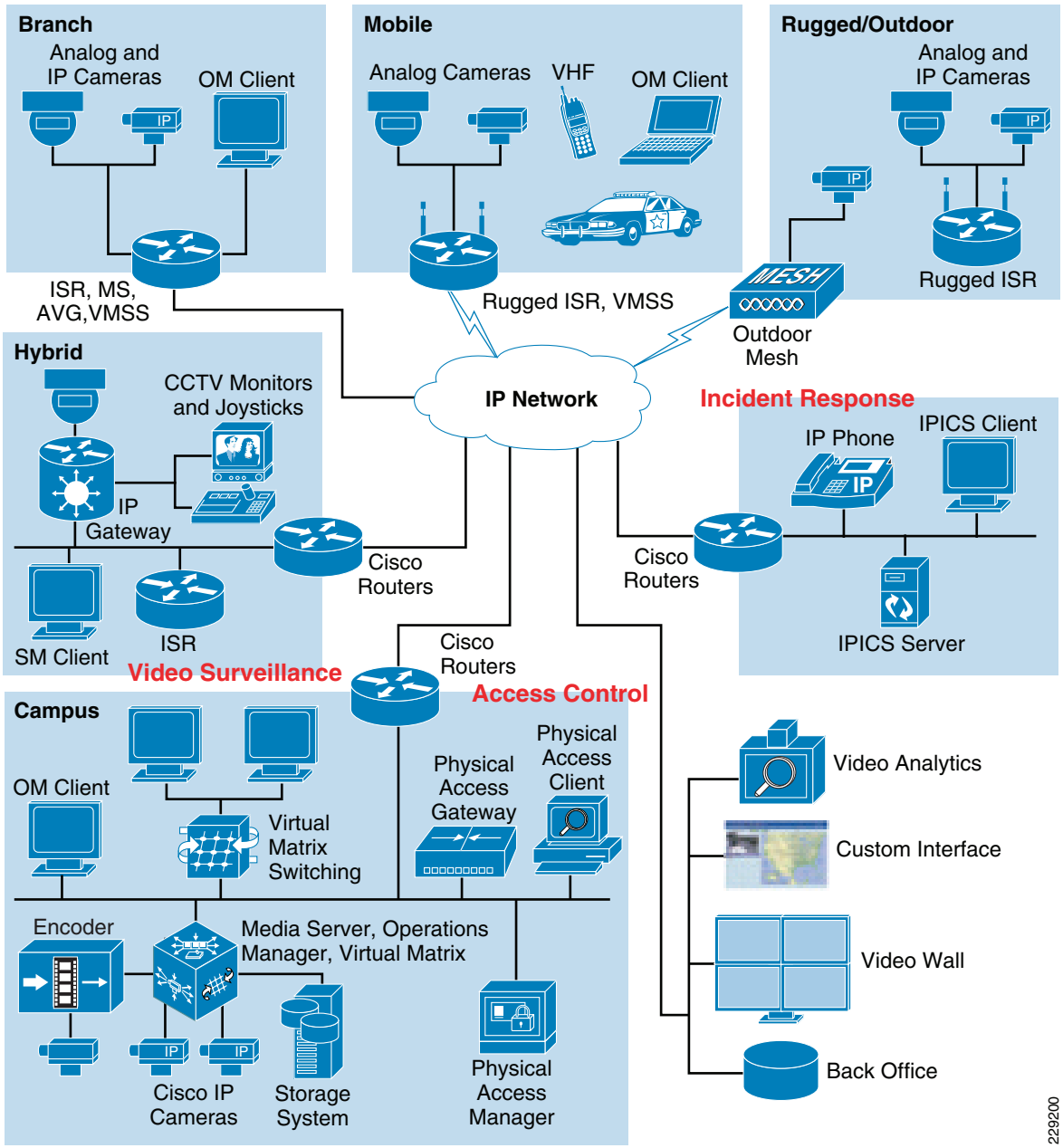


Figure 7-2 shows a sample of the PSS equipment that can be managed using the MAP solution.

Figure 7-2 PSS MAP Components under Management



The MAP solution provides the following three major management functions:

- Monitoring—The MAP collects and processes events from each of the PSS and infrastructure components based on industry best practices included in the MAP appliance and Cisco product -specific intellectual property.
- Detection of faults and potential network issues—The MAP is able to determine the severity of each event received and ensure that an appropriate fault is activated in the system.
- Isolation of faults and potential network issues—The MAP provides user-friendly interfaces to the monitoring organization to allow for easy identification of faults and potential issues. In addition, the MAP must also provide operators with tools to troubleshoot problems remotely to determine the root cause of each issue.

The Cisco MAP solution provides all of these features and is designed to be deployed in a variety of configurations from hosted, onsite, and high availability environments.

Benefits of the Cisco MAP

The MAP approach to managing PSS components provides the following benefits to the PSS system:

- Proactive monitoring of the PSS mission-critical network to detect and isolate faults as they occur. This allows faults to be isolated and corrected quickly to keep the PSS system up and running and serving its primary purpose of keeping citizens safe.
- Proactive monitoring and detection of potential issues such as high memory or disk utilization to prevent faults.
- Proactive collection and maintenance of statistics to determine areas of the PSS system needing improvement. Performance degradation over time may mean the original characteristics of the system have changed and certain components may need to be upgraded.
- Minimizing legal, regulatory, and financial liability by instituting policies to measure PSS system reliability, storage requirements, and other important metrics.

Cisco MAP focuses on the management capabilities required to proactively monitor the health of the Physical Safety and Security components deployed in the Urban Security model. The management capabilities described in this section have been validated in Cisco's Urban Security lab. The lab diagram and components are highlighted in chapter 8 – Lab and test overview.

For each component to be placed under management, the device or application must support polling via ICMP, SNMP, SQL, or an API and send status asynchronously via syslog or SNMP traps.

The core management capabilities validated in this solution guide are as follows:

- Device and application availability
- Receipt of asynchronous faults
- Generation of custom faults
- Collection of performance information
- Collection and storage of inventory information for each component in the system

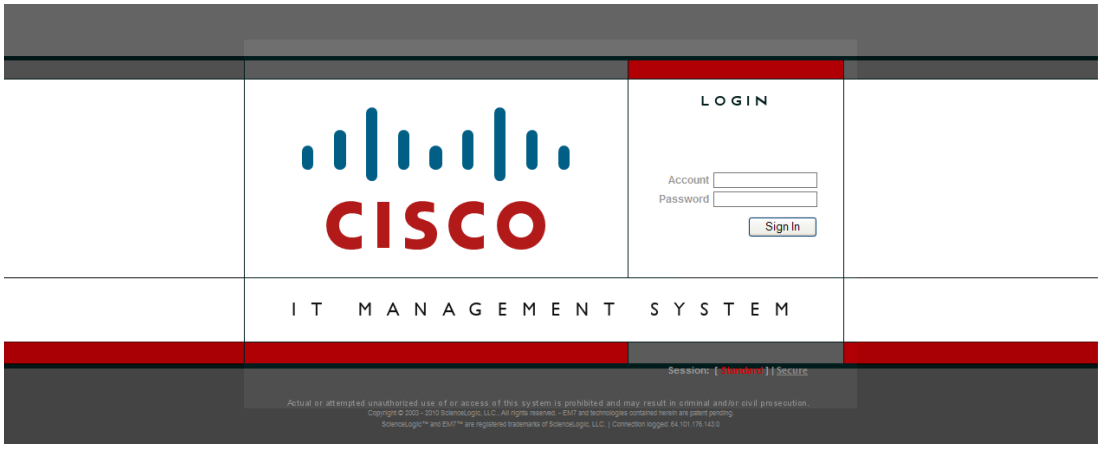
Cisco MAP Features

Several use cases were validated for this solution. The base line set of use cases required for successful remote management of the PSS system are also included.

Discovering PSS Components

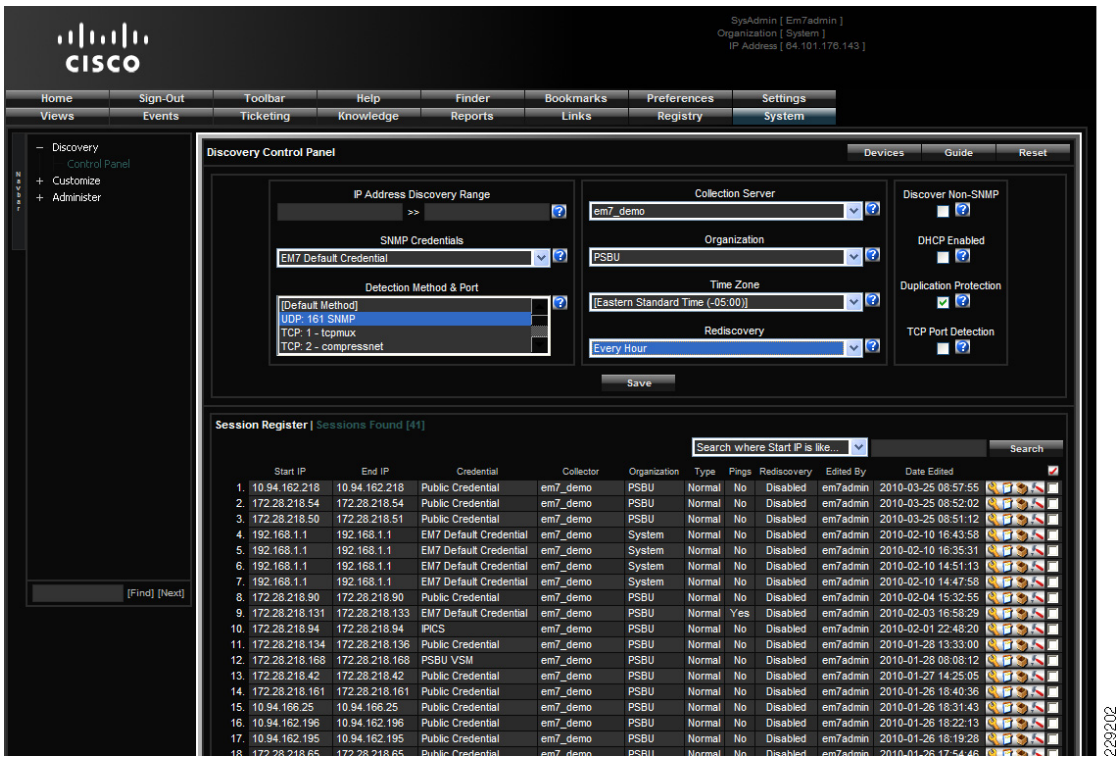
The MAP appliance must discover each PSS component to begin monitoring the health of the system. This can be done easily using the industry standard best practice discovery capabilities built into the MAP appliance. First, the user must log into the MAP appliance web portal and navigate to the System discovery screen, as shown in Figure 7-3.

Figure 7-3 MAP Web Portal Login Screen



After the user is logged into MAP appliance, it is simple to navigate to the System Discovery interface by selecting the System tab and then selecting the Discovery option on the left hand tree view, as shown in Figure 7-4.

Figure 7-4 MAP Discovery of PSS Video Surveillance Management Appliance



In this case, the MAP appliance is set up to discover a Video Surveillance Management appliance (VSM) using the SNMP protocol. The MAP appliance can discover any device or application that supports ICMP or SNMP.

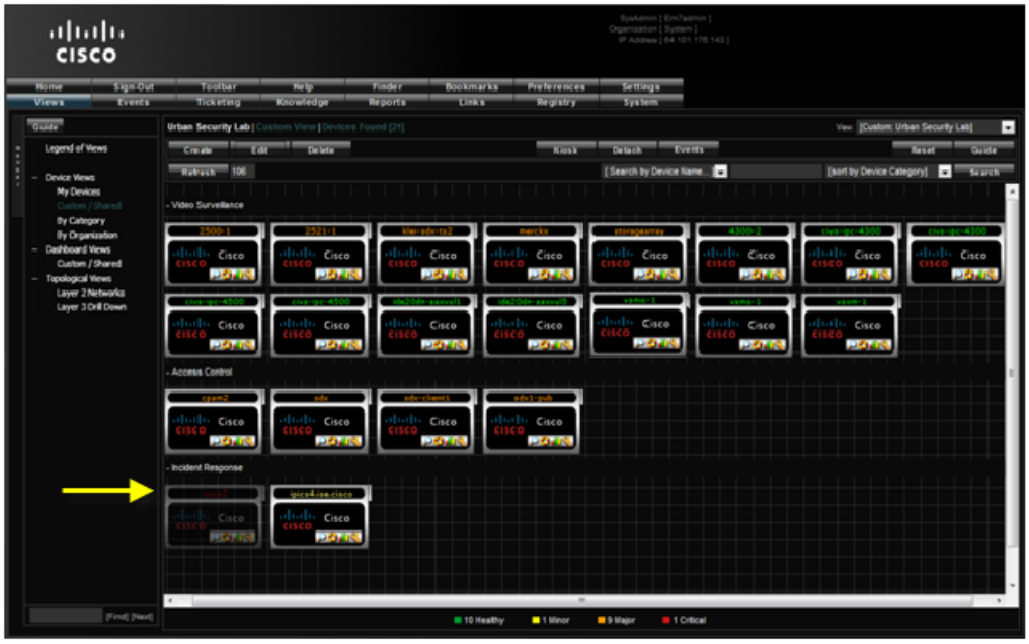
Monitoring PSS Mission-Critical Network

After the PSS devices are discovered by the MAP appliance, the entire PSS system can be monitored remotely. The MAP web portal provides multiple views of the PSS system showing the health of the system in a single pane of glass. Three sample monitoring views are displayed below.

The first view is a Cisco product specific view that allows the monitoring organization to view all of the PSS components by device category (see Figure 7-5):

- Video surveillance devices (Cisco IP cameras, AVG, VSMS, VMSS, and VSOM components)
- Access control devices (CPAG, CPAM)
- Incident response devices (IPICS, RMS)

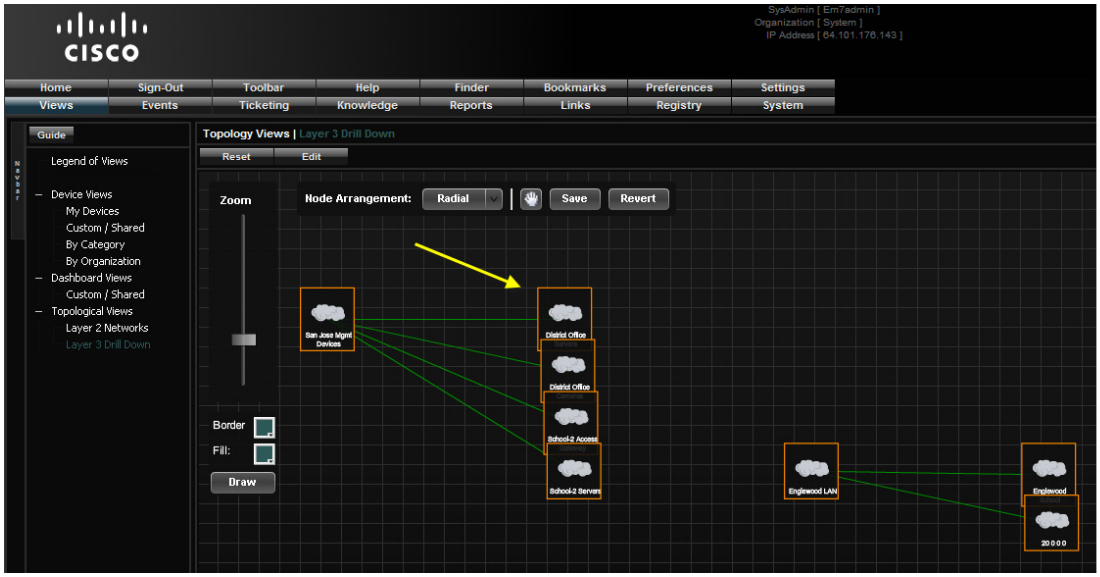
Figure 7-5 MAP Monitoring—Device Category View



In this view, the operator can quickly see any issues needing attention. The arrow in Figure 7-5 points to the first icon under Incident Response, which appears grayed out. The icon is actually blinking on the screen giving the administrator a visual cue that there is some kind of communication failure on that particular IPICS server.

The second view is graphical representation of the Layer 3 PSS network as shown in Figure 7-6. The Layer 3 PSS network includes an icon for each sub-network and shows a topological view of the status of the entire sub-network (a switch or router and all of the components connected to it in a downstream hierarchy). A color-coded box is drawn around each sub-network. The box color indicates the current state of each sub-network (green indicates no problems, yellow indicates a minor condition, orange indicates a major condition, and red indicates a critical condition). A sub-network icon with any color other than green indicates that at least one device in that sub-network is having problems.

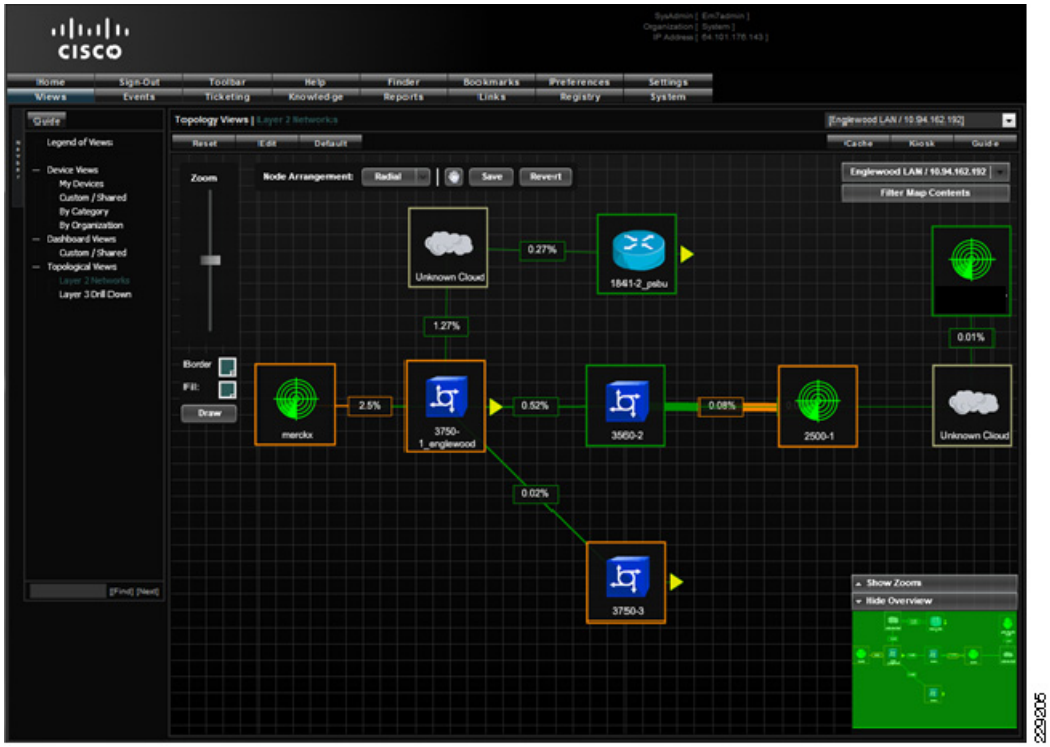
Figure 7-6 MAP Monitoring—Level 3 PSS System View



The arrow above is pointing at a sub-network with a major condition (orange box). This sub-network contains at least one device reporting a major condition that needs attention.

The third view is a graphical representation of the Layer 2 PSS network (see Figure 7-7). The Layer 2 PSS network can be viewed by clicking on one of the level 3 icons in Figure 7-6. An icon for each PSS component in the system (CPAM, CPAG, VSM, VSMM, IPICS, and so on) is present in the level 2 view with a color-coded box drawn around each component. The box color indicates the current state of the component (green indicates no problems, yellow indicates a minor condition, orange indicates a major condition, and red indicates a critical condition). In addition, each box is connected with color-coded lines representing the network links between components.

Figure 7-7 MAP Monitoring—Level 2 PSS System View



Each line includes a number inside a box, representing the current link utilization. Link utilization data is collected automatically by the MAP appliance and is used to determine the color of each link (utilization data is compared to Cisco product specific thresholds defined in the MAP).

Note The thresholds were set artificially low to induce the error conditions shown with orange-colored link lines. In a standard PSS system, the link thresholds are set based on Cisco product-specific recommendations.

Detecting and Isolating Faults

One of the primary functions of the MAP appliance is to allow the monitoring organization to detect and isolate faults and potential issues in the PSS system. There are several ways the MAP appliance allows detection of issues. The views described above are the starting point for the fault detection use cases. Figure 7-8 shows the PSS component view by category with additional reference points.

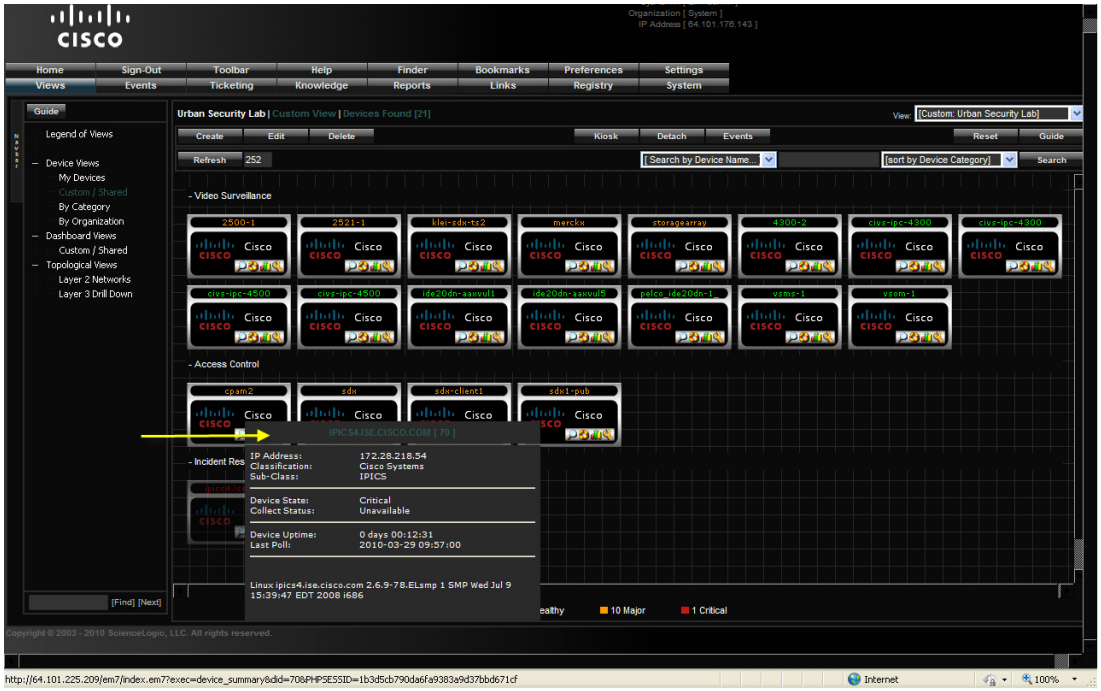
Figure 7-8 PSS Faults—Category View

Note the numbered arrows on the diagram. Arrow #1 shows a summary of the state of all of the PSS components in the system. The number of devices in each state is displayed at the bottom of the web portal user interface allowing an administrator to see the overall health of the PSS system at a glance.

Arrow #2 shows the first icon under Incident Response as grayed out. The icon is actually blinking on the screen giving the administrator a visual cue that there is some kind of critical communication failure on that particular IPICS server. Arrow #3 shows the label of one of the Video Surveillance components (a Cisco 2500 series IP camera) is orange indicating this PSS component has a major condition present. The label color indicates the health of each component in the system and provides an at a glance health status for the system administrator. Each of these cues serves as a starting point for detecting and isolating faults in the system.

Moving the mouse over the IPICS server pointed to by Arrow #2 above brings up a more detailed status dialog showing the vital statistics for the server (see Figure 7-9).

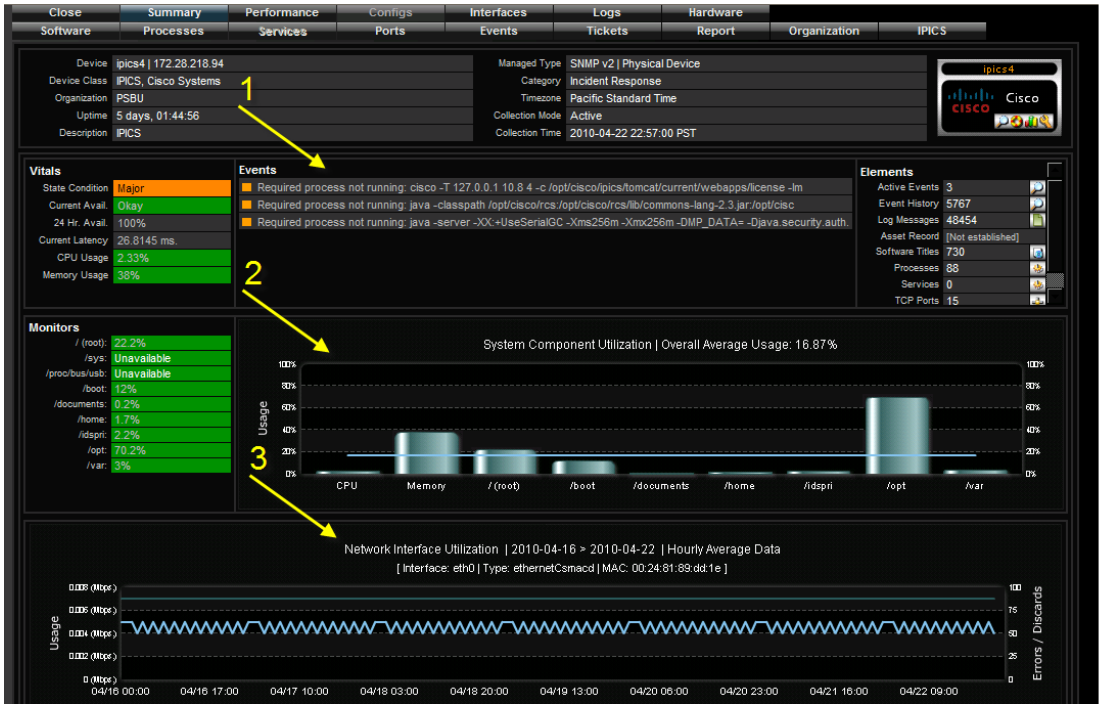
Figure 7-9 PSS Faults—Vital Statistics Dialog



The vital statistics dialog shows the last time this IPICS server was known to be operating properly and lets the administrator know it is currently not accessible to the MAP appliance.

From this point, the administrator can double-click on the IPICS server icon to navigate to the IPICS detail screen, as shown in Figure 7-10.

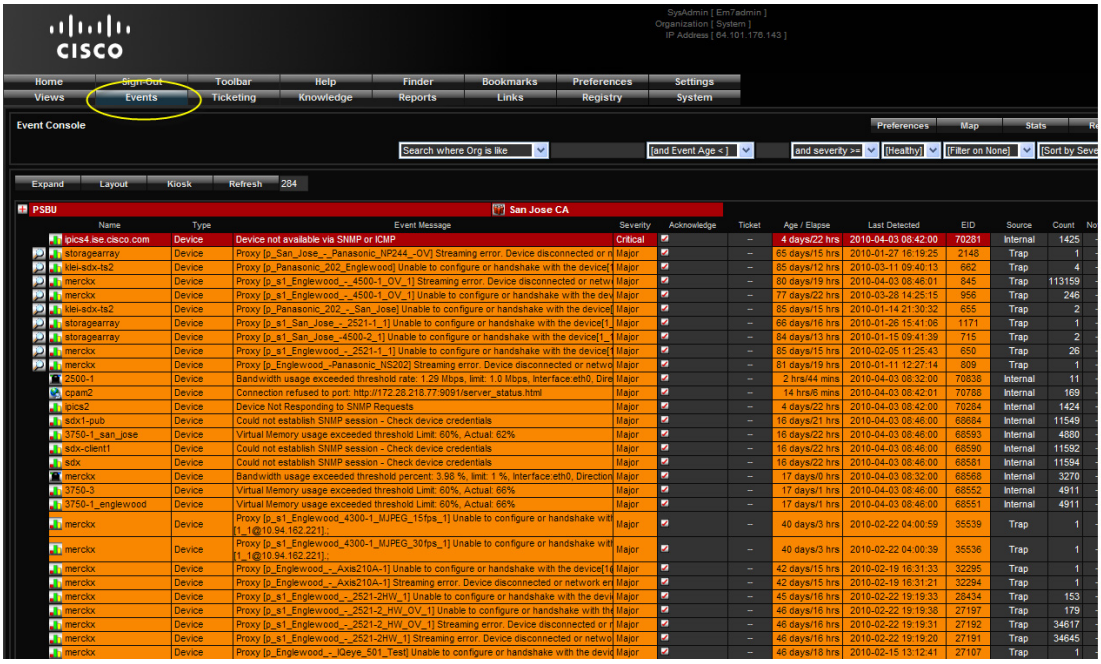
Figure 7-10 PSS Faults—IPICS Details



This view allows an administrator to review the currently active alarms and events on the IPICS server, current and historical memory utilization trends on the server, and vital network statistics. In this case, one of the alarms indicates that an important process on the IPICS server is not operating properly. An administrator can now take the appropriate actions to correct the issue on the IPICS server.

Another useful view for identifying and troubleshooting issues in the system is the Events view, as shown in Figure 7-11. This view can be started by selecting the Events tab on the main MAP menu bar.

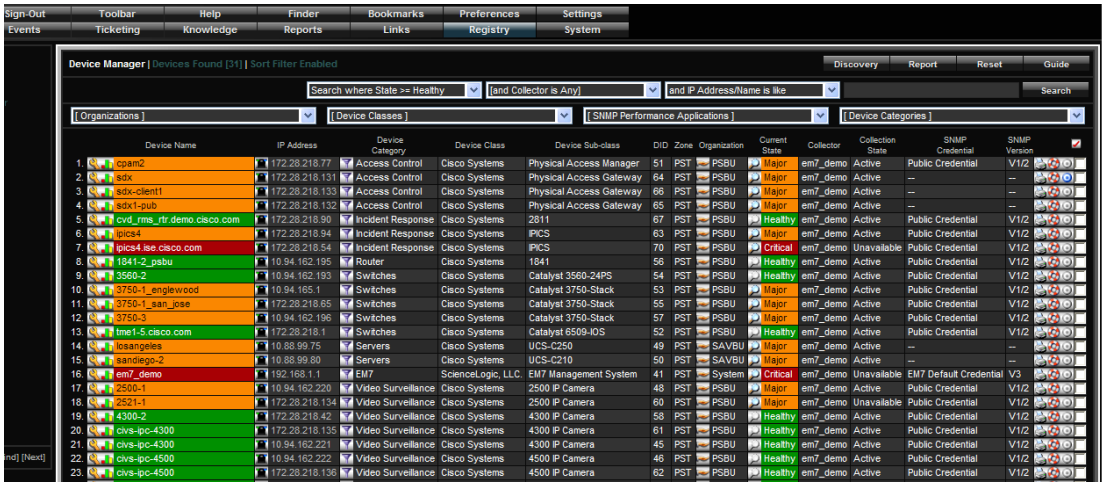
Figure 7-11 PSS Faults—Active Event View



All of the active events in the system are shown in this view. The top event in the table is highlighted red to indicate the device is in a critical condition. This event corresponds to the IPICS server from Figure 7-9. The administrator can navigate to the same IPICS details screen by selecting on the device summary icon on the left hand side of the top row.

The Registry view is another view that is very useful for detecting and isolating faults. This view can be started by selecting the Registry tab on the main MAP menu bar. Figure 7-12 shows the Registry view.

Figure 7-12 PSS Faults—Registry View



The registry view shows the condition of each of the devices under management. In this case, row 17 on the table shows a Cisco 2500 Series IP camera with a major condition (orange colored label). After the administrator has detected this fault on the camera and wants to isolate the problem, additional

information for the camera can be obtained remotely by selecting the camera device summary icon next to the camera name in the table. When the device summary icon is selected, detailed information about the camera is displayed, as shown in Figure 7-13.

Figure 7-13 PSS Faults—Component Summary View (Cisco IP Camera)

The device summary for the camera shows that it has exceeded the threshold set for bandwidth utilization. This is an example of a potential issue in the network that needs to be addressed. After the administrator is aware of the issue, corrective action can be taken before this escalates to a critical condition.

Collecting and Storing Compliance Information

Organizations that require collection and storage of information for compliance and liability reasons benefit from the MAP solution. The MAP appliance is able to collect many statistics using industry standard SNMP, SQL, or custom API calls, store the statistics, and provide standard and custom reports to show operational trends related to each statistic collected.

In the Urban Security lab on the Cisco campus, the MAP appliance has been configured to collect statistics such as memory and disk utilization. Custom thresholds have been set to allow the MAP appliance to generate alerts on behalf of PSS components when memory or disk utilization is too high. Figure 7-14 shows one of the applications created for the Urban Security lab.

Figure 7-14 MAP Application Configuration

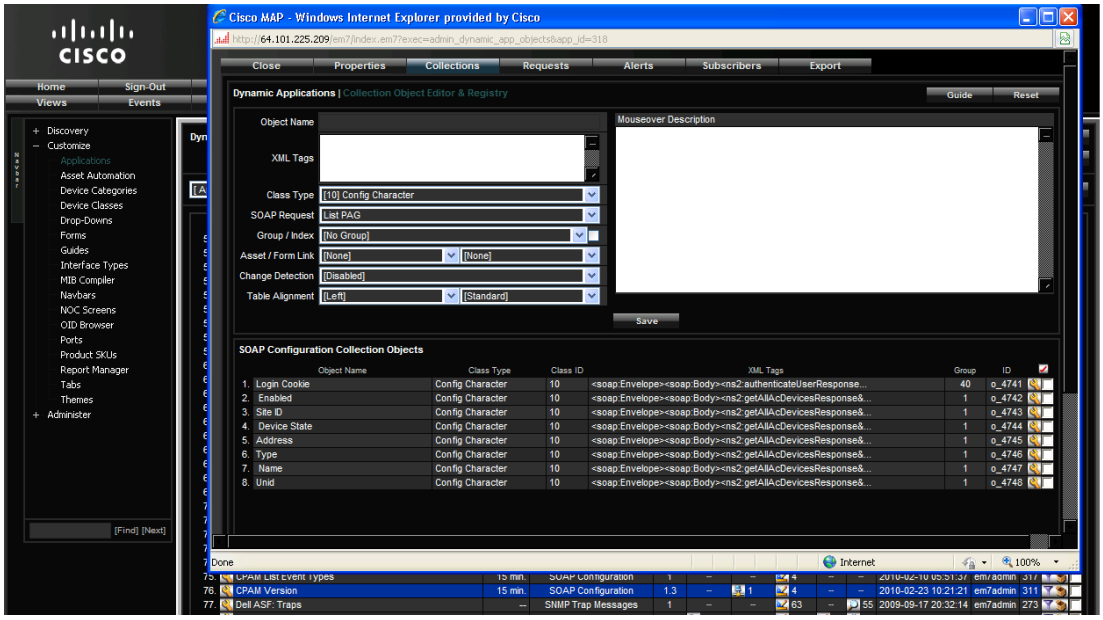


Figure 7-15 shows the physical memory utilization for a Cisco Physical Access Manager component. Reports can also be generated in a number of formats including HTML, CSV, PDF, and others.

Figure 7-15 MAP Memory Utilization Trends

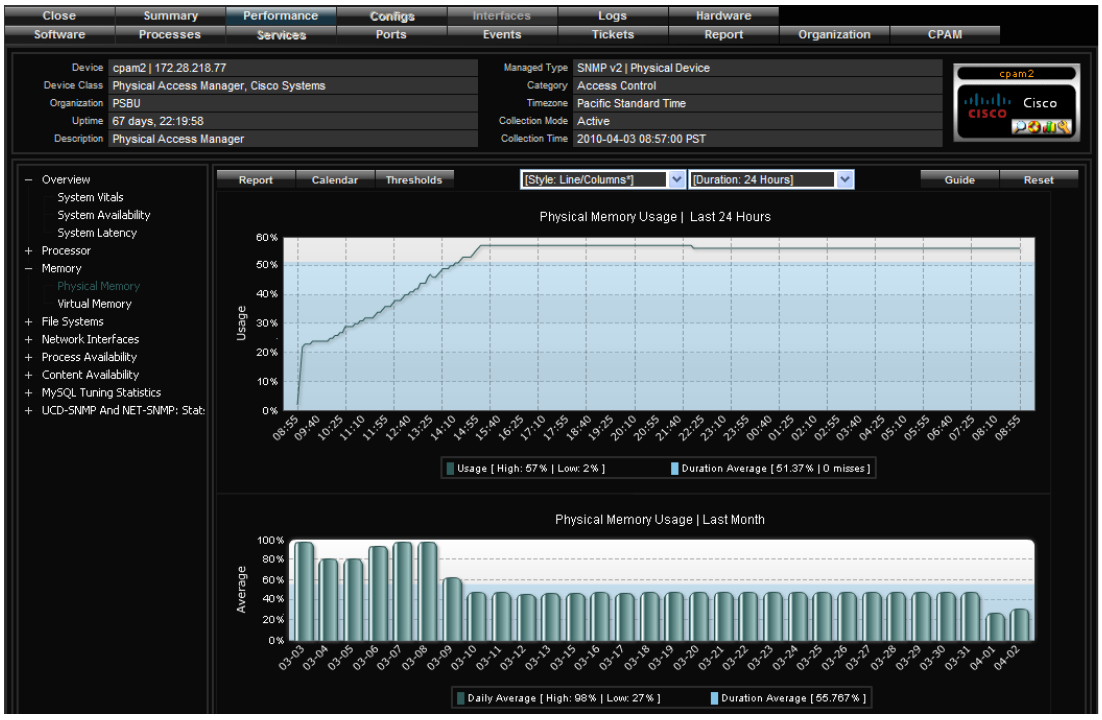
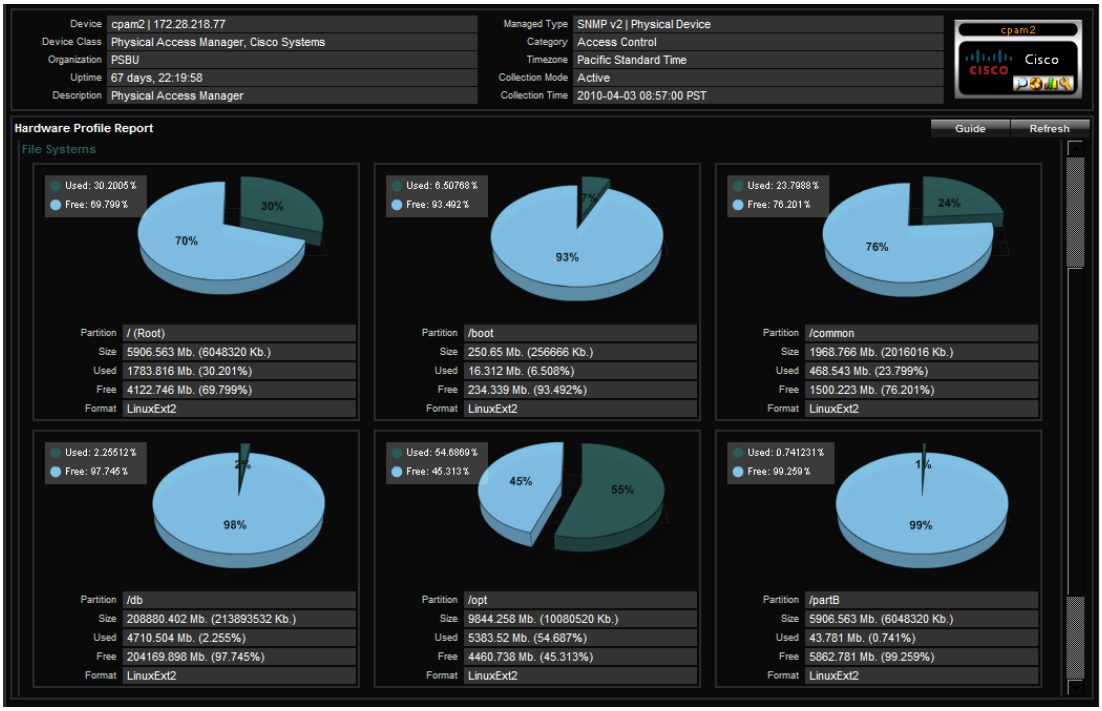


Figure 7-16 shows the disk utilization for a Cisco Physical Access Manager component. Reports can also be generated in a number of formats including HTML, CSV, PDF, and others.

Figure 7-16 MAP Disk Utilization Trends



Cisco MAP Deployment Options

The MAP appliance allows flexible deployment in the PSS system. It can be deployed as an all-in-one single appliance in a central location to monitor devices across the entire PSS system, or it can be distributed across the PSS system network with collectors in each branch or local office. It can also be configured in a redundant fashion to provide a highly available collector service.

This flexibility in deployment allows Cisco to provide remote monitoring capabilities tailored to meet each customer's needs based on individual sophistication and expertise levels. Following are a few potential deployment options for the MAP appliance:

- As a traditional Remote Managed Service (RMS) with proactive management of the PSS system provided as a service by Cisco where Cisco continuously monitors the PSS system on behalf of the customer
- As a light RMS deployed on-site or remotely where PSS components are monitored by the MAP appliance and notifications are automatically generated and sent to key customer personnel in the event of system failures
- As an integrated component of other Cisco smart services

The MAP appliance can be deployed as a distributed system with collectors in one or more of the remote locations. The configuration of the MAP solution can easily be tailored to meet the needs of each PSS solution developed to maximize the return on investment.

CHAPTER 8

Lab and Test Overview

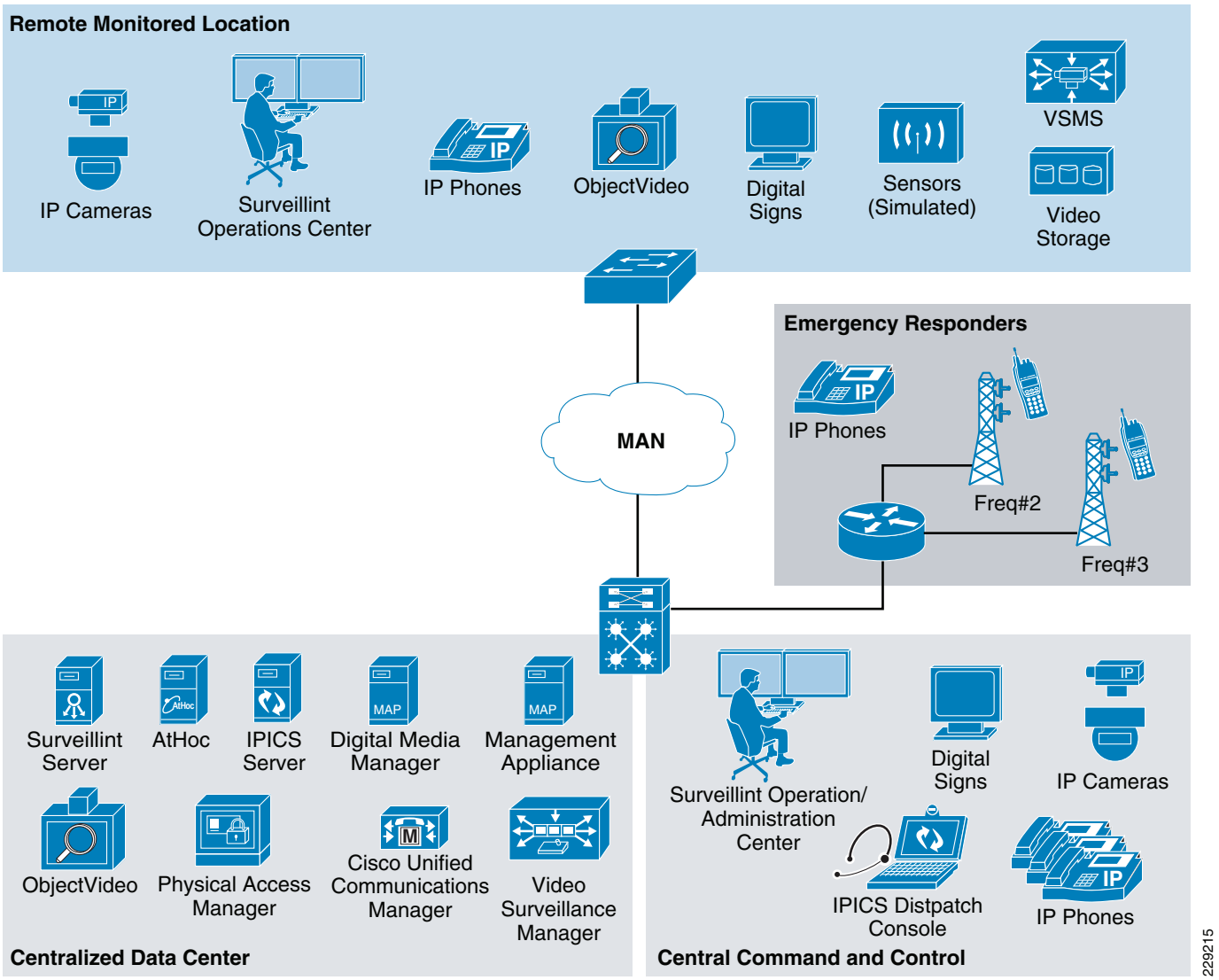
Test Overview

The main goal of the Urban Security solution was to simulate a security environment with various locations and diverse requirements. The main emphasis was on validating the interoperability of various devices and integrating them into a single security monitoring environment. Various events were used to integrate ObjectVideo analytics and access control into Surveillint's single command and control system. In turn, notifications were communicated to IPICS and AtHoc for incident response and mass notification.

The lab environment includes a centralized command and control center, remote monitored locations, and emergency responders connecting via land mobile radios. By centralizing the main communication devices, a large distributed environment can be created, with cameras, sensors, and security devices distributed to resolve security incidents quickly.

The solution did not focus on testing Layer 2 or Layer 3 features typical of a campus network or distributed deployments, because those features have been extensively documented in other solution guides. Figure 8-1 shows the various locations configured for the test environment.

Figure 8-1 Lab Environment



Cisco Video Surveillance

A single Cisco video surveillance Operations Manager was deployed at the centralized data center to manage Media Servers deployed at remote locations. The local Media Servers were able to archive video from local cameras to reduce the bandwidth requirements across the MAN. Because each Media Server acts as a proxy to the local IP cameras and viewers, the video traffic is contained as much as possible.

Cisco Physical Access Control

A single CPAM server was deployed at the central command and control center to manage access gateways deployed at various remote locations. Because the testing focused on integrating various components, rather than scalability, access gateways were installed only at the central site. Proximex Surveillint is able to send and receive alerts from multiple access gateways distributed in many locations.

Proximex Surveillint

A single Surveillint was deployed at the central command and control center, with multiple clients connecting from all remote locations. Surveillint is able to scale to support a large number of clients/sensors by distributing its services across multiple servers and locations.

Hardware/Hardware

Table 8-1 shows the different harware devices and software releases used during the solution testing.

Table 8-1 Device and Software versions

Device	Location	Software Release
Cisco VSOM	Command and control	4.2
Cisco VS Media Server	Command and control and remote locations	6.2
Cisco 2500 IP Cameras	Command and control and remote locations	2.1.2
Cisco 2521V Dome IP Cameras	Command and control and remote locations	2.1.2
Cisco 4300 IP Cameras	Command and control and remote locations	1.0.3
Cisco 4500 IP Cameras	Command and control and remote locations	1.0.1
Cisco CPAM	Command and control	1.2
Cisco Access Gateway	Command and control and remote locations	1.2
Cisco IPICS	Command and control	4.0
Cisco Unified Communications Manager	Command and control	7.1.3.1.10000-11
Cisco DMP	Command and control and remote locations	5.1
ObjectVideo	Command and control and remote locations	5.1.0
Proximex Surveillint	Command and control	5.0
AtHoc	Command and control	6.1.8.76

APPENDIX A

Reference Documents

- Cisco IP Video Surveillance Design Guide—http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_surveillance.html

Cisco Physical Access Control

- Cisco Physical Access Manager Appliance User Guide, Release 1.2.0—http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpam/1_2_0/english/user_guide/cpam_1_2_0.html
- Cisco Physical Access Gateway User Guide, Release 1.2.0—http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpag/gateway/1_2_0/english/user_guide/cpag_ug_1_2_0.html

Cisco Video Surveillance

- Cisco 2500 Series Video Surveillance IP Camera—http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9692/ps7307/data_sheet_c78-455613.html
- Cisco 4000 Series Video Surveillance High-Definition IP Cameras—http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9692/ps9716/data_sheet_c78-492032.html
- Cisco IP Video Surveillance Design Guide—http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_surveillance.html
- Cisco Video Surveillance Operations Manager User Guide—http://www.cisco.com/en/US/products/ps9153/products_user_guide_list.html
- Cisco Video Surveillance Media Server User Guide Release—http://www.cisco.com/en/US/products/ps9152/products_user_guide_list.html
- Cisco Video Management and Storage System Installation and Upgrade Guide—http://www.cisco.com/en/US/docs/video/cvmss/rel1_1/installation/guide/cvmssinst.html

Cisco Unified Communications

- Cisco Unified Communications Manager Install and Upgrade Guides—http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

Cisco IP Interoperability and Collaboration System

- Cisco IPICS Dispatch Console User Guide—http://www.cisco.com/en/US/docs/interoperability_systems/c_ipics/401/dispatch_console/user_guide/diconsole_ug.pdf
- Cisco IPICS Mobile Client for Apple iPhone—http://www.cisco.com/en/US/docs/interoperability_systems/c_ipics/401/iphone_app/guide/iphoneappbook.html
- Solution Reference Design (SRND) for Cisco IPICS Release 2.2(1)—http://www.ciscopowered.biz/en/US/docs/interoperability_systems/c_ipics/221/design/guide/IPICS_221.html
- Cisco IPICS API Reference Guide—https://www.cisco.com/en/US/docs/interoperability_systems/c_ipics/221/api/guide/api.pdf
- Cisco IPICS Compatibility Matrix —http://www.cisco.com/en/US/products/ps7026/products_device_support_tables_list.html

Cisco Digital Media Suite

- Cisco Digital Media Suite 5.2 Design Guide for Enterprise Medianet—http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/DMS_DG/DMS_DG.html

Cisco Management Appliance

- Cisco Management Appliance—http://www.cisco.com/go/ros

Partner Products

- Proximex—http://www.proximex.com
- AtHoc—http://www.athoc.com/products/athoc-iwsalerts/overview-a-benefits.html
- ObjectVideo—http://www.objectvideo.com/thesoftware