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.

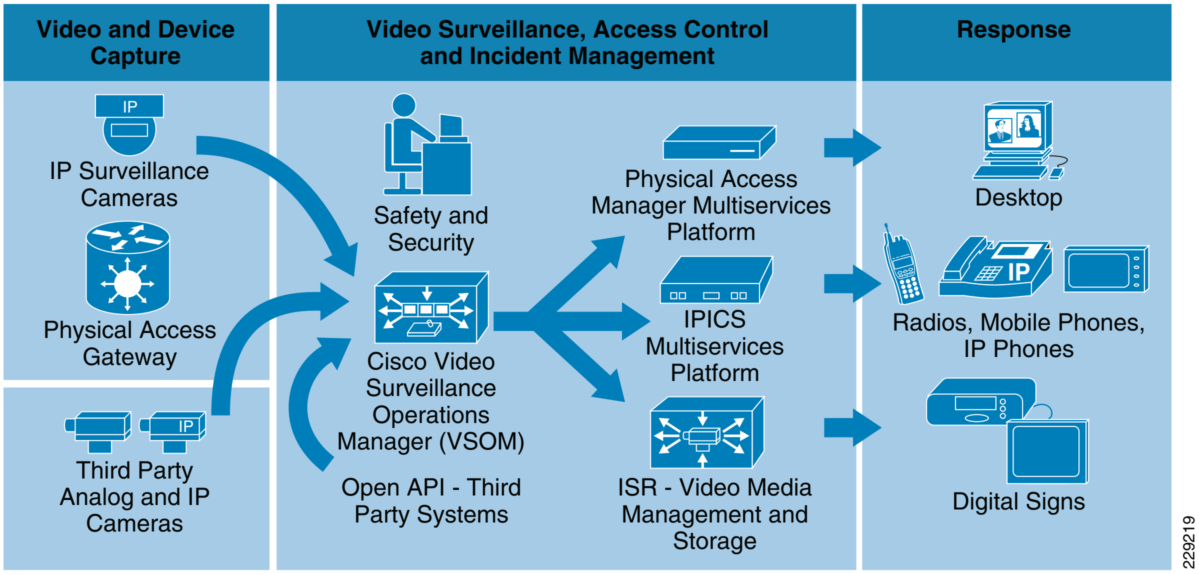
Cisco’s solution offers hardware and software to support video transmission, monitoring, recording, and management. Cisco video surveillance solutions work in unison with the advanced features and functions of the IP network infrastructure—switches, routers, and other network security devices—to enable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


Video and Device Capture
Video Surveillance, Access Control and Incident Management
Response
IP
IP Surveillance Cameras
Physical Access Gateway
IP
Third Party Analog and IP Cameras
Safety and Security
Cisco Video Surveillance Operations Manager (VSOM)
Open API - Third Party Systems
Physical Access Manager Multiservices Platform
IPICS Multiservices Platform
ISR - Video Media Management and Storage
Desktop
IP
Radios, Mobile Phones, IP Phones
Digital Signs
229219

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.

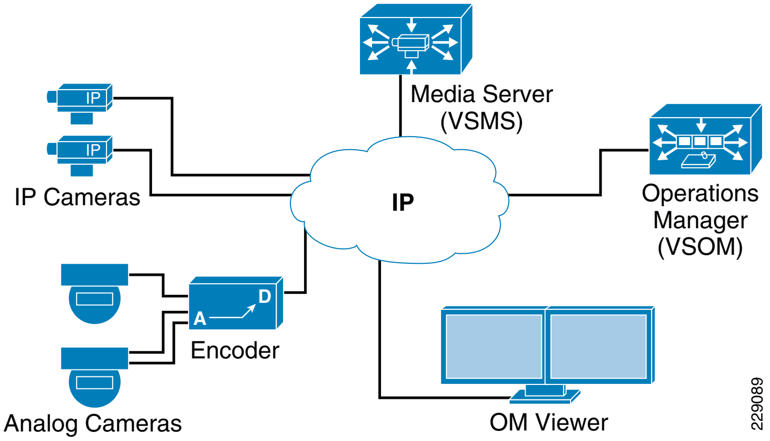
Cisco Video Surveillance Media Server

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



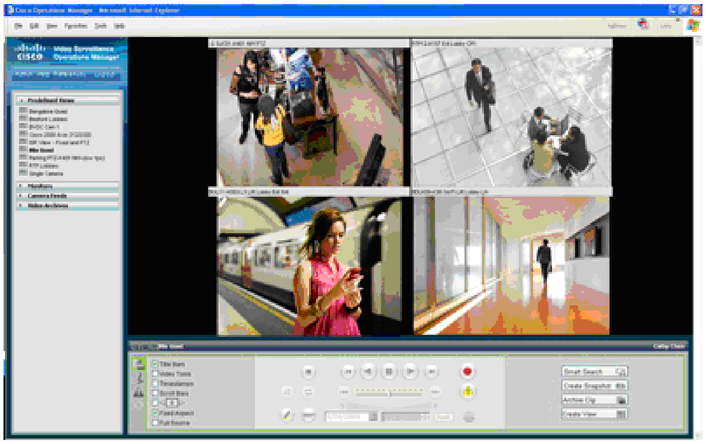
By using the power and advanced capabilities of today's IP networks, the Media Server software allows third-party applications, additional users, cameras, and storage to be added over time. This system flexibility and scalability supports the following:

- 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

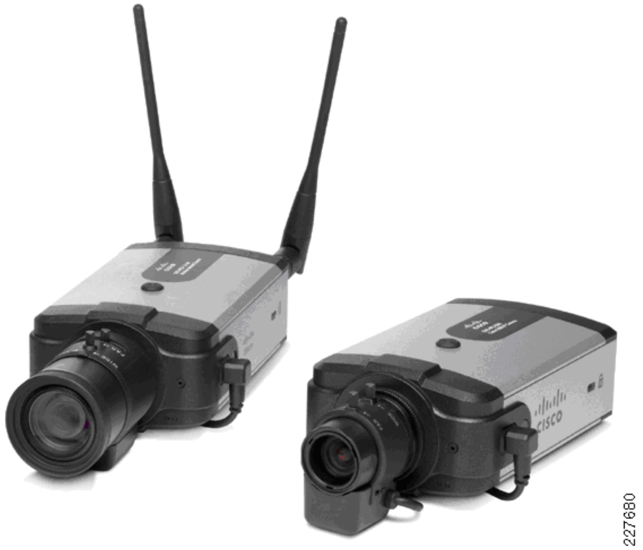
Cisco Video Surveillance IP Cameras

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:

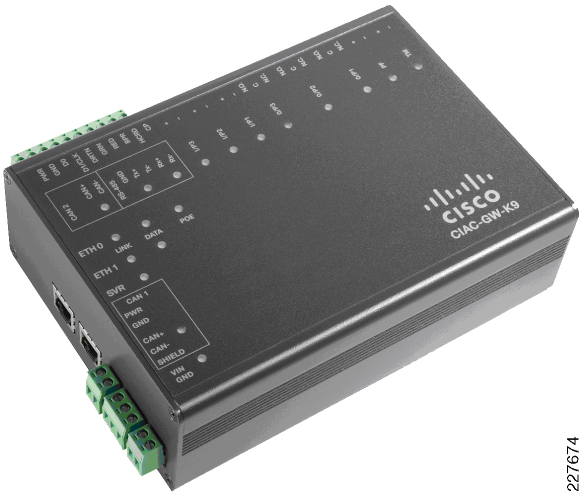
- True high-definition video—The camera streams crisp and clear 1080p (1920 x 1080) video at 30 frames per second while maintaining surprisingly low network bandwidth.
- Progressive scan video—The camera captures each frame at its entire resolution using progressive scan rather than interfaced video 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

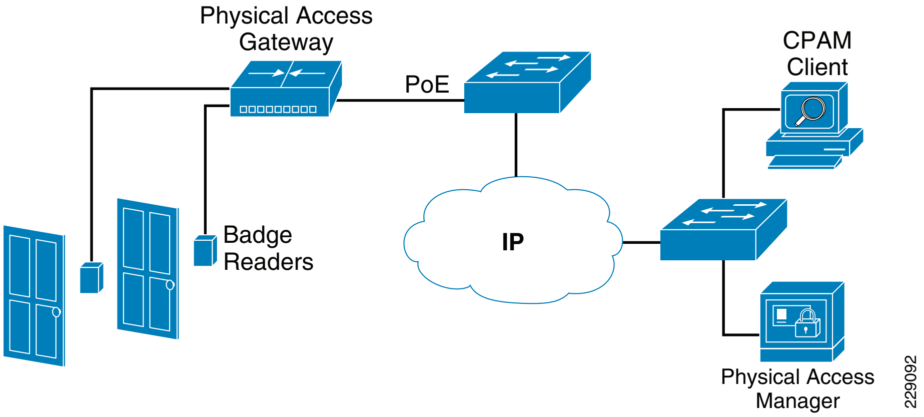


The Cisco Physical Access Manager (CPAM) is a management appliance for configuration, monitoring, and report generation. It can manage up to 2,000 Cisco Physical Access Gateways distributed across different network locations. Figure 3-8 shows a CPAM appliance.

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.

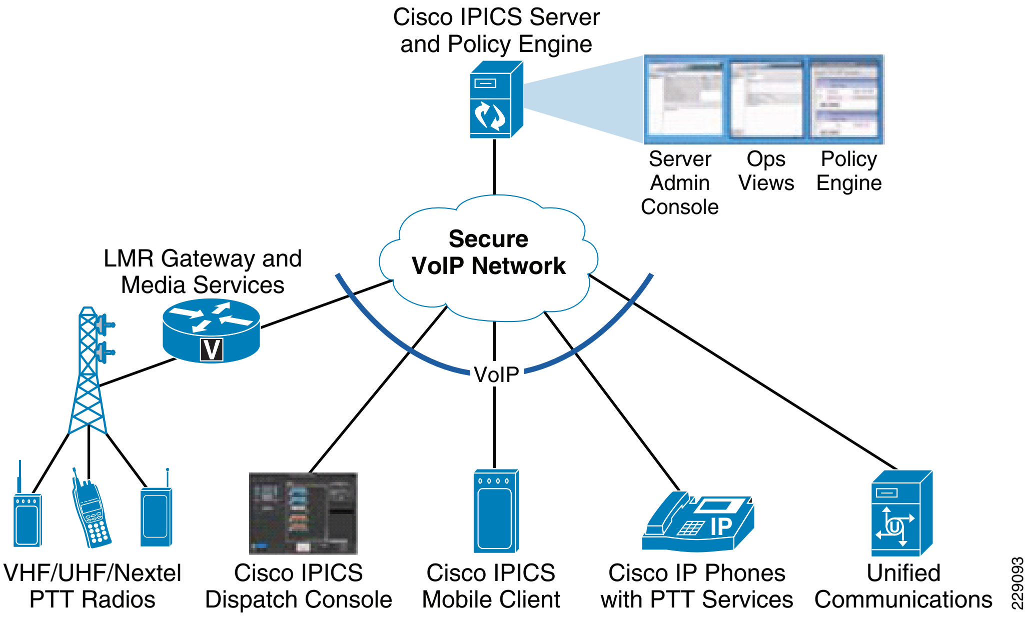
IPICS Functions

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


Cisco IPICS Server and Policy Engine
Server Admin Console
Ops Views
Policy Engine
LMR Gateway and Media Services
Secure VoIP Network
VoIP
VHF/UHF/Nextel PTT Radios
Cisco IPICS Dispatch Console
Cisco IPICS Mobile Client
Cisco IP Phones with PTT Services
Unified Communications
229093

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.

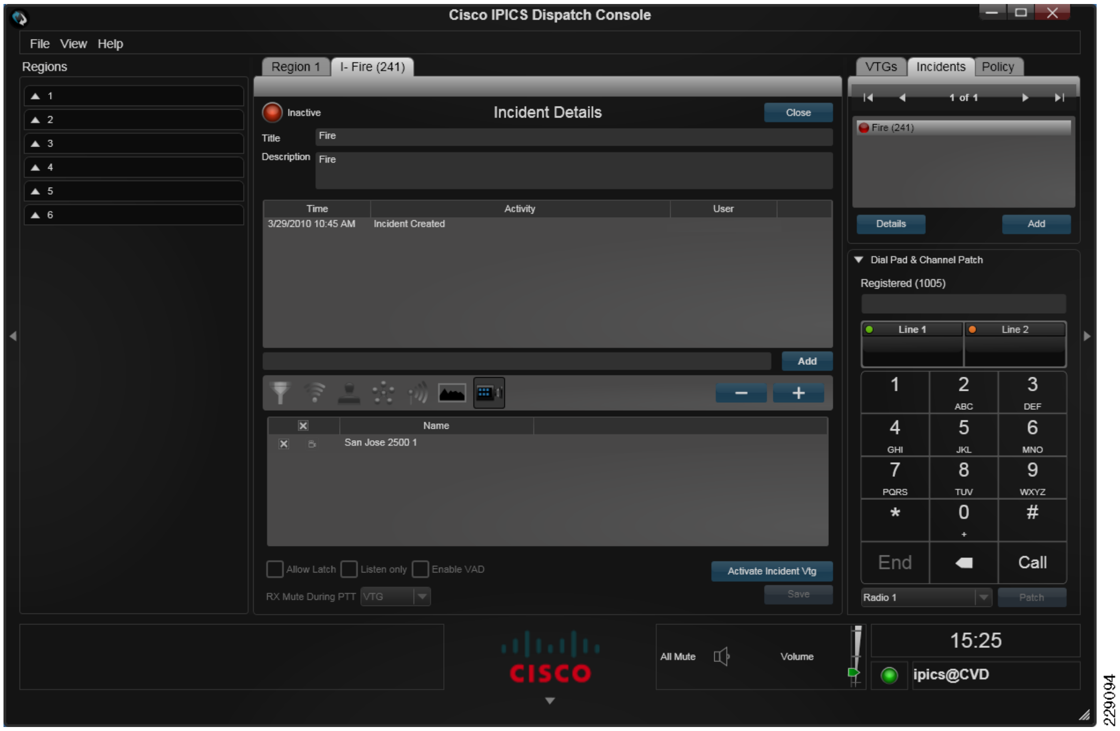
Step 2 Search for the application.

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



Inactive Incident Details

Title: Fire

Description: Fire

Time	Activity	User
3/29/2010 10:45 AM	Incident Created	

Name
San Jose 2500 1

□ Allow Latch □ Listen only □ Enable VAD

RX Mute During PTT: VTG

1 of 1

Fire (241)

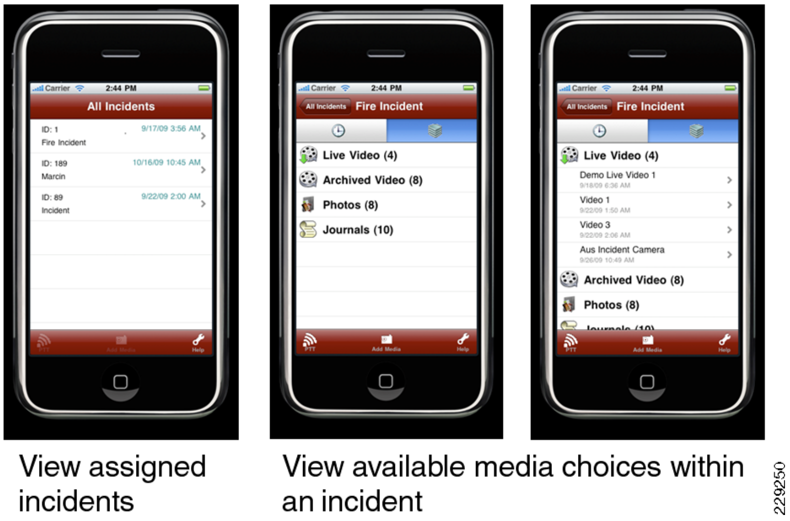
Registered (1005)

Radio 1

15:25

ipics@CVD

Figure 3-12 Menu on IPICS Mobile Client



All Incidents

ID: 1 Fire Incident	9/17/09 3:56 AM
ID: 189 Marcin	10/16/09 10:45 AM
ID: 89 Incident	9/22/09 2:00 AM

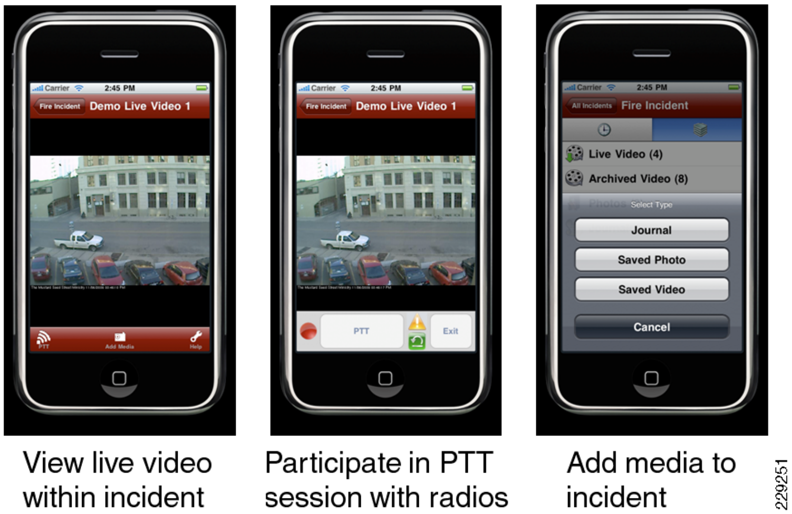
Fire Incident

- Live Video (4)
- Archived Video (8)
- Photos (8)
- Journals (10)

Fire Incident

- Live Video (4)
  - Demo Live Video 1 — 9/18/09 6:36 AM
  - Video 1 — 9/22/09 1:50 AM
  - Video 3 — 9/22/09 2:06 AM
  - Aus Incident Camera — 9/26/09 10:49 AM
- Archived Video (8)
- Photos (8)
- Journals (10)

Figure 3-13 Live Video on IPICS Mobile Client



View live video within incident

Participate in PTT session with radios

Add media to incident

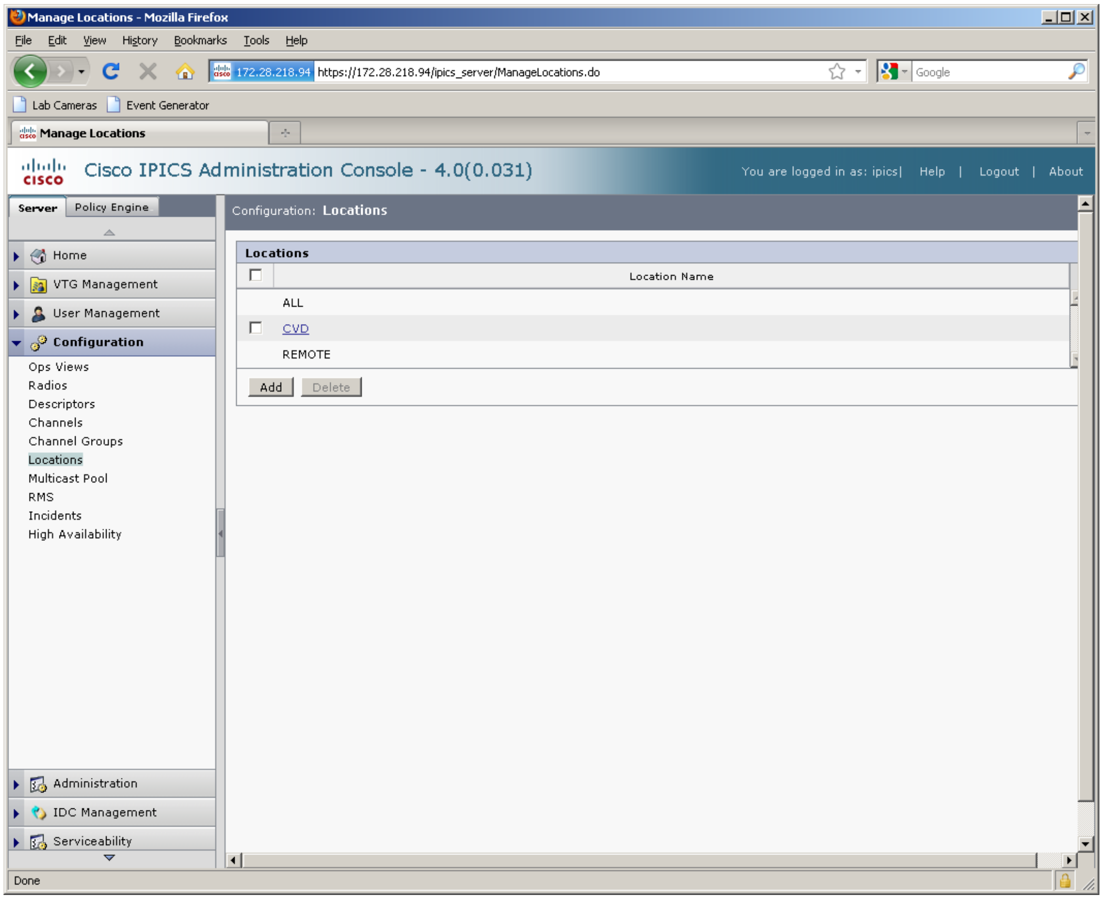
Components of IPICS

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



Locations

□	Location Name
	ALL
□	CVD
	REMOTE

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.

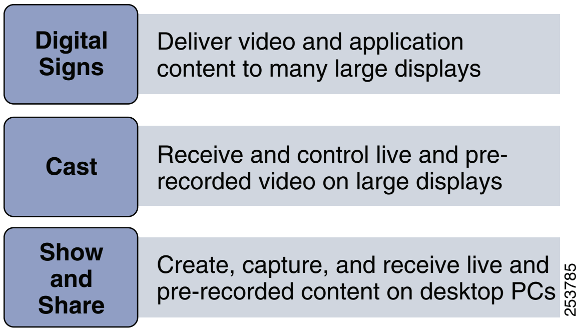
The Cisco Unified Communications Manager, deployable on the Cisco 7800 Series Media Convergence Servers or on third-party servers, offers the following features:

- 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 Signs	Deliver video and application content to many large displays
Cast	Receive and control live and pre-recorded video on large displays
Show and Share	Create, capture, and receive live and pre-recorded content on desktop PCs

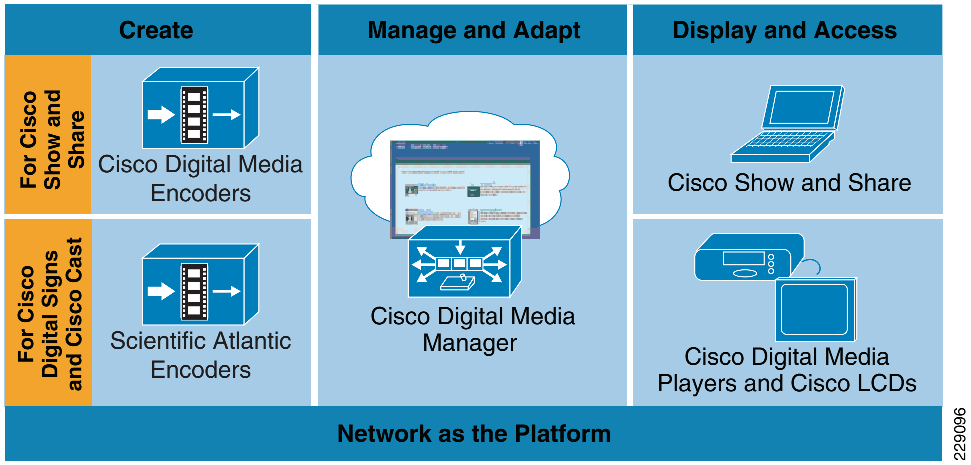
Digital Media draws viewers whether the content is marketing, internal communications, training, advertising, or entertainment materials. More and more organizations are using digital media to deliver timely and targeted communications. Digital Media is creating a new kind of customer experience and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



Create
Manage and Adapt
Display and Access
For Cisco Show and Share
Cisco Digital Media Encoders
For Cisco Digital Signs and Cisco Cast
Scientific Atlantic Encoders
Cisco Digital Media Manager
Cisco Show and Share
Cisco Digital Media Players and Cisco LCDs
Network as the Platform
229096

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.

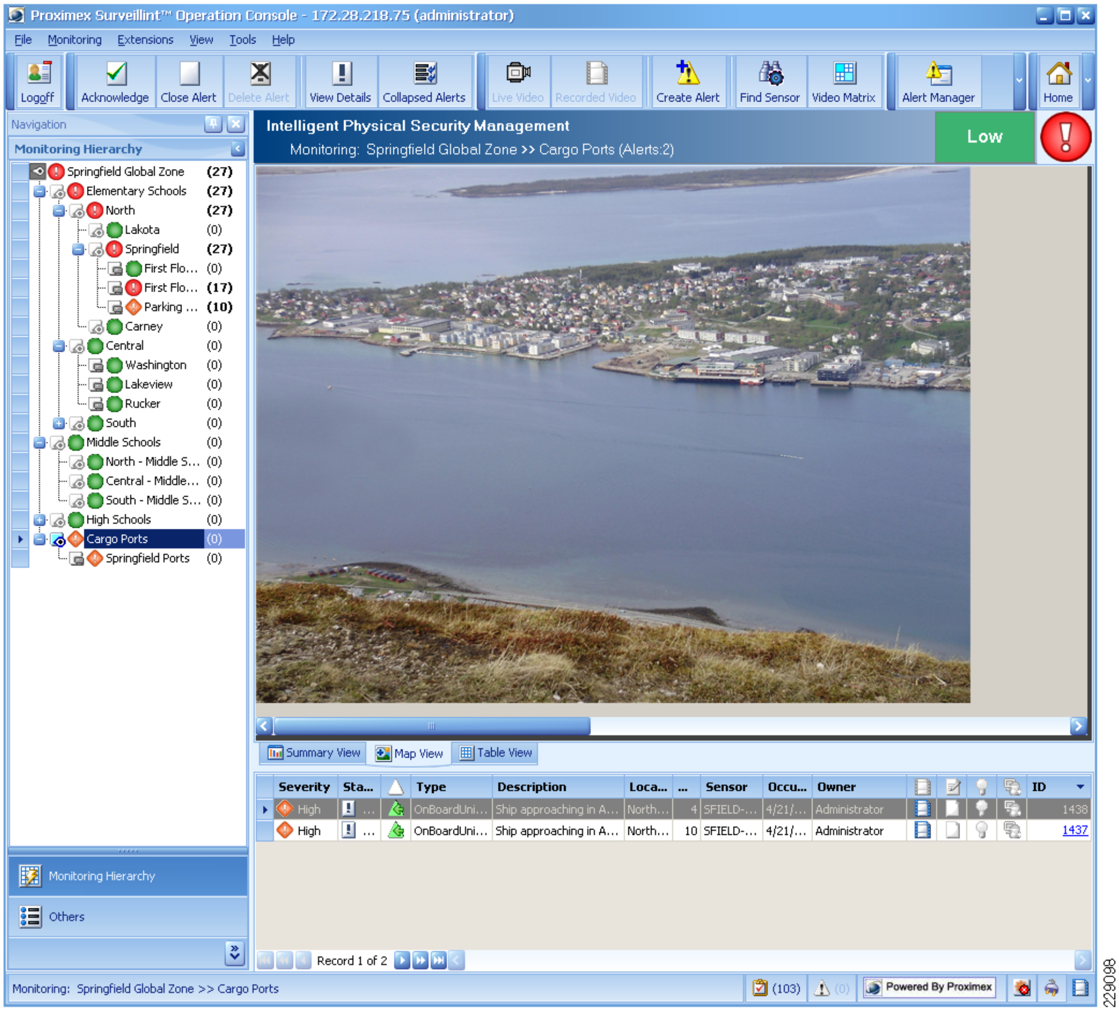
Surveillint connects disparate information to mitigate risk across an enterprise by providing actionable intelligence, speeding security incident resolution, and reducing security operations costs.

- 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



Proximex Surveillint™ Operation Console - 172.28.218.75 (administrator)

- Springfield Global Zone (27)
  - Elementary Schools (27)
    - North (27)
      - Lakota (0)
      - Springfield (27)
        - First Flo… (0)
        - First Flo… (17)
        - Parking … (10)
      - Carney (0)
    - Central (0)
      - Washington (0)
      - Lakeview (0)
      - Rucker (0)
    - South (0)
  - Middle Schools (0)
    - North - Middle S… (0)
    - Central - Middle… (0)
    - South - Middle S… (0)
  - High Schools (0)
  - Cargo Ports (0)
    - Springfield Ports (0)

Intelligent Physical Security Management

Monitoring: Springfield Global Zone >> Cargo Ports (Alerts:2)

Low

Severity	Sta…		Type	Description	Loca…	…	Sensor	Occu…	Owner					ID
High	! …		OnBoardUni…	Ship approaching in A…	North…	4	SFIELD-…	4/21/…	Administrator					1438
High	! …		OnBoardUni…	Ship approaching in A…	North…	10	SFIELD-…	4/21/…	Administrator					1437

Record 1 of 2

Monitoring: Springfield Global Zone >> Cargo Ports (103) (0) Powered By Proximex

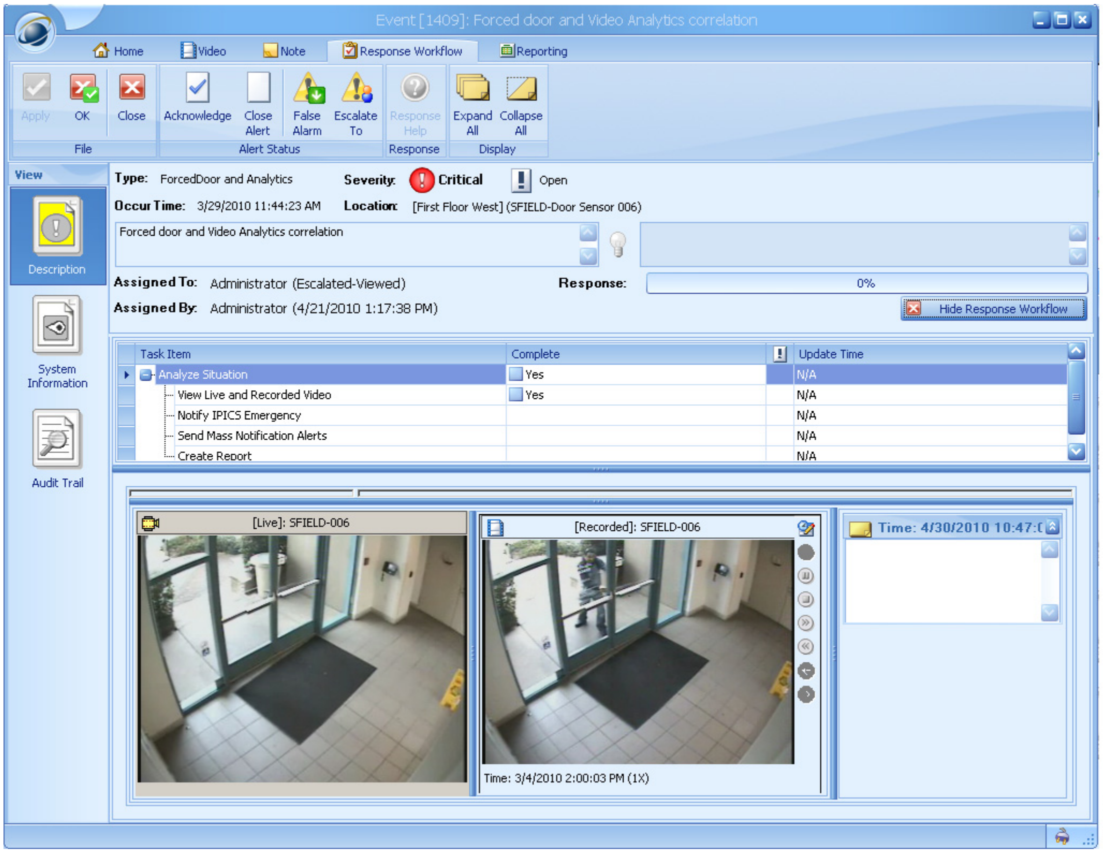
The hierarchical maps enable security teams to find resources and quickly identify the precise location of incidents. Operators can visualize sensor and alert locations, simultaneously view live and recorded video, view asset/external event location displays, and execute sensor commands directly from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



Type: ForcedDoor and Analytics
Severity: Critical ! Open
Occur Time: 3/29/2010 11:44:23 AM
Location: [First Floor West] (SFIELD-Door Sensor 006)

Forced door and Video Analytics correlation

Assigned To: Administrator (Escalated-Viewed)
Response: 0%
Assigned By: Administrator (4/21/2010 1:17:38 PM)

Task Item	Complete	!	Update Time
Analyze Situation	☐ Yes		N/A
View Live and Recorded Video	☐ Yes		N/A
Notify IPICS Emergency			N/A
Send Mass Notification Alerts			N/A
Create Report			N/A

- 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.

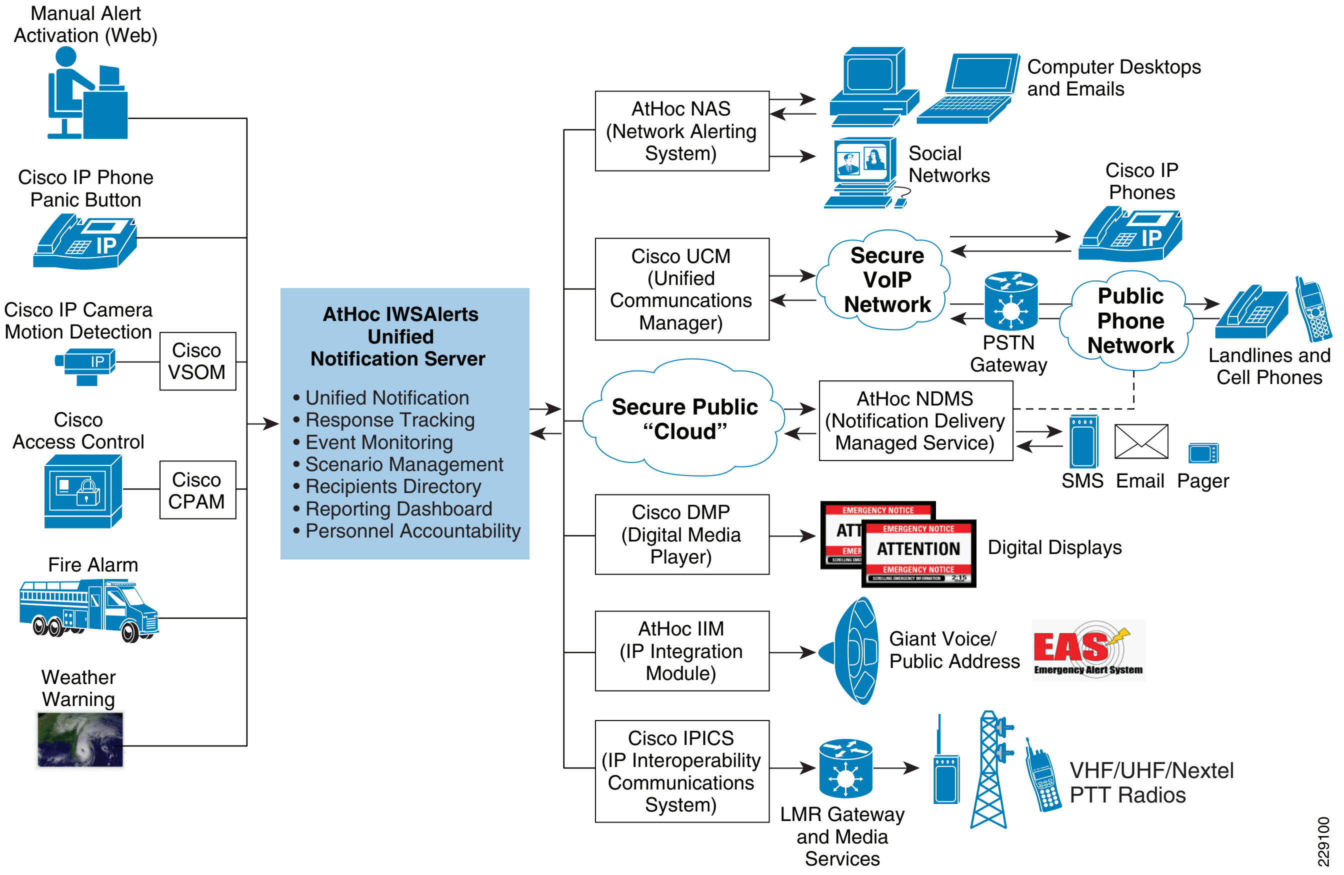
AtHoc IWSAlerts provides several benefits, including the following:

- 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


Manual Alert Activation (Web)
Cisco IP Phone Panic Button
IP
Cisco IP Camera Motion Detection
IP
Cisco VSOM
Cisco Access Control
Cisco CPAM
Fire Alarm
Weather Warning
AtHoc IWSAlerts Unified Notification Server
• Unified Notification
• Response Tracking
• Event Monitoring
• Scenario Management
• Recipients Directory
• Reporting Dashboard
• Personnel Accountability
AtHoc NAS (Network Alerting System)
Computer Desktops and Emails
Social Networks
Cisco IP Phones
IP
Cisco UCM (Unified Communications Manager)
Secure VoIP Network
PSTN Gateway
Public Phone Network
Landlines and Cell Phones
Secure Public "Cloud"
AtHoc NDMS (Notification Delivery Managed Service)
SMS
Email
Pager
Cisco DMP (Digital Media Player)
EMERGENCY NOTICE
ATTENTION
Digital Displays
AtHoc IIM (IP Integration Module)
Giant Voice/ Public Address
EAS
Emergency Alert System
Cisco IPICS (IP Interoperability Communications System)
LMR Gateway and Media Services
VHF/UHF/Nextel PTT Radios
229100