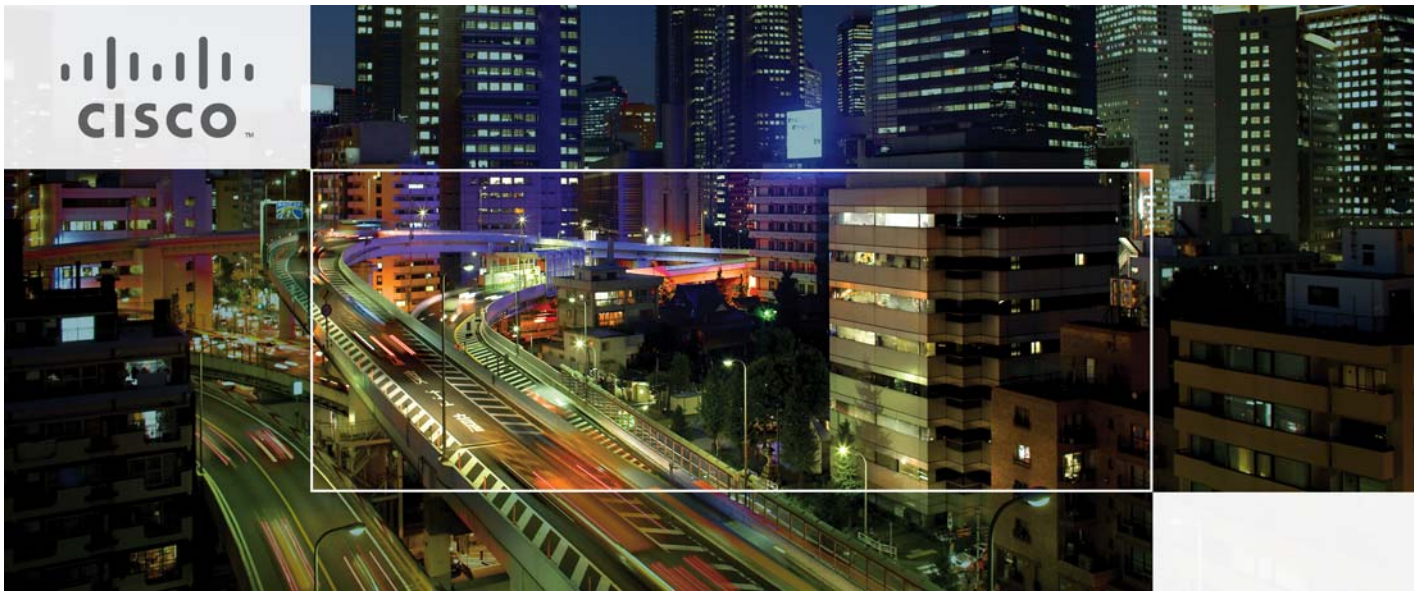


Physical Safety for Schools Application Deployment Guide

Last Updated: November 4, 2009

Overview 1
Executive Summary 1
Solution Description 1
Solution Benefits 2
Scope of the Solution 2
Use Cases 2
Smoke Alarm 2
Fire Detection 2
Hall Monitor 2
Forced Entry 3
Theft Detection 3
CRE Integration 3
Solution Components 3
Cisco Physical Access Control 3
Cisco Video Surveillance 4
Cisco Video Surveillance Media Server 5
Cisco Video Surveillance Operations Manager 5
Cisco Video Surveillance IP Cameras 6
Cisco Unified Communications 7
Cisco Unified Communications Manager 7
Cisco Unified Communication Manager Express 7
Phones 8
Partner Products 8
Augusta EdgeFrontier 8
Singlewire InformaCast 9
Solution Framework 9
Designing the Solution 10
Cisco Physical Access Control 12
Time Synchronization 12
CPAM and Augusta EdgeFrontier 12
Cisco Video Surveillance 12
Video Surveillance Media Server 12
Video Surveillance Operations Manager 12
Augusta EdgeFrontier Notifications to VSOM 13
Required TCP/UDP Ports 13
Distributed Media Servers 14
Cisco 2500 and 4000 Series Cameras 14
Cisco 2500 Series Camera 14
Cisco 4000 Series Camera 15
Cisco Unified Communications 15
Required TCP/UDP Ports 15
IP Multicast 15
IP Phones 15
Other Considerations 15
Augusta EdgeFrontier Server 15
Augusta EdgeFrontier Notifications to Singlewire InformaCast 16
Video Feeds and Archives 16
High Availability 16
Baseline Architecture 17
Augusta EdgeFrontier 17
Video Surveillance 17
Physical Access Control 17
Notification 18
Implementing and Configuring the Solution 18
Cisco Physical Access Control 18
Establishing Connection Between CPAM and Physical Access Gateway 18
Configuring Door Hardware and Access Policies 19
Configure CPAM to Send Requests to Augusta EdgeFrontier 19
Cisco Video Surveillance 20
Managing Permissions and Rights 20
Camera/Time Synchronization 22
Viewing Archived and Live video from the District Office 23
Setting Up Video Surveillance Operations Manager for Motion Detection 25
Setting Up the 2500 Camera for Motion Detection 26
Setting Up the 4000 Series Camera for Motion Detection 27
Cisco Unified Communications 28
Cisco Unified Communications Manager 28

Cisco Unified Communications Manager Express 29
Partner Products Setup 29
Singlewire InformaCast 29
Augusta EdgeFrontier 31
Lab and Test Overview 55
Test Overview 55
Cisco Video Surveillance 55
Cisco Physical Access Control 56
Augusta EdgeFrontier and Singlewire InformaCast 56
Hardware/Software 56
Appendix A—Reference Documents 57

Physical Safety for Schools Application Deployment Guide

Overview

Executive Summary

Education stakeholders need to focus on the safety and security of schools, colleges, and universities. With the wide spectrum of safety incidents occurring on campuses, the need to protect students and monitor school assets has become increasingly important. From natural to man-made incidents, across both the virtual and physical domains, education institutions today must confront myriad challenges, including the following:

- Student, faculty, and staff safety
- Situational-awareness and common operating picture
- Outbound communications to students, parents, and authorities
- Operational status—What is happening?
  - Fire, smoking, drugs, violence, vandalism, and loitering

Using the Cisco end-to-end network as the platform, a variety of solutions can be deployed to meet safety and security needs. The Cisco Physical Safety for Schools solution portfolio features the following:

- Unified Communications
- Self-Defending Network
- Physical Access Control
- Video Surveillance

The Physical Safety for Schools solution provides educational institutions with the capabilities to evolve their schools into safe, secure institutions able to protect their students and respond appropriately in case of emergencies.

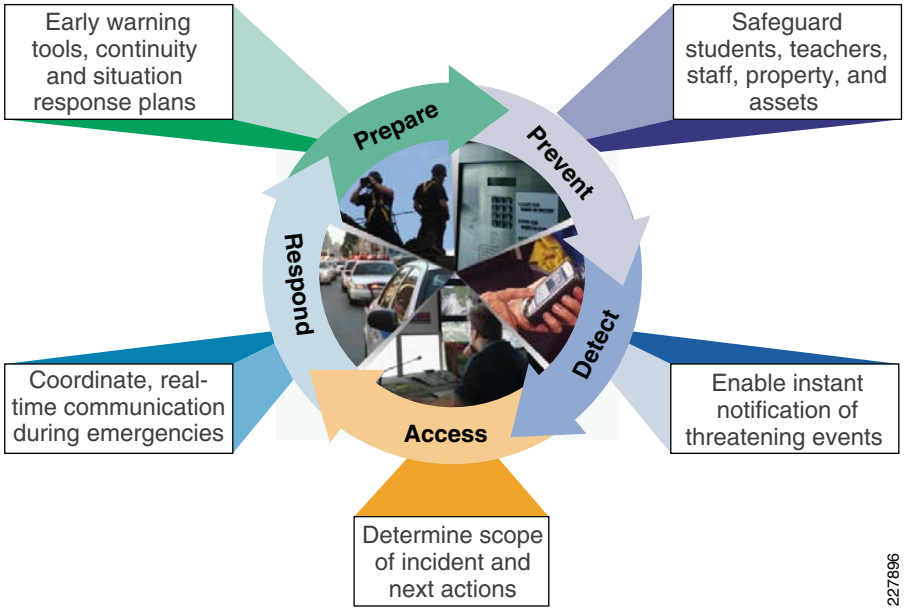
Solution Description

The Physical Safety for Schools solution focus on protecting the actual campus environments of schools and districts. Working with area law enforcement, facilities, and Information Technology (IT), schools can protect student data, better control network access, and help prevent unwanted intrusion.

The solution takes a holistic approach to security by integrating physical security devices with the IT infrastructures of districts and schools. See Figure 1.

There are three major functions of the solution as defined: *detect*, *monitor*, and *respond*.

Figure 1 Unified Command and Control



Detection takes on many forms, from keeping out unwanted guests at various times of the day to keeping in high value assets and equipment. The solution combines physical access control with video surveillance to provide a solid mechanism to secure educational environments.

Monitoring requires not only a way to watch what is happening, but a way to notify officials, faculty, and staff in the case of an emergency. Being able to correlate all of the alarms from the various sensors, cameras, and physical access control devices requires the ability to correlate that information and provide automated responses to avoid the need for human interaction in every situation. This correlation also provides a way to go back and review incidents, and creating plans and procedures to avoid them in the future.

Effective response requires a way to notify not only to the authorities, but also students, faculty, and parents. By integrating the correlation engine and the notification engine, notification to various groups of individuals can be automated. Additionally, there is the capability to provide proactive alerts and notification (i.e., egress directions, in the case of emergencies).

Solution Benefits

The Physical Safety for Schools solution provides several benefits to educational institutions, including the following:

- Improved communications and collaboration—A single communications system combining voice, video and data ensures on-and off-campus safety and security staff can respond immediately and appropriately to safety incidents.
- Enhanced visibility—Gain critical insight into safety and security systems with tools designed for sophisticated education environments.
- Minimized legal, regulatory, and financial liability—With more effective safety and security systems in place, schools can better protect students, teachers, staff, and assets while enduring appropriate response in the event of an incident.
- Improved motility—Access security resources and tools while in motion from anywhere on campus (indoors or outdoors).

Scope of the Solution

The Physical Safety for Schools solution focuses on the products and services necessary to create a safe environment for education. The scope of the solution focuses on the functional interaction between the products included. This also includes the actions/reactions necessary to properly secure the campus. Specific use cases have been tested in order to show the capabilities of the products, components and systems included.

This application deployment guide is not intended to instruct the reader on how to install and configure the specific components used in this solution. See the appropriate product user guides for installation and general configuration information for the appropriate products. References to these guide are provided in "Appendix A—Reference Documents" section on page -57.

Scale testing or load testing are not included in this application deployment guide. Where available, information has been included that covers some of these aspects.

High availability (HA) is always a challenging area to cover, with availability ranging from basic to 99.99999% uptime. This solution does not repeat HA testing that is covered at various component levels. Refer to the corresponding design guides listed in the "Appendix A—Reference Documents" section on page -57 for HA at various component levels. The solution includes limited-scope HA testing. The design guide discusses how HA could be implemented for K-12 schools and universities.

For more information on the baseline architecture, see the *Service Ready Architecture Design Guide* at the following URL:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns826/landing_srArchit_edu.html

For more information on designing and implementing video surveillance in an enterprise environment, refer to the *Cisco IP Video Surveillance Design Guide* at the following URL:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_surveillance.html

Use Cases

This application deployment guide focused on uses cases that can provide added safety and security to educational institutions.

Smoke Alarm

If smoke is detected, there are multiple responses that need to occur in rapid succession, if not simultaneously. In some cases, an alarm from a single smoke detector does not indicate the presence of a fire. For example, it could just be a student lighting a cigarette in the lavatory or it could be a motor overheating in the mechanical room.

In the case of smoke, the camera in closest proximity should ensure that it has a video record of the incident, and notification should be sent to the appropriate staff to investigate the situation.

Multiple secondary alerts may be required (i.e., to the school administrator, to the teaching staff in close proximity to the alert, and potentially to the maintenance staff). These alerts should include which camera is within proximity so that any staff can access the camera feed directly to monitor the situation.

Fire Detection

This situation could be triggered in multiple ways, and could have different reactions based on the method of trigger; for example, a fire pull station or a fire detection sensor.

Multiple alerts need to occur in rapid succession or simultaneously. The camera in closest proximity should ensure that it has a video record of the incident, and notification should be sent to the appropriate staff to investigate the situation. Evacuation instructions should be announced over the public address system with the preferred evacuation path. All of the phones in the building should indicate the preferred evacuation path based on the location of the fire. The system could also place the 911 call and provide the fire location within the building.

Note While the smoke and fire alarms with network-centric alerting is fully approved with DoD building codes and regulations, it has not yet been fully approved by the commercial market. This market is regulated by the National Fire Protection. For DoD regulation, refer to Section 7, Appendix C of the following document: http://www.wbdg.org/ccb/DOD/UFC/ufc_4_021_01.pdf

Hall Monitor

The potential for false positives is high in this situation. For example, it would not make sense to monitor a hallway for movement during the time between classes, and maybe not while the janitorial staff is working. But, after hours, when the hallways should be empty, any motion detected should trigger a notification so that a proper course of action can be determined. If a teacher decided to stay after hours to work on the next day's plan, that would not require a response. But, if a student was seen in the hallway after a predetermined time, this could indicate a situation that required a response. While it may not be possible to determine if the movement is the result of a student, a teacher, or even a mouse, the ability to quickly review and respond to the situation is required.

If motion is detected during defined hours, there should be no alarm notification. However, the video feeds should continue to be available for monitoring purposes.

If motion is detected outside of acceptable hours, the camera detecting motion should ensure that it has a video record of the incident, and notification should be sent to the appropriate staff to investigate the situation.

Additionally, if an abnormal incident occurs during normal working hours, a message could be sent to the staff on-site via the wireless phone and a prerecorded message could be sent to specific outside numbers (i.e., school administrators) indicating the nature of the alarm.

Forced Entry

The ability to monitor entry/exit doors is critical in the security of the building. The ability to identify when a fire door is opened that should not be, or an entry door opened after hours is a minimum requirement. By the same token, the exit doors can be opened during the day and should not create a notification situation. So similar to the motion detection, there is a need to monitor the doors and allow for different actions to be taken based on specific conditions (i.e., time of day).

If a fire door is opened during the day, the camera in the closest proximity should ensure that it has a video record of the incident, and notification should be sent to the appropriate staff to investigate the situation. The notification should provide the camera that is monitoring the door so that anyone can access the camera directly.

If an exit door is opened during the day, no alarm should be sent. If any door is opened outside of a predetermined time of day, notification should be sent to the appropriate staff to investigate the situation. The message should be sent to a predetermined list of individuals and the text should indicate the nature of the alarm. Depending on the workflow, a call should be placed to the police department and the video captured during the alarm situation should be forwarded to them for review.

In the case of a specific incident, an additional reaction to a situation could be the lockdown of a specific area that allows passage only to authorized persons; for example, an access to a mechanical room when smoke is detected. Allowing anyone access to that location could be dangerous and access should be controlled.

One other potential is controlling access during specific times of the day. For example, one school has been able to reduce tardiness in the students because they lock the entrance doors at a specific time of the morning. If students do not arrive by the specified time, they have to be allowed entry to the school. Knowing that they have the potential to be locked out of the school in the morning makes them more conscientious as to when they arrive.

At any time of the day, a forced entry is a critical incident. If a door sensor indicates a door is open but there is no associated card reader access or request for exit (exit from inside the building), it is a forced entry incident. Multiple alerts need to occur in rapid succession or simultaneously. The camera in closest proximity should ensure that it has a video record of the incident, and notification should be sent to the appropriate staff to investigate and respond to the situation.

Theft Detection

With the cost of hardware, software, and physical assets needed in the schools going up, the cost of theft for any of these assets is having a greater impact.

There are multiple ways to track assets within the campus, and the deployment and complexity will depend on the size of the campus that is being monitored. Using Active RFID tags and a wireless infrastructure with location-based services to actively monitor the movement of assets on the campus is one such mechanism. Alternatively, using passive RFID tags on the physical assets and securing the perimeter to monitor any assets moving outside of the secured area is a less expensive alternative.

By using passive RFID tags on physical assets and locating RFID exciters at the exits, it is possible to effectively monitor the movement of the assets outside of the secured perimeter.

Should an asset pass through the exit door at any time of day or night, the camera in closest proximity should insure that it has a video record of the incident. Additionally, a text message should be sent to all phones associated with security notifying that an asset has been removed, the type of asset that was removed, the door that it passed through and the camera that is monitoring the situation. An audible alarm is optional.

CRE Integration

A more complicated example of physical security is the integration of the physical security system with the mechanical systems, or the Connected Real Estate infrastructure. An example of this would be the potential to shut down the ventilation system in the event of a fire in a particular location.

Take for example a fire detected in a particular location. Once that location is identified, a automated signal could be sent to the ventilation system to shut all dampers in the affected location, and to shut off electricity in that location. While this use case was not tested in the lab due to the lack of available hardware resources, it is easy to understand how this could work based on the integration done in other cases.

Solution Components

The solution includes Cisco security products such as physical access control and video surveillance in addition to networking and unified communication products. In addition, the integration with products from Augusta Systems and Singlewire software provides a complete end-to-end solution.

Cisco Physical Access Control

The Cisco Physical Access Control 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.

The Cisco 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. The gateway has Ethernet ports to be connected to an IP network. This enables the gateway to be controlled over the network. To allow more inputs and outputs, additional Cisco modules (input, output, reader modules) can be connected to the gateway through a controller area network (CAN or CAN-bus). The door hardware connects to the gateway or other Cisco modules via either a Wiegand interface for card readers or directly to inputs for door sensors and output relays for locking hardware or Local Door Alarms. The gateway will function normally when network is down. Figure 2 shows a Physical Access Gateway.

Figure 2 Physical Access Gateway

The Cisco Physical Access Manager (CPAM) is a management appliance for configuration, monitoring, and report generation. CPAM server can support any combination of 2000 Access Control Gateways as well as input, output, or reader modules. Figure 3 shows a CPAM appliance and a management screen.

Figure 3 Cisco Physical Access Manager

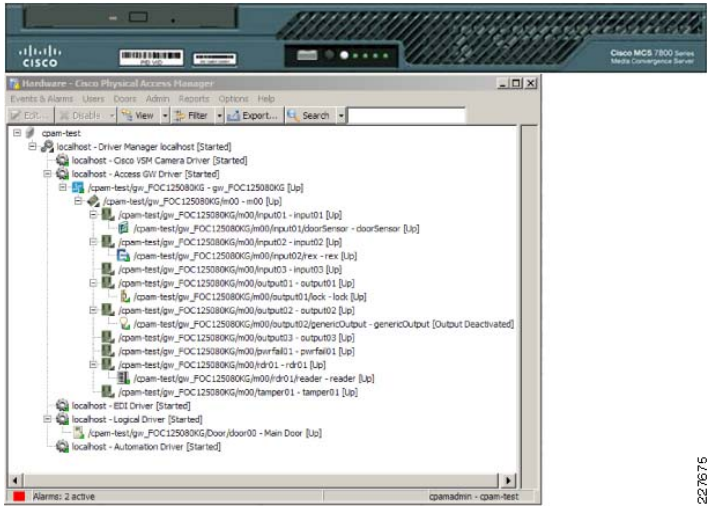
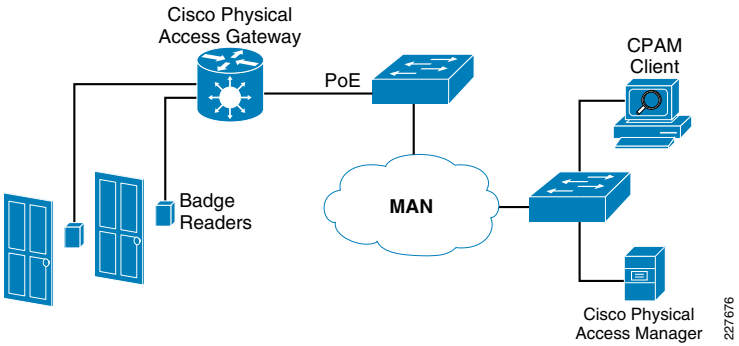


Figure 4 shows a typical physical access control deployment with badge readers located at different locations. With the proper authorization, users are able to connect to the CPAM remotely through CPAM client software to manage the environment.

Figure 4 Physical Access Control Deployment



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 as well as by recording events for subsequent investigation, proof of compliance, and audit purposes.

For school systems that need to visually monitor 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 motion, heat, and environmental sensors.

In a typical school environment, several systems are deployed for disparate applications, such as physical 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 and limit the return on their system investments.

Cisco's solution offers software and hardware 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.

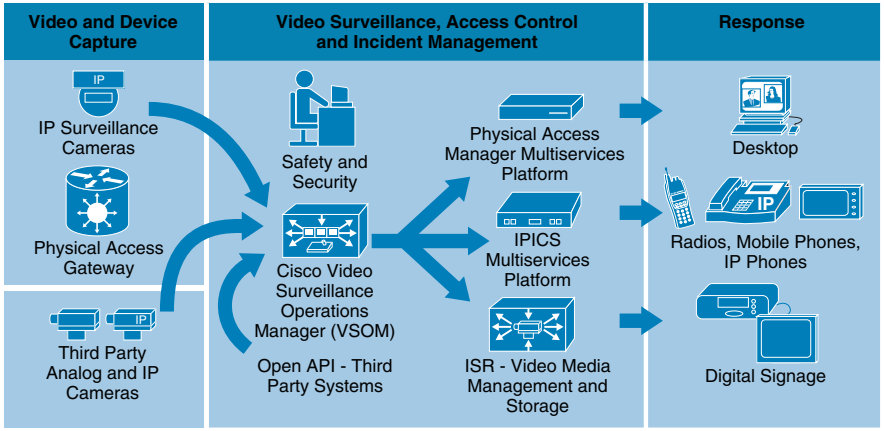
Through the Cisco architecture, video can be accessed at any time from any place, enabling real-time incident response, investigation, and resolution. As an extension of the Cisco Self-Defending Network, the Cisco intelligent network enables educational institutions to use existing investments in video surveillance and physical access control while enhancing the protection of assets and the safety of students.

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 design of a highly available hierarchical network has been proven and tested for many years and allow applications to converge on an intelligent and resilient infrastructure.

Figure 5 shows the main components of the Cisco Physical Security solution, including video surveillance, physical access control, incident response and integration with third-party systems.

Figure 5 Cisco Physical Security Components



Some of 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 alarms 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 solution. 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 for analog cameras. 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 subsections describe the components used for this solution.

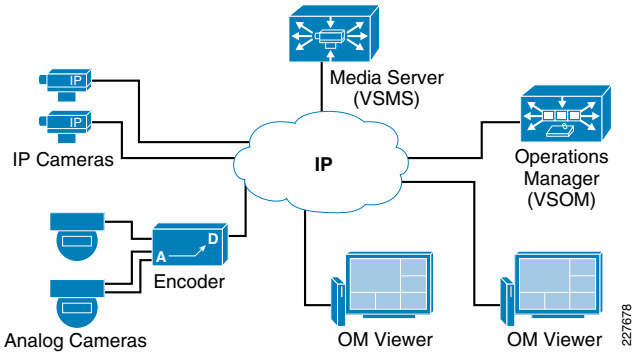
Cisco Video Surveillance Media Server

The Cisco Video Surveillance Media Server (VSMS) is the core component in the Cisco Video Surveillance Manager solution 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

In Figure 6, the Media Server is responsible for receiving video streams from different IP cameras and encoders and replicating them as necessary to different viewers.

Figure 6 Video Surveillance Media Server (VSMS)



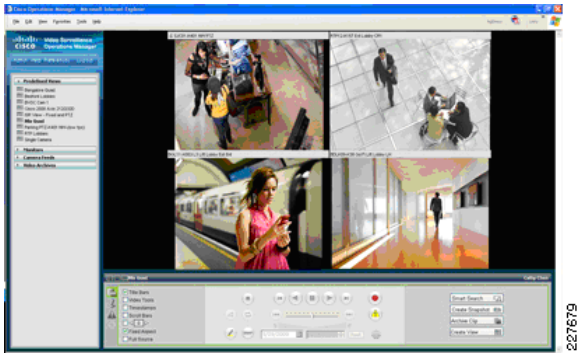
By using the power and advanced capabilities of today's IP networks, the Media Server software allows third-party applications, additional users, cameras, and storage to be added over time. This system flexibility and scalability supports the following:

- 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 7 shows the Operations Manager main screen, which is accessed through a web browser.

Figure 7 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 resolution standard-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 8 shows both the wired and wireless models of the 2500 IP Camera.

Figure 8 Cisco 2500 Series IP Cameras

The 2500 Series IP camera provides the following features:

- 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 1X2 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 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 IP Camera series also supports contact closure and two-way audio 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.

Figure 9 shows a Cisco 4000 IP Camera with an optional DC Auto Iris Lens.

Figure 9 Cisco 4000 Series IP Camera

The 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 interlaced 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 infrared (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 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 enables schools to use their network as an intelligent platform for effective, collaborative, scalable, and secure communications to better run the school system.

By integrating the systems with an intelligent IT infrastructure, the network is transformed into 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.

In this solution, the Cisco Unified Communications system offers a method for providing audio and text notification of alerts and can provide information customized for the specific alert. For example, if a fire alarm is triggered in the school gym, an audio and text message could be transmitted to all the IP phones and other IP enabled communications devices (such as IP-based speakers) with the following message "*A fire has been detected in the gym. Please exit the building through the main entrance*". If an intruder is detected after hours, audio and text messages such as *"an intruder has been detected in the north hall*" could be sent to all phones associated with security.

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, etc.), either Unified Messaging or voice mail, and WebEx.

The following sections describe the components used in this solution.

Cisco Unified Communications Manager

The Cisco Unified Communications Manager Express (CCME) integrates a core set of key system and small PBX functionality with a wide variety of rich IOS voice features inside the Cisco multiservice and integrated services routers. By converging voice and data into a single platform, CCME streamlines operations and lowers network costs, while increasing productivity.

CCME is optionally available on the Cisco 1861, 2800, 3800 Series ISRs, or the IAD 2430 to customers with 240 or less users. Whether deployed through a service provider's managed services offering or implemented directly by the end customer, CCME provides an intuitive graphical user interface for easy moves, adds, and changes; internetworking with Cisco Unified Communications Manager; and a number of advanced features not available on traditional telephony solutions.

The Cisco Unified Communications Manager, deployable on the Cisco 7800 Series Media Convergence Servers or on third-party servers by HP or IBM, includes 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 Unified Communication Manager Express

The first of its kind, the Cisco Unified Communications Manager Express (CCME) integrates a core set of key system and small PBX functionality with a wide variety of rich IOS voice features inside the Cisco multiservice and integrated services routers. By converging voice and data into a single platform, CCME streamlines operations and lowers network costs, while increasing productivity.

CCME is optionally available to any customer with 240 users or less who owns or is looking to purchase Cisco 2800 and 3800 Integrated Services Routers or the IAD 2430 and Cisco 1861. Whether deployed through a Service Provider's Managed Services offering or implemented directly by the end customer, CCME provides an intuitive graphical user interface for easy moves, adds and changes; internetworking with Cisco Unified Communications Manager; and a number of advanced features not available on traditional telephony solutions.

CCME provides the following features:

- A cost-effective IP telephony offering that can be easily added to a service provider's existing voice and data managed service for small-and-medium business (SMB) customers with telephony needs of up to 240 phones.
- A converged solution for voice, data and IP telephony services on a single Cisco integrated services or multiservices router.
- Interoperability with Cisco Unified Communications Manager (H.323 or SIP trunking).
- Special features for small businesses (i.e. internal paging, basic automatic call distribution, intercom, customer-relationship management integration).
- Application support for Cisco IP Communicator soft phone and Cisco Unified Video Advantage for video telephony.
- A cost-effective telephony solution for industries like retail and financial services, where customers have numerous, independent sites.
- Multiple Voice Mail integration options with localized Unity Express or centralized Cisco Unity.
- Support for XML services via Cisco Unified IP Phones, which provide users access to a wealth of information right at their desktop.
- A risk-free protected initial investment in Cisco IP Telephony for customers migrating to a Cisco Unified Communications Manager and Cisco Unified Survivable Remote Site Telephony (SRST) deployment.

Phones

Cisco provides a complete range of next-generation communications devices that take full advantage of the power of the data network while providing a convenient and easy-to-use system. The Cisco Unified IP phones can enhance productivity and address the needs of entire organizations.

Simple-to-use and fully featured, the Cisco Unified IP phones provide an enhanced user interface with display-based access to features, productivity-enhancing applications, and value-added services. This portfolio of robust next-generation devices includes the industry's first Gigabit Ethernet IP phone.

Cisco offers a comprehensive portfolio of IP phones. With their distinctive look, the phones provide a unique, positive communications experience. Their advanced unified communications services and applications are available only with an exclusively IP solution.

Easy-to-use display:

- Information display is graphical.
- Symbols are internationalized and easy to understand.
- Operation is intuitive.
- A user guide is built-in.
- Softkeys are dynamic.
- Color touch screens are user-friendly.

Modern style:

- The design is modern.
- The handset is comfortable.
- A unique ringing and message indicator is built into the handset.

Ease in adding new features:

- XML enables users to add unique new features and access time-saving applications quickly and easily.

Increased accessibility:

- The large LCD screen provides a visual display of what is happening on the phone.
- The LCD screen color provides high contrast and backlighting.
- The speakerphone can connect to external speakers for increased audio output.
- The phone is hearing-aid compatible.
- Audible and visual alerts give the phone status (audible tone during mute activation).
- The Cisco Unified IP phone portfolio offers a range of choices based on needs, preferences, budget, and use.

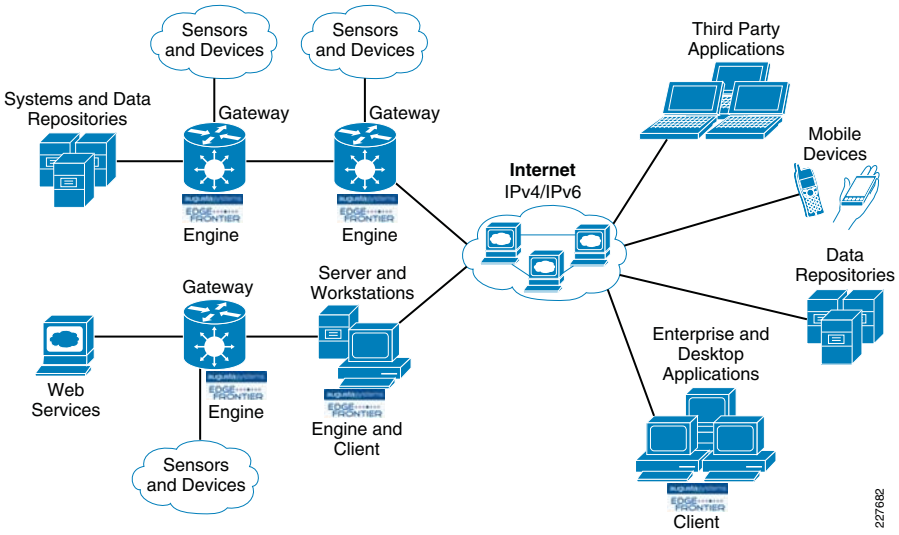
Partner Products

Augusta EdgeFrontier

Augusta EdgeFrontier is a remotely configurable middleware that resides on a server or servers providing a complete platform for intelligent convergence solutions. Augusta EdgeFrontier is a drop-in software solution that supports the convergence of devices, systems, and networks where robust network infrastructure exists.

Augusta EdgeFrontier supports the integration and normalization of data, events, and control functions from diverse sources, regardless of manufacturer or communications protocol, including devices and systems utilized in safety and security, energy and utilities, asset tracking, and other applications. In addition, Augusta EdgeFrontier provides structures for event processing and configuration of event or policy-based actions through a policy engine. See Figure 10.

Figure 10 Augusta EdgeFrontier Converged Network



Augusta EdgeFrontier is made up of an Augusta EdgeFrontier Engine application, which provides the field-level power for the software, and an Augusta EdgeFrontier Client application, which enables customers to configure/support the Augusta EdgeFrontier Engine application remotely.

Augusta EdgeFrontier can distribute data to and exercise control over multiple network devices and applications via various communication protocols within wired and wireless deployments including WiFi, WiFi mesh, WiMax, ZigBee, and others. In addition, third-party processing software and algorithms or user-produced code can be implemented easily to further extend the capabilities of Augusta EdgeFrontier as a middleware platform technology for convergence.

Specifically, Augusta EdgeFrontier can:

- Enable connectivity between diverse devices, systems, and networks through communication methods (including TCP/IP, UDP, serial, HTTP, SNMP, WMI, message queue, and web services); support the reading and writing of files and databases; and enable connectivity to systems via third-party and custom application programming interfaces (APIs)
- Serve as a mediator between diverse systems, devices, and networks, including support for protocol/format encoding/decoding and data transformation
- Provide real-time, edge-of-network event processing, including data filtering, correlation, anomaly detection, and notification/alert generation
- Provide a policy engine for configuration of event or policy-based actions
- Enable distributed processing and event or policy-based actions to be automated throughout the network infrastructure
- Provide an extensible application server for core and edge-of-network computing systems, including routers, servers, gateways, and other computing platforms
- Provide sophisticated network and system management capabilities
- Distribute data as network data, data files (e.g., text, Excel, XML, binary, etc.) and for databases (e.g., Microsoft SQL Server, Oracle, MySQL, etc.) for use with enterprise systems and interface platforms
- Extend the IP network and IT infrastructure to remote devices, systems, and networks

Singlewire InformaCast

Notification to Cisco Unified Communications phones and IP-based speakers was accomplished using Singlewire InformaCast IP Broadcasting solution from Singlewire. Singlewire InformaCast is a server or Cisco AXP-based application that can be used to simultaneously send an audio stream and text messages to any combination of Cisco IP phones, Singlewire InformaCast-compliant IP speakers, and PCs. With the push of a single button on the phone or a single click from a PC, a user can send a live, recorded, or scheduled broadcast to one or more paging groups.

- Singlewire InformaCast has the following features/benefits:
- Create live, ad-hoc, or pre-recorded audio broadcasts and/or text broadcasts
- Create paging groups using a variety of flexible means
- Filter access to message types and recipient groups by user
- Schedule messages to be sent at a preset time or on a recurring basis
- Configure the frequency of message playback
- Administer broadcasts from a secure web interface or IP phone
- Broadcast multiple messages simultaneously to different paging groups
- Use pre and post tones to signal to users the beginning and end of messages
- Use the Whisper Page functionality to mix audio broadcasts with a conversation if a phone is in use, or choose for the broadcast to simply skip phones that are in use
- Integrate flexible IP speakers to provide an indoor or outdoor loudspeaker option
- Use the Bell Scheduler's calendar format for complex ringing environments such as schools; schedule passing bells for an entire school district and modify the bells as needed

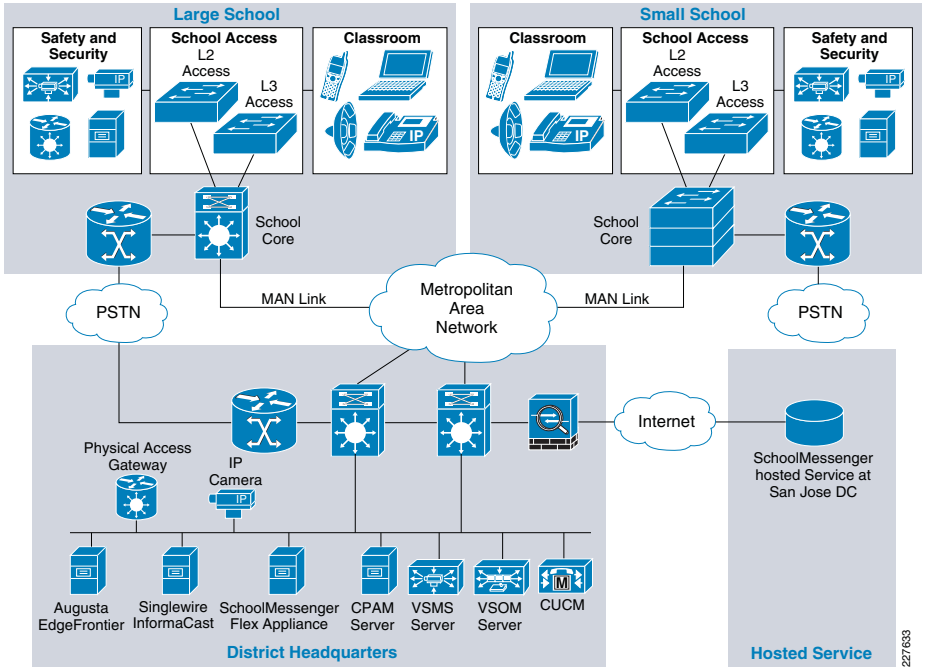
Typical uses:

- For every-day notification, the system can notify a coworker he/she has a call on Line 1 or tell the entire staff that E-mail is down.
- In emergency situations, the system can notify people onsite at the organization quickly and efficiently.
- Organizational notices—Give the district office the ability to send a message to the entire school district while a specific principle can only send to their school.
- Zoned paging—Page all of the teachers across the district.
- In an education environment, paging, bells, and clocks can be consolidated to a single server at the district office and integrate IP speakers with clocks at the schools.

Solution Framework

Figure 11 shows the location of the various components used in the Safety and Security for Education solution. The solution is based on the Service Ready Architecture (SRA) design and expands on the previously published Notifi-Ed solution. Figure 11 shows how each solution builds on top of the next, providing a complete solution architecture for safer educational environment.

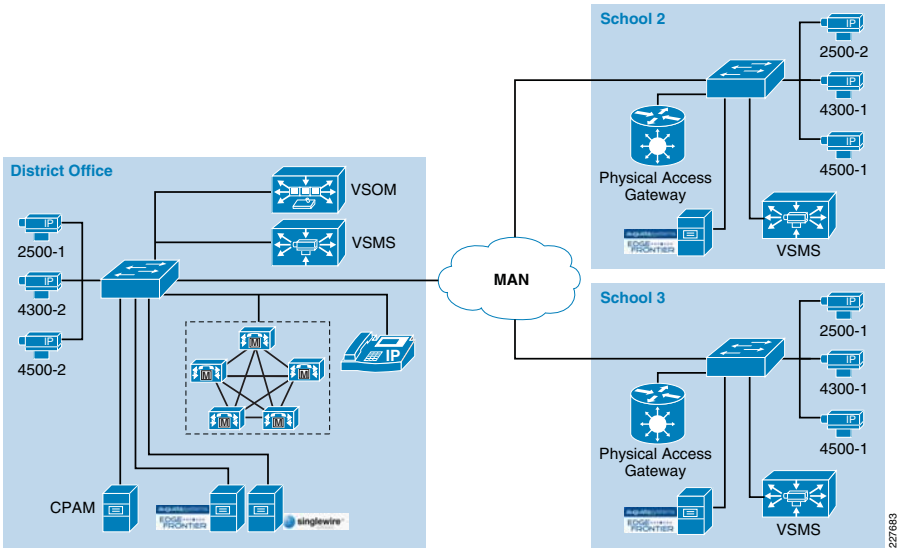
Figure 11 Safety and Security for Education—Based on SRA



Designing the Solution

There are multiple considerations that need to be addressed when designing a solution as large and integrated as Safety and Security for Education (see Figure 12). The components allow for a great deal of flexibility and scale, so selecting the appropriate products for the proper location is crucial. The design presented here attempts to show the various components and alternatives available based on size and scope of the customer environment. The ability to mix-and-match components and deployment options should give enough variety to meet most deployment needs.

Figure 12 District Office, School 2 and School 3 Lab Environments



With this type of deployment, it is assumed that the district office contains the data center environment, and has the staff necessary to support the technology. Scope dictates the components used.

For the Cisco Communications Manager, it is assumed that a CUCM cluster resides in the data center environment and is used for all phones in the district. To provide phone service in the case of a WAN outage, each school location would have a 2800 or 3800 series ISR to provide voice gateway and Survivable Remote Site Telephony (SRST) functions.

A single Video Surveillance Operations Manager (VSOM) server would be used in the district office. This server would be used to manage the Video Surveillance Media Servers (VSMS) used at each school. By placing a VSMS server at each location, bandwidth requirements are minimized to support multiple remote cameras, but still provide a centralized management capability and the ability to view remote video feeds. These feeds would also be available by any device on the network (assuming proper credentials) so that video can be viewed locally as well.

Cisco Physical Access Manager (CPAM) is the server side management tool for Cisco Physical Access control. This is located at the district office to provide a centralized management tool that can be used to control all of the Physical Access Gateways in the district.

Augusta EdgeFrontier servers are placed at each site. This allows for a centralized correlation point at each site, which can be used to enhance network security and minimize bandwidth requirements on the WAN.

Singlewire InformaCast is placed in the district office to handle all of the notifications for the district. Centralizing the Singlewire InformaCast server when managing schedules, notifications and CUCM interaction is one of the benefits of the product. However, schools without a backup MAN connection need to install a local copy of the Singlewire InformaCast application. Refer to the "High Availability" section on page -16 for details.

For the test environment used, the district office included the following components:

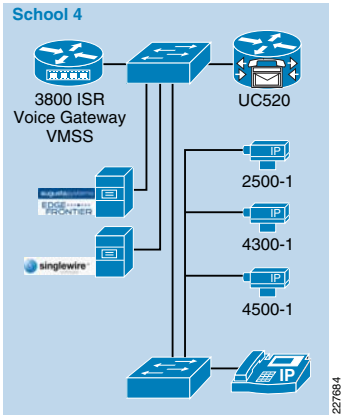
- Centralized Cisco Video Surveillance Operations Manager (VSOM)—A single VSOM server was used to manage all of the media servers in the configuration
- Cisco Video Surveillance Media Server (VSMS) to store video from cameras located at the district office
- Cisco Physical Access Manager (CPAM) used to manage/monitor all of the physical access gateways
- Cisco Physical Access Gateways—Used at each door, window, etc being monitored or requiring controlled access
- Cisco Unified Communications Manager (CUCM)—CUCM cluster centralized for the entire school district
- Singlewire InformaCast server—Used to provide paging and notifications for the entire district
- Augusta EdgeFrontier server—Used to correlate notifications from the various cameras and sensors and to automate notifications to VSOM and CPAM
- IP phones, IP speakers and IP cameras—Used for notifications and video surveillance

School 2 (and subsequent schools) included the following components:

- Cisco VSMS to store video from cameras located locally at each location
- Cisco Physical Access Gateways—Used at each door, window, etc being monitored or requiring controlled access
- Cisco ISR—Used for SRST functions as well as PSTN access for the location.
- Augusta EdgeFrontier server—Used to correlate notifications from the various cameras and sensors and to automate notifications to VSOM and CPAM
- IP phones, IP speakers and IP cameras—Used for notifications and video surveillance

There may come a time where deploying a full video surveillance solution with multiple servers, hundreds of camera and the supporting infrastructure is just not necessary. For the environment listed as School 4 shown Figure 13, the design focuses on delivering a fully-integrated solution at a standalone site.

Figure 13 School 4 Lab Environment



In this design, the choice of components used is the biggest difference. For example, instead of deploying multiple servers to support the VSOM and VSMS, the testing was performed with a VMSS module in a 3800 ISR and included the ISS module, which provides an additional 500Gb of storage. The software on the VMSS module is the same version/release as that used on the VSOM/VSMS, but in a smaller, easier to manage package. Same functions exist, the biggest difference being the number of cameras that are supported. There is an option for 16 or 32 cameras supported by the VMSS module. If more cameras are necessary, it will be necessary to deploy the server strategy in the district office/remote school scenario.

Another change in this design is the use of the Cisco Unified Communications 500 device. This device is based on CCME, and could be used in the design instead of CUCM. Additionally, a 3800 ISR with SRST functionality also provides the option of deploying Cisco Unified CME on the ISR while providing the same level of functionality.

In this design, the need for servers still exists, but the size and horsepower of those servers is not as great as in an enterprise deployment. For testing purposes, the Singlewire InformaCast server and Augusta EdgeFrontier servers were both installed on a VM guest machine running on a single Cisco MCS 7835 server. The memory and processing requirements are minimal, so this posed no problems from a performance perspective. Additionally, the Singlewire InformaCast server is available to be deployed on a Cisco AXP blade in the 3800 ISR, so if there is an open NME slot, this is a reasonable alternative.

The Cisco Physical Access Control was not tested in the isolated scenario, but the design and deployment considerations would be the same as for the district office and remote school environment.

For the test environment used, the standalone environment known as School 4 (see Figure 13 above) included the following components:

- Cisco 3845 ISR
- Cisco VMSS enhanced network module (integrated VSOM and VSMS)
- Cisco ISS enhanced network module (additional storage for VMSS)
- Cisco UC500 CME device
- Augusta EdgeFrontier server
- Singlewire InformaCast server

- IP Phones and IP Cameras

Cisco Physical Access Control

The Cisco Physical Access Control solution benefits from a distributed architecture while lowering deployment and operational costs. For this application deployment guide, the Cisco Physical Access Gateways are placed at each school. CPAM is centrally located at the district office and is able to manage thousands of gateways installed at the schools. Through CPAM, a user can configure the policy for each access gateway at each school. For example, the entrance door to the school will remain locked during school hours from 8:00am to 3:30pm, while a door to a building may be unlocked during class break.

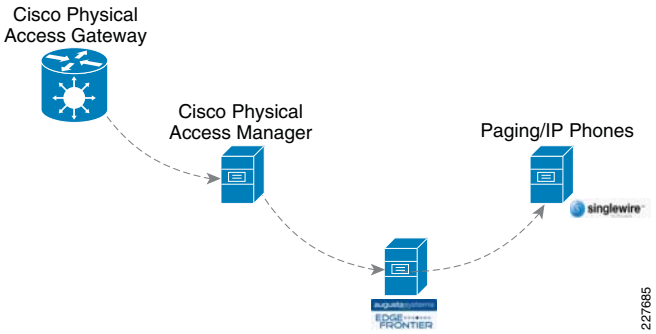
Time Synchronization

The Network Time Protocol (NTP) is widely used to synchronize clocks of viewers, application server, routers and other network elements with a reliable time source. The Cisco Physical Access Manager relies on NTP to synchronize the time of the server and all of the gateways. When the server and gateways are not synchronized properly, issues occur, such as corruption of the keys passed between the systems.

CPAM and Augusta EdgeFrontier

For emergency situations, such as a forced entry, CPAM will send an HTTP request to the Augusta EdgeFrontier application. The Augusta EdgeFrontier application will trigger notification to security officers and instruct VSOM to archive videos before and after the incidents. This application deployment guide focuses on two types of incidents: forced entry and theft. Figure 14 shows the interaction between CPAM and Augusta EdgeFrontier.

Figure 14 Interaction between CPAM and Augusta EdgeFrontier



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

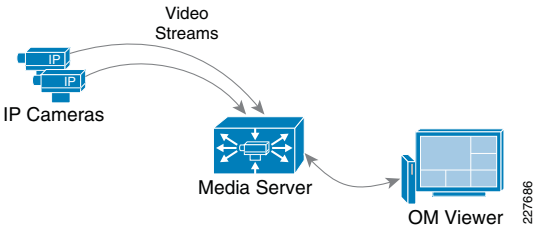
Cisco Video Surveillance

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 15 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 15 Media Server



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

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

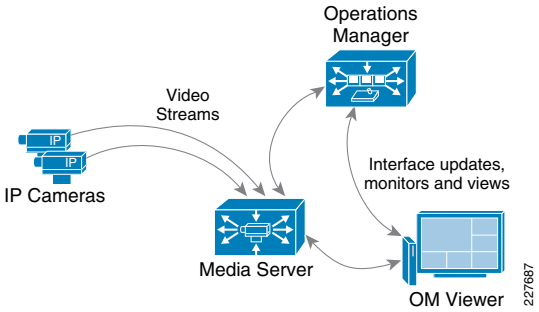
Video requests and video streams are delivered to the viewer using HTTP traffic (TCP port 80).

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. Once 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 16 shows the traffic flow of video requested by a viewer.

Figure 16 Operations Manager Traffic Flows



Once 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.

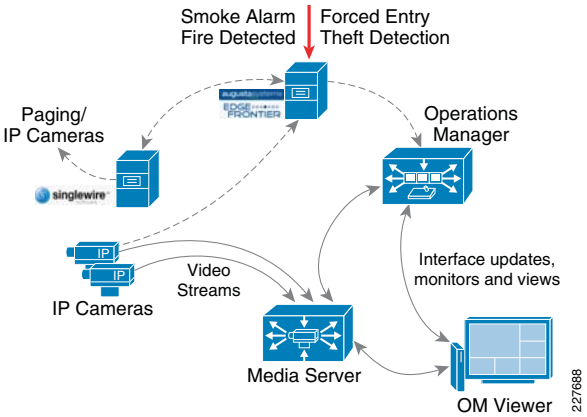
The Media Server acts as a proxy between the camera and the viewer, which receives video feeds over TCP port 80 (HTTP). If another OM Viewer requests the video from the same IP Camera, the Media Server simply replicates the video stream as requested, and no additional requests are made to the camera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

Augusta EdgeFrontier Notifications to VSOM

For the integration with VSOM, this deployment guide relied on the soft trigger mechanism of the VSOM server. This is simply a GET call to the VSOM server from the Augusta EdgeFrontier server with the properly-formatted URL that is defined when a trigger is created. The only difference between triggers is the ID number. The soft trigger needs to be created in VSOM before an Augusta server can initiate the request.

Once the trigger is called, additional functions are performed based upon the setup of the trigger itself. Use cases defined for this solution include the marking of the video from N seconds before the incident until Y seconds after the incident, and how long to keep the video. Additional configuration options include adding the incident to the event list in VSOM and provide a notification on the VSOM Operations view that an incident has occurred. See Figure 17.

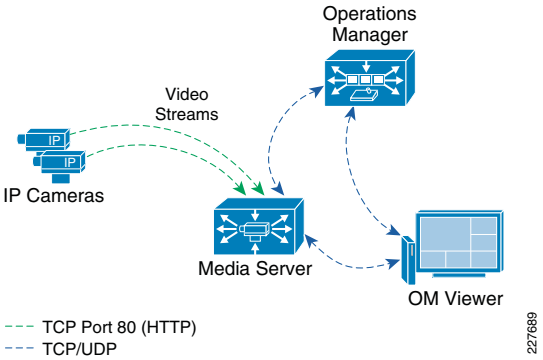
Figure 17 Augusta EdgeFrontier Notifications



Required TCP/UDP Ports

The example in Figure 18 shows that the communication between the Media Server and viewers relies on TCP port 80 (HTTP) while the communication between edge devices and the Media Server may vary, depending on the camera manufacturer.

Figure 18 Required TCP/UDP Ports

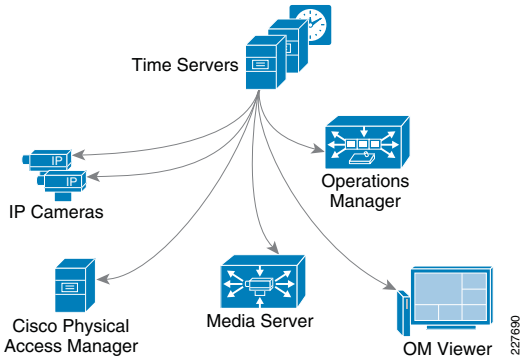


In order to allow video streams to flow between the Media Server, edge devices and viewers, the proper security must be in place to allow TCP/UDP ports to traverse the different subnets or locations.

Time Synchronization

The Network Time Protocol (NTP) is widely used to synchronize clocks of viewers, application servers, routers and other network elements with a reliable time source. The Cisco Video Surveillance Manager solution relies on NTP to synchronize the time of all its applications and viewers. Clock synchronization is critical when retrieving previously recorded video streams. Figure 19 shows how the NTP servers propagate the current time to IP cameras, viewers and application servers.

Figure 19 Network Time Protocol (NTP)



The application servers and viewer's workstations should be configured to receive time from an NTP server.

Note NTP servers keep time in Universal Time (UTC), and each device on the network is configured for the proper geographical time zone. The conversion to the proper local-time is handled by the operation system on each device.

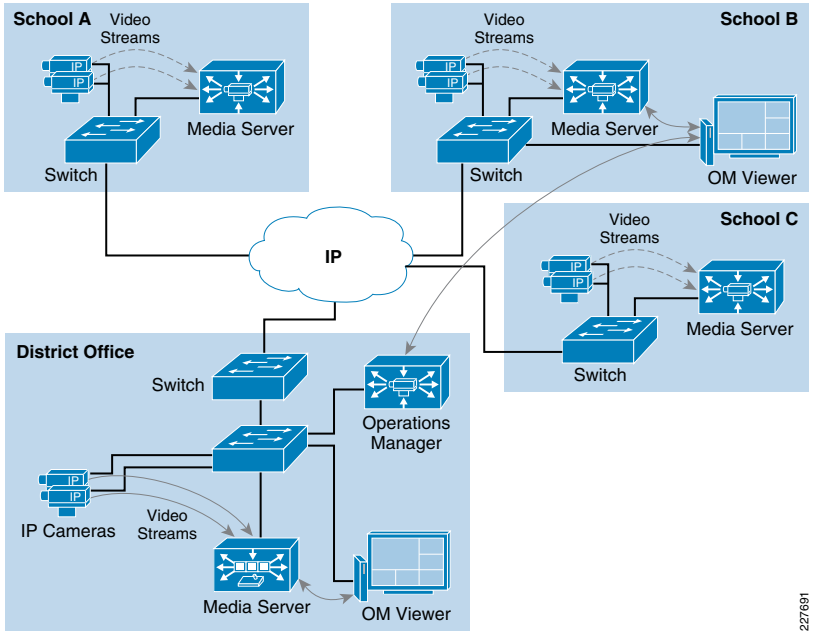
Distributed Media Servers

Figure 20 shows a deployment with several remote schools, 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 Monitors (video walls) at the headquarters.

In the case of School B, a viewer is installed locally in order to view cameras from the local school. The viewer at School B contacts the Operations Manager for a list of allowed resources (camera feeds/views/archives) and contacts the local Media Server in order to view local cameras. The traffic remains local to the site, unless the viewer selects video from camera feeds at different schools.

Note A single Operations Manager is able to manage resources at all schools.

Figure 20 Media Servers at Each School



The Media Server at the headquarters could 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 since the traffic would be contained locally in the headquarters LAN.

Cisco 2500 and 4000 Series Cameras

One of the things necessary to consider in the implementation of this solution is the identification of the location of the incident. This was done in multiple ways, using the Augusta EdgeFrontier server as the correlation engine. For camera integration, and motion detection, the camera was used to help identify the location of the camera as well as provide some necessary information for the Augusta server to create the proper notifications. However, not all cameras are created equal. As a result, several different mechanisms were used in this solution.

Cisco 2500 Series Camera

The Cisco 2500 camera has basic communication functionality in the case of an event, which includes FTP and Mail. For this solution, the FTP service was used to connect to the Augusta EdgeFrontier server when an event occurs. Since the Augusta EdgeFrontier server does not support FTP, data could not be moved using full FTP protocols with the server. Rather, data transfer relies on a connection and port established between the camera and the server. Once that connection is established, the Augusta EdgeFrontier server can identify the IP address of the connecting server, and subsequent actions are based on this information.

Additionally, the 2500 camera allows for a schedule in which the notification should or should not occur. This is used as a base functionality to prevent false positives (i.e., motion detected in the hallway during normal school hours should not send a notification).

Cisco 4000 Series Camera

The Cisco 4000 Series camera has similar capabilities as the 2500 Series including the schedule for event notification, but includes one additional function that proved to be useful in this solution. The 4500 includes HTTP notification, and when triggered, performs an HTTP Post function with specific information from the camera itself. The information is in XML format as shown below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<DeviceInfo>
    <version>0.0.1</version>
    <EventNotificationAlert>
        <deviceID>1</deviceID>
        <deviceName>Back Hall Camera</deviceName>
        <ipAddress>192.168.32.52</ipAddress>
        <macAddress>00:1E:BD:FC:19:4B</macAddress>
        <dateTime>08242009 11:52:19</dateTime>
        <activePostCount>1</activePostCount>
        <eventType>2</eventType>
        <eventState>1</eventState>
        <eventDescription></eventDescription>
        <DetectionRegionList><DetectionRegionEntry>
        <regionIndex>1</regionIndex>
        <sensitivityLevel>50</sensitivityLevel>
        <detectionThreshold>50</detectionThreshold>
            </DetectionRegionEntry>
            </DetectionRegionList>
    </EventNotificationAlert>
</DeviceInfo>
```

Knowing where this information comes from and how it is valued provides a mechanism to identify the camera within the event itself. As a result, the *devideID* was correlated with the soft trigger ID in VSOM. The *deviceName* provides a way to include the location of the notification in the Singlewire InformaCast message that is dynamically built when a notification occurs. The *dateTime* of the event is used in the notification as well, which is useful in locating the incident on the video surveillance playback system.

Cisco Unified Communications

In this solution, Cisco Unified Communications is used to provide audio and text notification of alerts and can provide information customized for the specific alert. There is a complete set of APIs and communications mechanisms between Cisco Unified Communication Manager and third-party applications for device monitoring, call control, provisioning, and serviceability. In this solution, Singlewire InformaCast communicates with the Cisco Unified Communications System. Communications occur between Singlewire InformaCast and the Cisco Call Control platform (CUCM, CUCME or UC500) and directly between Singlewire InformaCast and the phones. Singlewire InformaCast uses the Computer Telephony Interface – Java Telephony Application Provider (CTI-JTAPI), Administrative XML (AXL), and SNMP to communicate with CUCM and XML and RTP to communicate with the phones. In addition to the standard basic configuration, the latest Cisco JTAPI library must be installed on the Singlewire InformaCast Server. This process, as well as the configuration of the call control platforms for all supported versions, is well documented in the Singlewire InformaCast documentation that can be found at the following URL:

http://www.singlewire.com/pdf/InformaCastCME-7.0.pdf

Required TCP/UDP Ports

As with any Cisco Unified Communications deployment, refer to the documentation on the ports required for the particular version of the software being deployed to ensure the network is ready. Ports used specifically for communications between CUCM 7.0 and Singlewire InformaCast 7.0 are 161 for SNMP, TCP 2748 for CTI, and 443 for encrypted communications. Traffic observed between Singlewire InformaCast and the phones include TCP ports 80 and 8081 for phone control. These ports may vary with different versions of code.

IP Multicast

Since IP multicast is used to transport the audio traffic from the Singlewire InformaCast server to the phones, the network should be able to support multicast protocols.

IP Phones

This solution relies on the phones to deliver the audio alert and their text display to provide a text alert. Singlewire InformaCast has the ability to include a graphic display in the alarm. All of the Cisco 7900 series IP phones support the audio playback, XML, and text display. If graphics are desired, some of the lower-end phones have limited or low graphic capabilities. There are no other phone considerations required for this solution.

Other Considerations

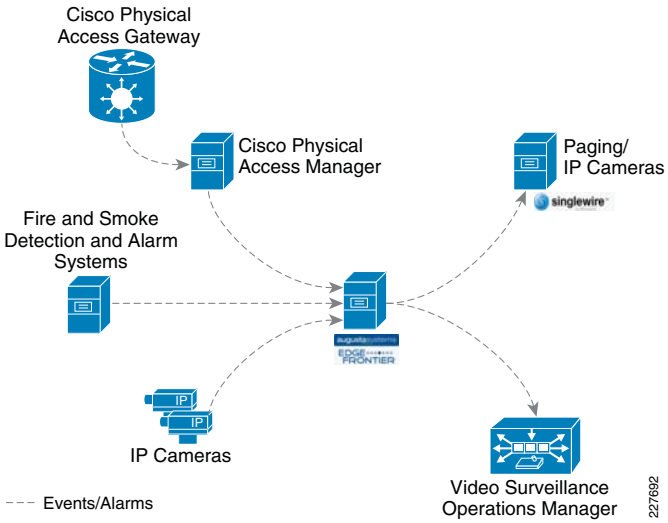
Augusta EdgeFrontier Server

The Augusta EdgeFrontier server has various mechanisms that can be used to communicate with other servers, applications, and systems, such as a web method, HTTP call, or TCP requests. EdgeFrontier is also able to start other applications on command.

By correlating the notifications through the Augusta EdgeFrontier server, the devices have the same connection properties, making support easier for similar device types, provide a greater deal of flexibility, and build in additional security if necessary. This also allows for a single incident to generate multiple responses, rather than configuring a single device to talk to multiple services.

Figure 21 illustrates the correlation capabilities in Augusta for this solution.

Figure 21 Augusta EdgeFrontier Location in the Solution



Augusta EdgeFrontier Notifications to Singlewire InformaCast

The basic functionality of the Singlewire InformaCast server is to provide audio and text messages to a variety of devices. The easy way to deal with this is to create a message for each possible incident that needed to be reported and call that message from each sensor or camera. Although it may be easy from a flow perspective, it is not so easy to setup or maintain. In this solution, a web method supplied by Singlewire was used. This is similar to initiating a message via the web interface or calling a message using an HTTP post, but instead, it can be called remotely and pass parameters and custom messages based on the incident being reported.

The web method, offers the capability of including various pieces of information in real-time in the messages sent by the Singlewire InformaCast server. The following parameters are available in the **sendMessageWithDynamicText** web method:

- *messageId*—Shell message defined in the Singlewire InformaCast system. The shell message determines if message is text, audio or combined audio / text message
- *shortText*—Short text message initially displayed on the phone
- *detailText*—Additional information included in message accessed using the "MORE" softkey
- *recipientGroupIds*—Recipient group ID configured in Singlewire InformaCast used to determine the distribution list for the messages
- *userLogin*—Login used to access the Singlewire InformaCast server application
- *userPassword*—Password used to access the Singlewire InformaCast server application

By using a dynamic text mechanism, messages may be built dynamically based on the incident being reported. The Augusta EdgeFrontier server can correlate the information from the device, build the message, and initiate the connection to the Singlewire InformaCast server when the incident occurs. Some of this information comes from the camera or sensor itself, other information is coded in the Augusta EdgeFrontier server.

Video Feeds and Archives

There are numerous ways to create archives for any number of reasons. The real challenge is to identify the need for the archive before actually creating them. Depending on the storage location, camera location, etc. multiple feeds or unnecessary high resolution video results in increased bandwidth, unnecessary archives result in increased storage requirements, etc. Understanding what needs to be retained, for what reason it will be used, and for how long will go a long way in identifying the archive strategy and the storage requirements.

The following is an example strategy:

- Primary cameras or public area cameras have an active archive loop that is kept for a short period of time. The purpose of this archive would be to have a record of an event not otherwise captured, (i.e., if a parent calls to say that their son/daughter was injured in the parking lot, you would not necessarily have a record of that event). If you have a general archive, you can go back to the approximate time the event happened and review the scenario.
- Use triggers for specific incidents. Triggers allow you to capture video for a period of time before and after the incident occurred. This is helpful when doing video forensics to see what type of actions occurred leading up to the incident and the subsequent actions of those involved. These archives would likely be kept for an extended period of time, and an extended default can get set when the archive is created.
- Create an archive clip to maintain a historical record of an incident. An archive clip can be created and stored on the VSMS server or on a local hard drive. When a clip is created, a passcode for that clip may be provided. The passcode is required to play video stream, and if the video has been tampered with, the video will not play. This provides an extra layer of security for high-risk incidents. Additionally, the video player can be bundled with the video clip for extended playback requirements.

Another option could be to use multiple streams on the cameras. A standard definition feed could be used for a general-purpose archive to minimize storage, and a high-definition feed for a trigger archive to allow for a higher quality image. However, the 4000 Series camera is not able to dual-stream with a primary feed configured at 1080P, requiring to limit the primary feed to 720P. If the requirements demand a high-resolution image, using a dual-stream is likely not an acceptable configuration.

High Availability

While a mission critical application requires maximum availability, many applications require only fast detection of failure and fast recovery. The Physical Safety for Schools solution provides high availability (HA) suitable for schools and yet keep cost down.

Key considerations include the following:

- A distributed architecture enables an economical implementation of high availability by placing expensive resources at a central site and sharing them with other sites. A backup MAN connection is typically required between a local site and the central site to allow the local site to continue using resources from the central site. Having a secondary link is not a problem for a university and its extension, or a community college and its smaller campuses. However, having a secondary connection may be challenging for K-12 schools since the government funding (e-rate) only covers a primary connection. Without a backup MAN connection, an Singlewire InformaCast application needs to be installed at each school site. A backup WAN usually has

smaller bandwidth than the primary WAN link. QoS is deployed to give higher priority to data from access gateway and voice/text notification from Singlewire InformaCast than video traffic.

- Consider if a resource is critical. For example, when CPAM in the district office is down, the Cisco Physical Access Gateway at each school continues to provide normal card access and will sound an alarm mounted near the door upon a force entry incident. The only function lost is the notification to the Augusta EdgeFrontier which in turn triggers the call to security officers and the archive of video surveillance near the entrance door. If this behavior is acceptable for the school environment, then a single copy of CPAM at the district office is sufficient.
- The cost of a device is also important when deciding whether to place it on a central location or at each site. For example, Augusta EdgeFrontier plays a critical role in this solution and it is inexpensive (can be installed on a virtual machine on a server running VMware). An Augusta EdgeFrontier was placed at each site. If a resource is critical but expensive, it can be placed at a central site and provide HA through redundant MAN connections.
- The size of a location also plays a role. If a university extension has only a couple of classrooms, a local copy of Augusta EdgeFrontier may not be necessary, since the forced entry alarm would be heard locally, including the security officer.

Baseline Architecture

For high availability design for the baseline architecture, refer to the "Building Resilient School Campus Network" section in the *School Service Ready Architecture Design Guide* (see the"Appendix A—Reference Documents" section on page -57 for reference).

Augusta EdgeFrontier

An Augusta EdgeFrontier server is located at each location. In this solution, the EgdeFrontier has the following three main functions:

1. It is the correlation engine. It collects information from all of the sensors, cameras, etc. at that location and sends alerts or other information based on the rules created for that event.
2. The Augusta EdgeFrontier can be configured in various ways to allow for HA. Consider the following examples:
   a. Augusta EdgeFrontier outbound—For example, if VSOM is down or not available because of a WAN outage, the Augusta EdgeFrontier server will attempt to send the message once. Alternatively, the Augusta EdgeFrontier could be configured to verify the path to the VSOM server prior to sending the message, thereby providing guaranteed message delivery. It could also be configured to evaluate the response and make a determination as to whether the server is available. If not, it can perform a store-and-forward type mechanism, waiting for the server to be available. The flexibility of the product makes it easy to configure it according to the needs of a deployment.
   b. Augusta EdgeFrontier inbound—For example, a sensor is trying to send a notification to the Augusta EdgeFrontier server and the server is not available. The message is likely lost for good. Again, understanding the requirements is key to the proper deployment. The Augusta EdgeFrontier server could be configured for hot-standby, with the same configuration, same IP address, etc, just waiting to be brought online if the primary fails. Take this one step further, and one Augusta EdgeFrontier server can monitor the other, and then bring the production server (in Augusta EdgeFrontier, the server is the physical configuration of the device) online in case of a failure.

      It is also possible to create a hierarchy of Augusta EdgeFrontier servers. A child server could attempt to send a notification to its parent server, and if not available, be configured to send its notification to an alternate server.

      For this solution, CPAM was configured to send an HTTP request to both the Augusta EdgeFrontier server at the school and the Augusta EdgeFrontier servers at the district office. Since both local Augusta EdgeFrontier and central Augusta EdgeFrontier have the same policy (upon receiving CPAM request, trigger Singlewire InformaCast), InformaCast will send out two copies of messages.
3. The Augusta EdgeFrontier application plays a star role in high availability by detecting device failure and triggering notification of such failure, such as a non-responding camera.

Video Surveillance

Cameras at each site are monitored by the Augusta EdgeFrontier server on the same site. When a camera stops responding, the Augusta EdgeFrontier application will trigger Singlewire InformaCast to send notification about the camera failure.

A media server is placed at each school in order to reduce the amount of traffic traversing the MAN. The media server can be configured to store video on a backup server in case the primary media server fails.

While VSOM does not currently support high availability features, it does not affect the key functionality of this application deployment guide. First, Augusta EdgeFrontier will monitor VSOM. If VSOM is not responding, Augusta EdgeFrontier will trigger Singlewire InformaCast to send notification about the VSOM failure. Second, Augusta EdgeFrontier queues a message, such as "*VSOM needs to archive the video from camera 1 in School 1 from 11pm to 11:06pm.*" Upon VSOM coming online, Augusta EdgeFrontier will retransmit this message. Since the media server at School 1 has the video stored typically for a week, it is not a problem that VSOM request the archive of a short video at the moment or some time later.

Physical Access Control

The CPAM server can have a redundant CPAM server in a Linux HA 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 alarm to be triggered on the gateway locally. However, today no other input alarms from the gateway, such as a glass break sensor or duress signal, can trigger the output alarm locally. It would require going back to the CPAM server to arbitrate. Release 1.2, scheduled by December 2009, will allow any input alarms to trigger the local output alarm using the device I/O rules similar to the door forced open example.

Notification

When triggered by the Augusta EdgeFrontier application, Singlewire InformaCast server will send notification to Cisco IP phones and IP-based speakers. If the MAN connection is down or the Cisco Unified Communication Manager (CUCM) in the district office is down, a school with an Singlewire InformaCast server can still send the notification. This is because CUCM is not required for Singlewire InformaCast to broadcast to IP phone(s). Even when a Singlewire InformaCast message is sent to a single phone, it still uses multicast. CUCM only comes into play when Singlewire InformaCast uses SNMP to find out what phones are there and when recording a message which can be done in advance.

The above is for notification through Singlewire InformaCast. For normal phone conversations, if the MAN connection is down or CUCM in the district office is down, an Integrated Service Router (ISR) at each school will offer Cisco Unified Survivable Remote Site Telephony (SRST).

Implementing and Configuring the Solution

This section is divided into four subsections, corresponding to the components of this solution. Configuration of each component is provided, but the focus is on how the components integrate as a whole. The following tips may accelerate the system implementation:

1. Decide what devices will be installed at a central site and what devices will be installed at other sites.
2. Decide what software/firmware version is required. A new device usually has a default IP address. It is easier to upgrade it to the decided version before you modify its IP address.
3. Decide whether to use DHCP or static IP address. Decide IP address scheme for the devices at each site.
4. If a device, such as a physical access gateway or an IP camera, uses static address, access its web interface through its current IP address and specify its new IP address before moving it to a new network.

Cisco Physical Access Control

The Cisco Physical Access Manager was installed at the district office and Cisco physical access gateway was installed at a school. Configuring CPAM and Cisco physical access gateway includes the following three steps.

1. Establish connection between CPAM and Cisco physical access gateway.
2. Configure door hardware and access policies.
3. Configure CPAM to send requests to Augusta EdgeFrontier.

Establishing Connection Between CPAM and Physical Access Gateway

When configuring physical access control, first configure the CPAM then configure the Physical Access Gateway. The same order also applies when performing software upgrades to these devices. Both devices can be configured through a secure web interface. First access CPAM through its default IP address https://192.168.1.2, then modify its IP address, as shown in Figure 22.

The physical access gateway has two Ethernet ports. The ETH0 port is used for network communication. The ETH1 port is used to connect a PC to the Gateway for configuration and monitoring. First access the physical access gateway through its ETH1 default IP address https://192.168.1.42.

Then modify the ETH0 IP address to the decided value. Finally, specify the IP address of CPAM so the physical access gateway and CPAM can establish connection. Figure 23 shows the IP address configuration on the physical access gateway. It also shows the specification of CPAM address.

Note Before moving physical access gateway or CPAM to a new network, first modify its IP address.

Figure 22 Configure IP address on CPAM

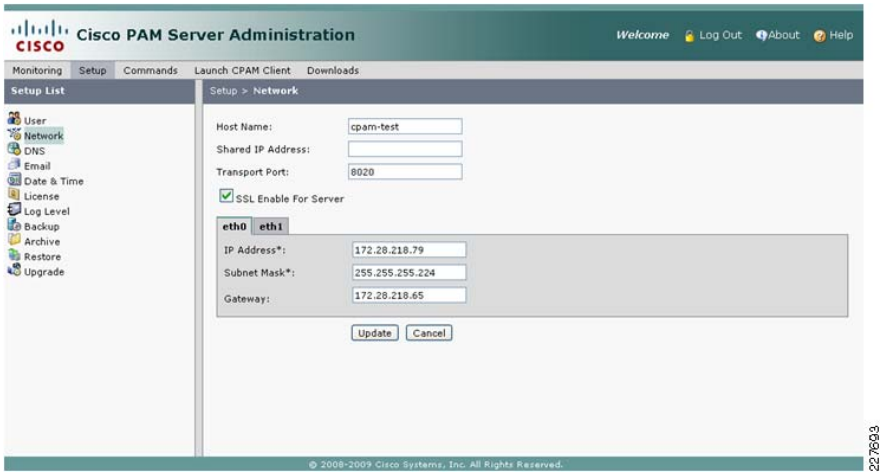
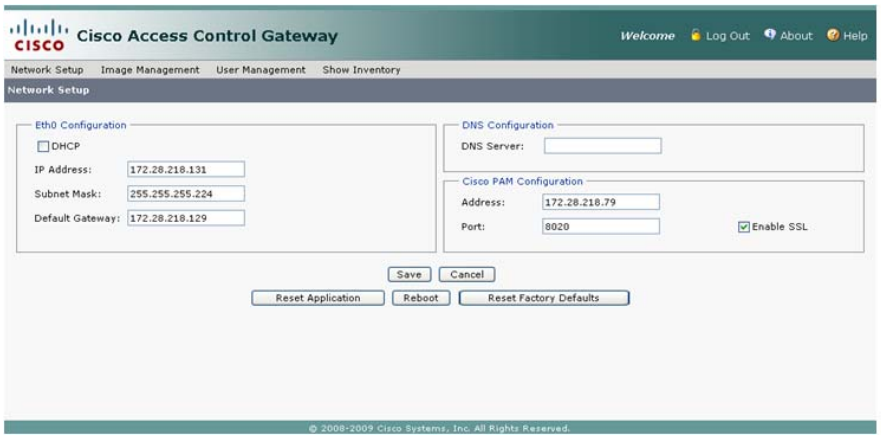


Figure 23 Configure the Physical Access Gateway

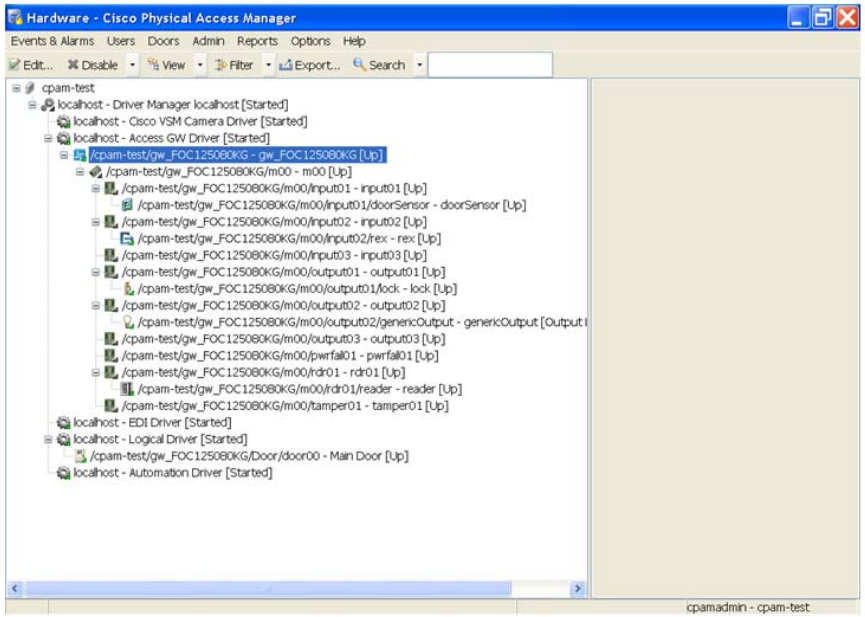


Configuring Door Hardware and Access Policies

Once CPAM and the physical access gateway establish connection, use the CPAM client software to configure door hardware and access policies for the physical access gateway. This enables convenient control and monitoring of many physical access gateways through one central interface.

1. Install CPAM client software on a laptop. Then launch CPAM client in one of these methods:
   a. From the web interface of CPAM, click **Launch CPAM** client.
   b. From the laptop, click **Start->All programs->Cisco Physical Access Manager**.
2. After launching CPAM client, click on **hardware**. The hardware window will appear. The physical access gateway should show up as a device under **localhost-Access GW Driver**, as highlighted in blue in Figure 24. If it does not show up, check the following:
   c. Whether the correct IP address of CPAM is specified in the physical access gateway configuration.
   d. Whether or not the physical access gateway and CPAM running the same version.

Figure 24 Hardware Window



1. Once the physical access gateway appears under localhost – Access GW Driver, first configure the door hardware (refer to Figure 24):

- A door sensor as input01
- Request for Exit (REX) as input02
- A lock as output01
- An alarm as output02
- a card reader as rdr01

2. Then configure access policies:
   a. If a valid card is presented to the card reader, lock will open.
   b. When pushing the REX button, lock will open.
   c. When the door sensor indicates door is open but it is due to neither valid card access nor REX, the alarm will be on.
3. Configuration of door hardware and access policies is documented in *Cisco Physical Access Manager User Guide* (see the "Appendix A—Reference Documents" section on page -57 for reference).

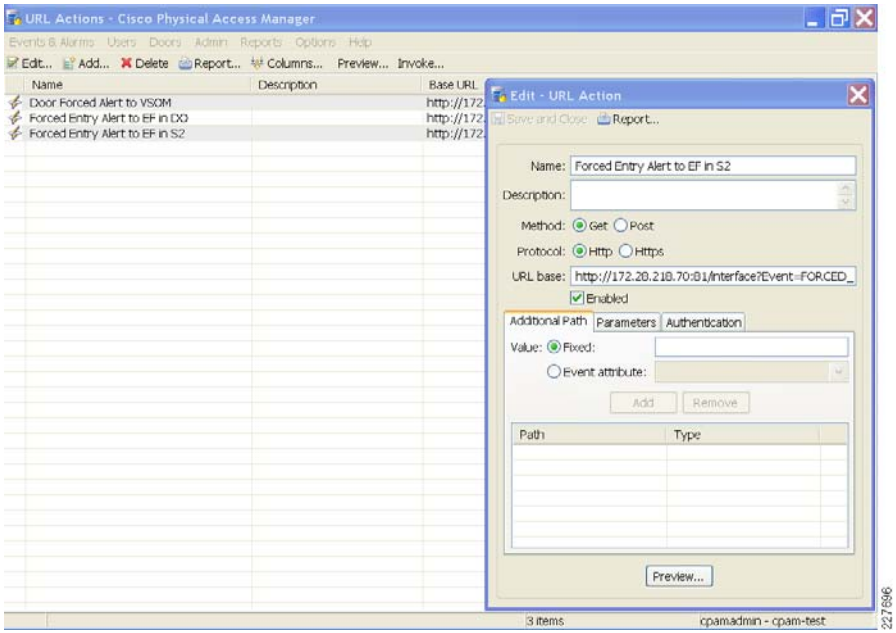
If during a power failure the doors require free egress, the locks used in that location should be configured as *fail-safe*. This means that power is required to keep the locking mechanism engaged.

Configure CPAM to Send Requests to Augusta EdgeFrontier

A physical access gateway can send HTTP requests directly to an Augusta EdgeFrontier server. The configuration includes configuring a URL action and associating an event to a URL action. Use the following steps to configure a URL action:

1. Launch CPAM client. Click **Admin** from the menu bar in CPAM client. From the drop down menu, select **URL Actions**.
2. The *URL Actions—Cisco Physical Access Manager* window opens. Click **Add** to add a URL action for forced entry incident. Figure 25 shows the configuration of a URL action. The IP address specified in URL base is the address of Augusta EdgeFrontier server.

Figure 25 URL Action

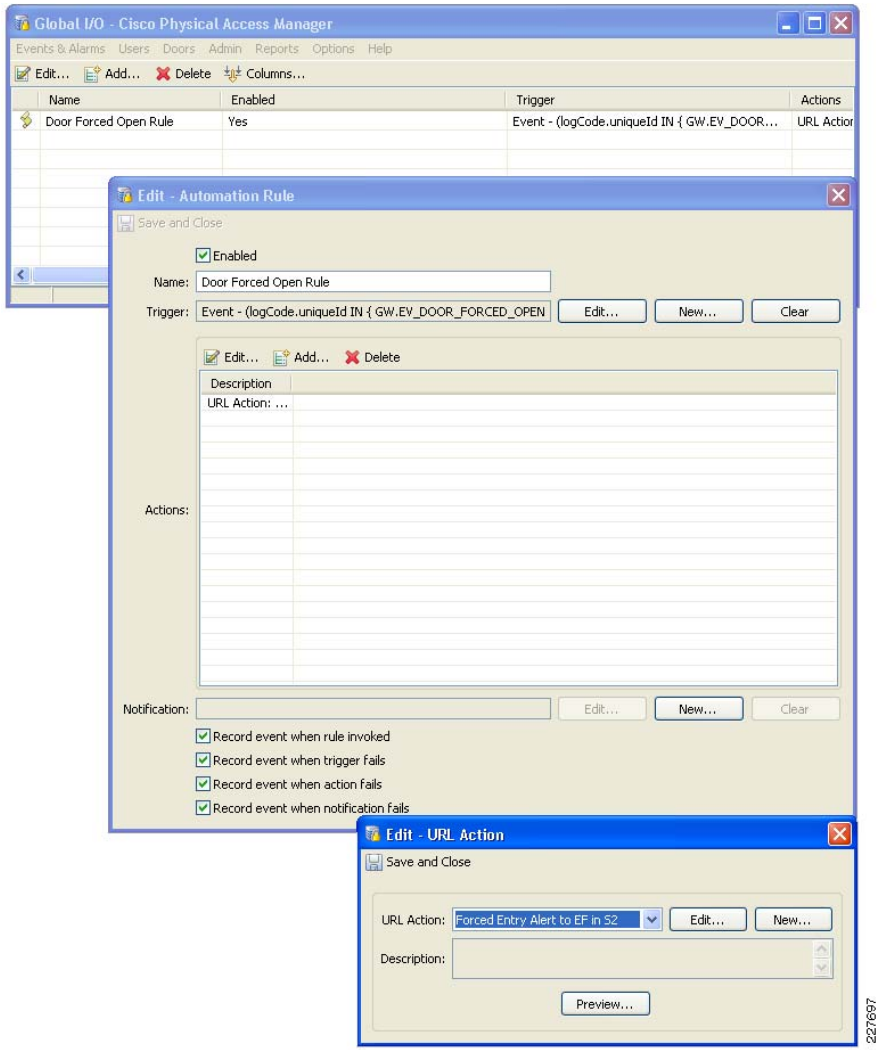


To associate an event to a URL action:

1. From CPAM client, click **Events & Alarms**. From the drop down menu, select **Global I/O**.
2. Click **Add** to associate the forced entry incident to the forced entry URL action. Figure 26 shows the association of a forced entry incident to the URL action.

To send multiple notifications for the same event, multiple URL actions may be configured and associate the same event to multiple URL actions.

Figure 26 Associate Forced Entry Incident to a URL Action



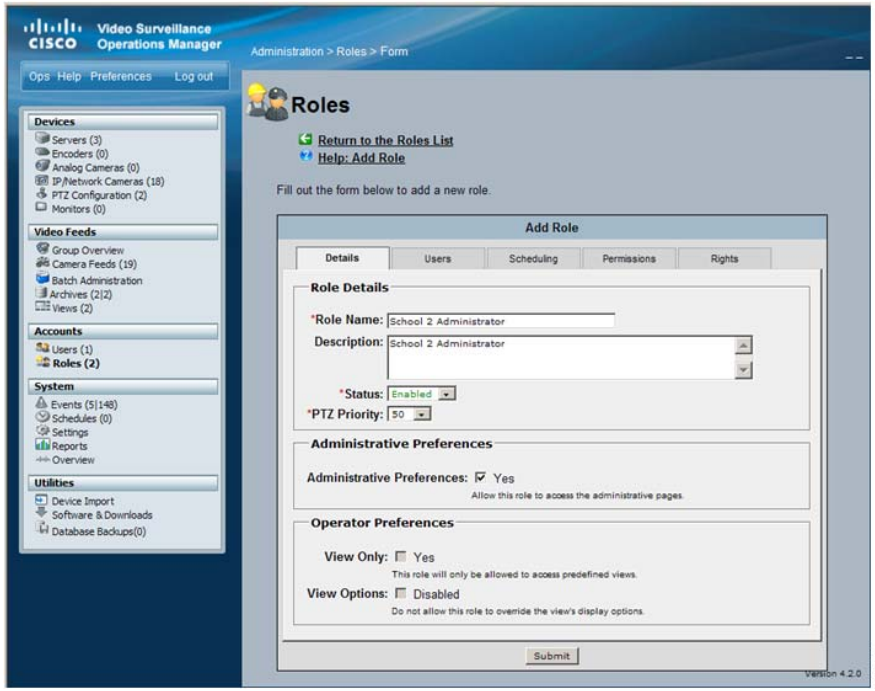
Cisco Video Surveillance

Managing Permissions and Rights

The Video Surveillance Operations Manager provides a detailed management and access control to the application, and resources such as servers, camera feeds and archives. In an environment with different schools monitored by multiple users and a single VSOM, the proper access control should be configured for all users.

Figure 27 shows how to define a role for administrators at School 2. The role can be assigned different access to resources at different locations.

Figure 27 Access Roles



Under **Admin > Roles > Rights**, specify the access rights for the new role. In the example in Figure 28, their role is only allowed access to a single Media Server.

Figure 28 Access Rights to a Role

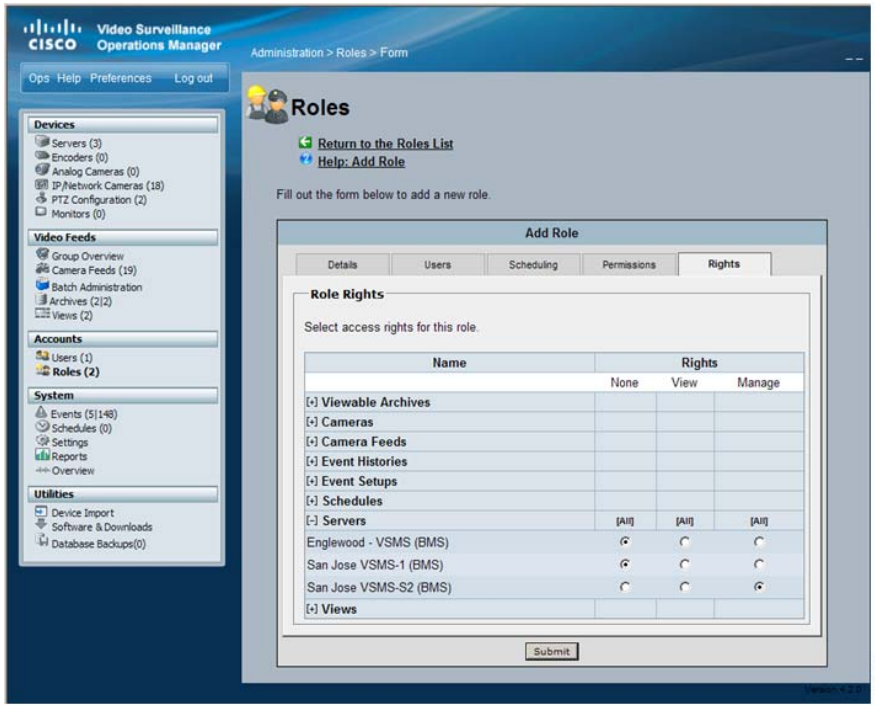
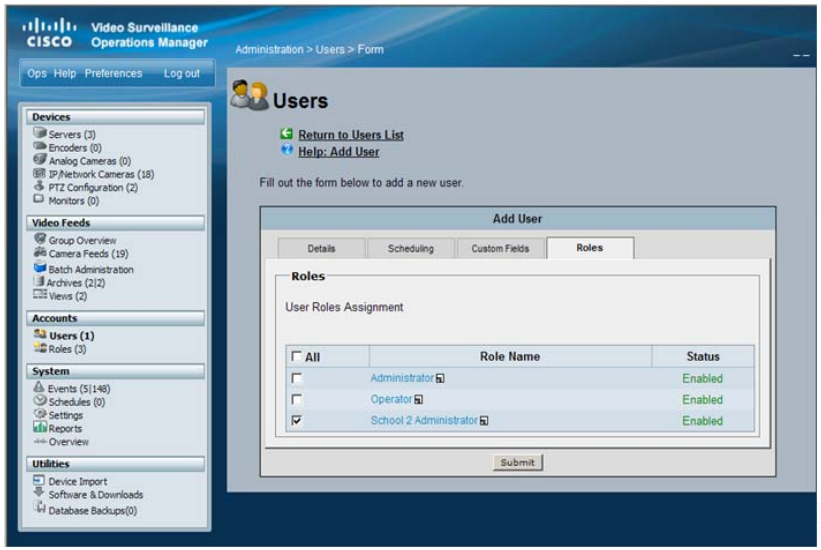


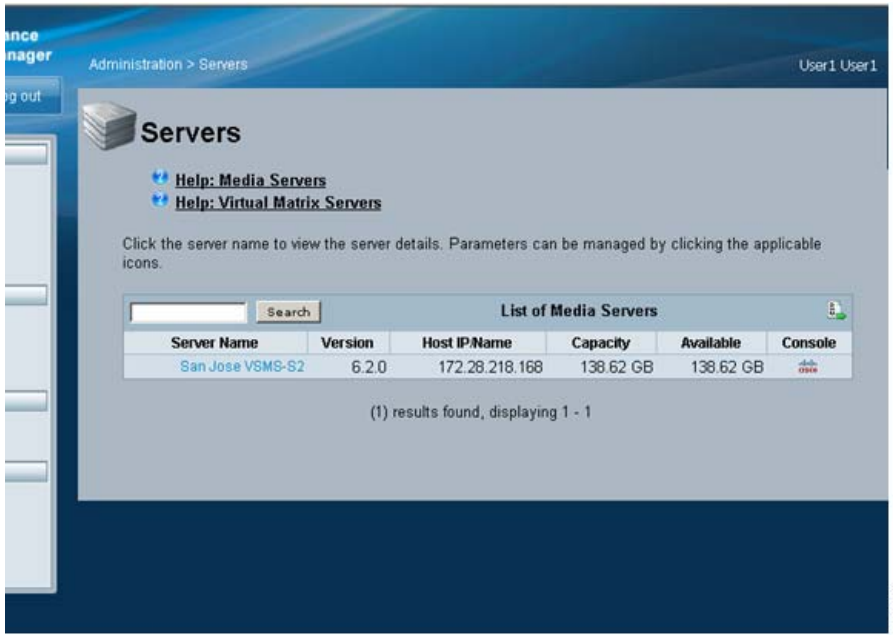
Figure 29 shows how a user is assigned to the new School 2 Administrator Role. All users must be a member of at least one role and can be a member in up to 100 roles.

Figure 29 User Roles



By assigning the user to the new role, the user can only access one Media Server from the server's list and is unaware of all their servers in the system, as shown in Figure 30.

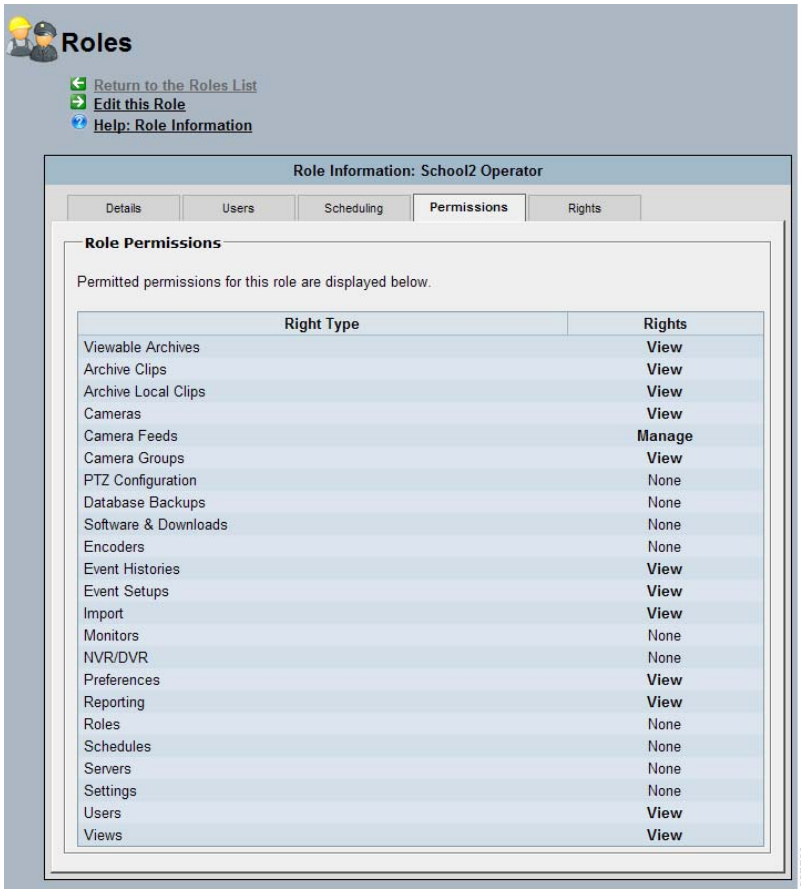
Figure 30 Server Restrictions



With the combination of Users and Roles, VSOM allows for a granular definition of rights to specific resources. For example, it is possible to have permissions to manage some camera feeds but have no rights to others. This feature becomes attractive in a system with a large number of devices and locations, since VSOM only displays the resources allowed to each user.

Figure 31 shows how the School2 Operator role has limited access to VSOM resources by selecting **Admin > Roles > School2 Operator > Permissions** in VSOM.

Figure 31 Roles for School2 Operator



Those changes are reflected on the main screen for User1, who is assigned to the School2 Operator role. In Figure 32, User1 has now limited access to VSOM resources and is unaware of devices at other schools.

Figure 32 School2 Operator Admin Page

VSOM supports defining schedules for the different roles, allowing for a flexible and secure management of devices based on the time of day.

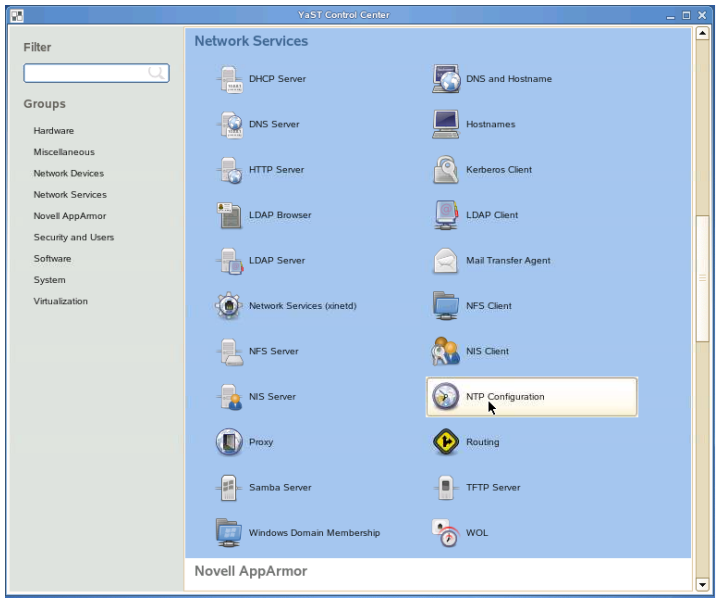
Camera/Time Synchronization

In order to keep video synchronization, it is important to maintain the correct time on the servers and cameras. The need for time synchronization becomes apparent when reviewing video from archives and the time stamp becomes critical to the reviewing process.

NTP configuration should be completed before archive recording is configured. NTP should be configured on all cameras, VSMS, and VSOM servers.

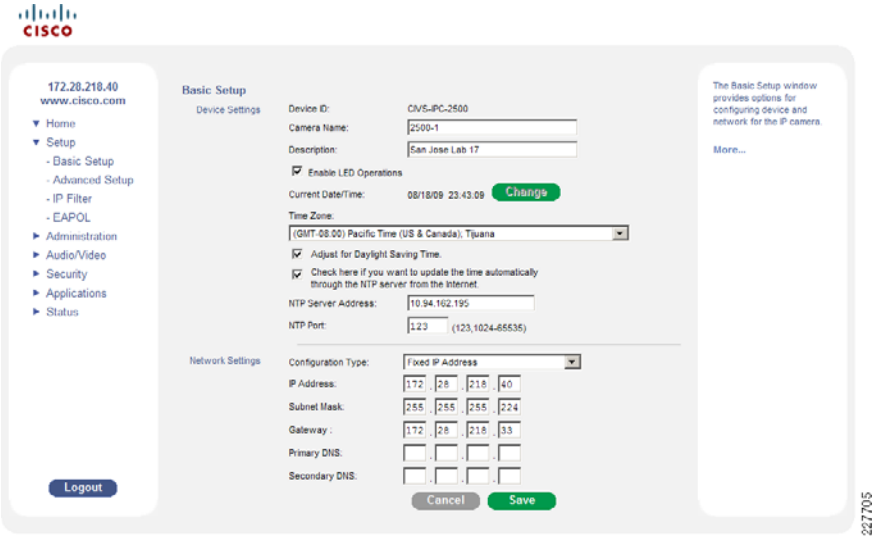
For SUSE installations the YaST is used to configure NTP settings. From the server, select **Computer > YaST > Network Services >NTP Configuration** as shown in Figure 33. On the following screen, specify the NTP servers' IP address.

Figure 33 SUSE NTP Configuration



IP cameras can also be synchronized to the same NTP server. The configuration steps vary by camera type and manufacturer. To configure NTP for a Cisco 2500 IP Camera, click on **Setup > Basic Setup** and specify the NTP Server Address and Time Zone as shown in Figure 34.

Figure 34 NTP Configuration Cisco 2500 IP Camera



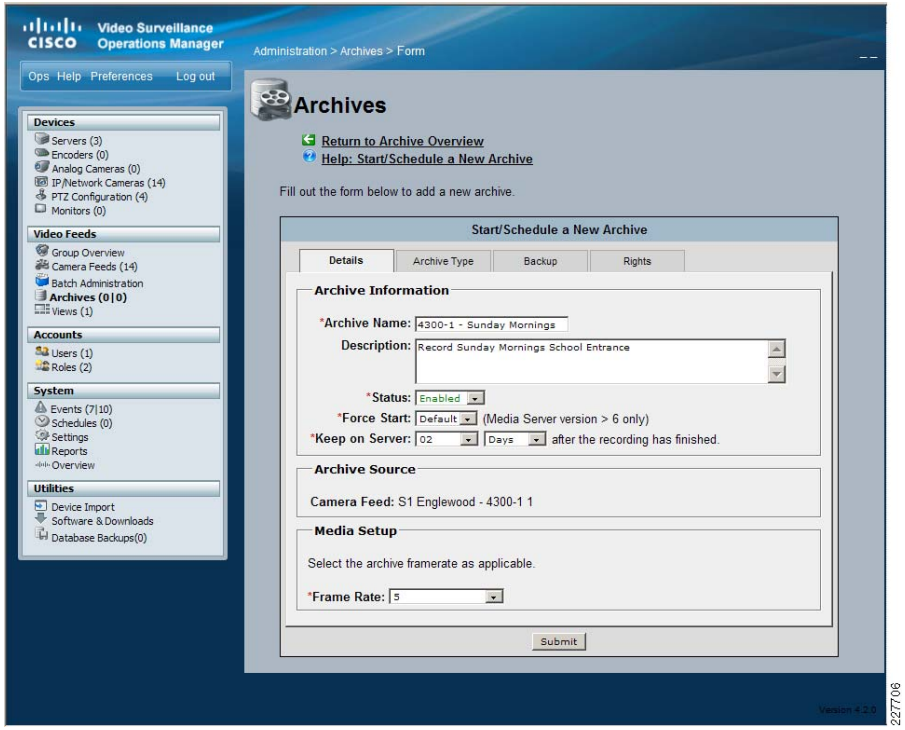
To configure the time settings on a Cisco 4300 IP Camera, click on **Network Setup / Time > Use the NTP Server to Update Time** and specify the NTP Server Settings and Time Zone.

Viewing Archived and Live video from the District Office

VSOM provides flexible video archive capabilities for all cameras in the system, regardless of their location. For this application deployment guide, archives were stored at each location in order to maximize the bandwidth use across the WAN. With the proper permissions, any user is able to monitor and view archived video from any school.

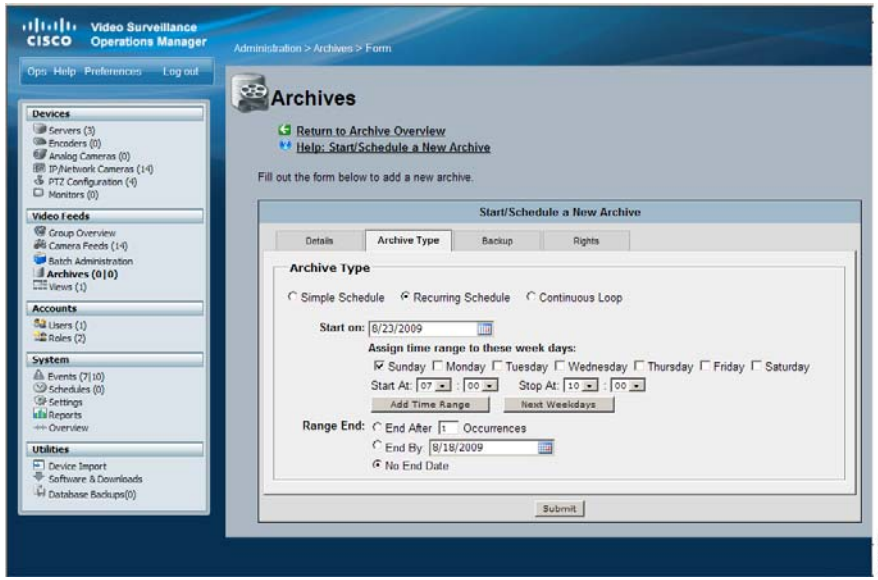
To create a recurring recording loop under VSOM, select **Admin > Archives > Start/Schedule a New Archive** and select the camera source. Click **Next** and define an archive name, frame rate, and for how long to keep in the server, as shown in Figure 35.

Figure 35 Create New Archive



Before clicking **Submit**, define the Archive Type and recurring parameters. The example in Figure 36 creates a recurring archive for Sunday mornings, from 7:00am to 10:00am.

Figure 36 Specify Archive Type

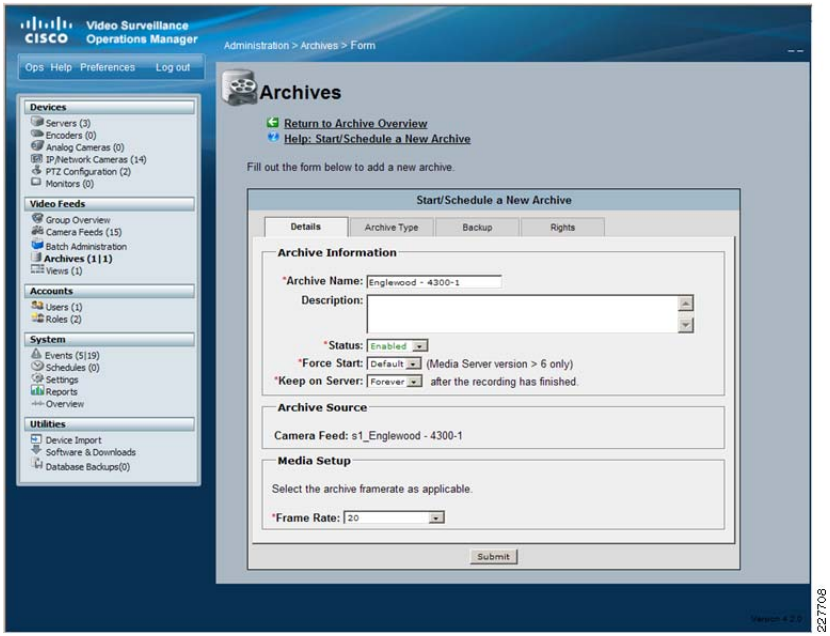


VSOM offers the option to keep archives for a predefined number of days. After recording is complete, the archive is kept on the server for predefined number of days. In the previous example, the archive is kept for two days after the archive is complete and automatically deleted.

With the use of Child Feeds, VSOM is able to transmit a camera feed to other locations as video is requested. In this application deployment guide, camera feeds are recorded locally at the school, but they can be transmitted to the district office using all lower frame rate in order to save bandwidth.

In the example in Figure 37, an archive has been created at the local Media Server with a frame rate of 20 frames per second. The Media Server will get the video feed directly from the camera and the archive will not generate any traffic to the district office unless archive video is requested.

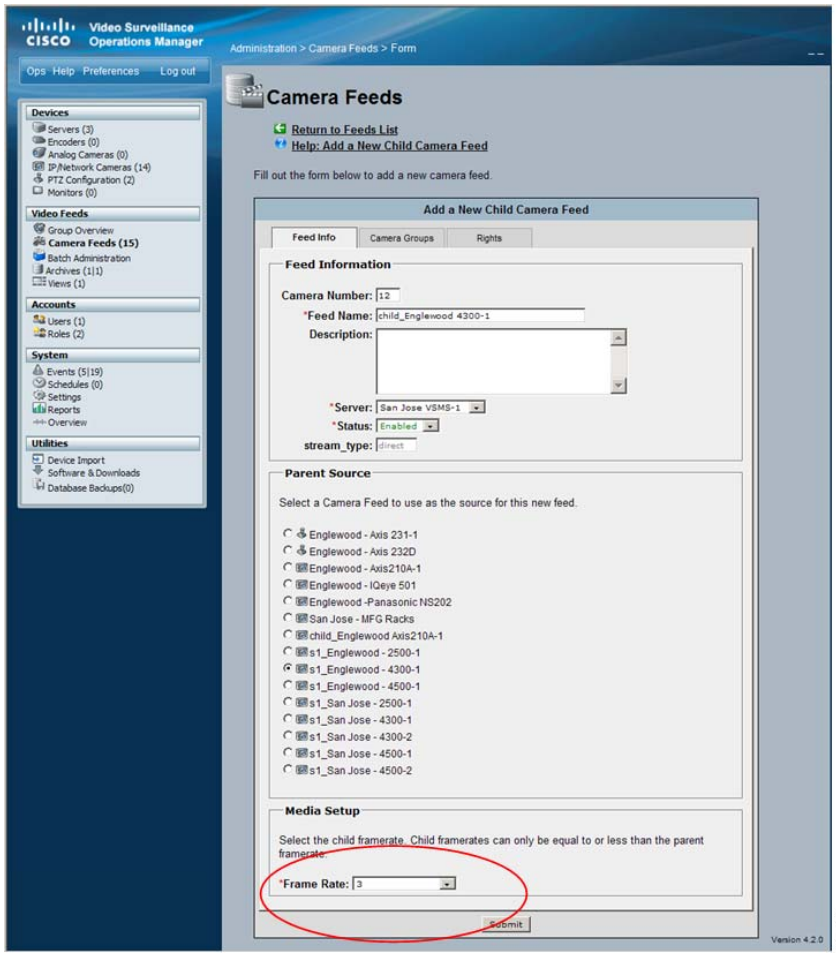
Figure 37 Local Archive



While VSOM does not provide transcoding capabilities to video streams, a ChildFeed may be configured with the same image quality and lower frame rate in order to reduce bandwidth utilization across the locations.

To create a child feed, select **Admin > Camera Feeds > Create a New Child Feed**. Figure 38 shows a child feed created from a parent source. The child feed will be reduced to three frames per second, reducing the bandwidth requirements between locations.

Figure 38 Child Feed



Setting Up Video Surveillance Operations Manager for Motion Detection

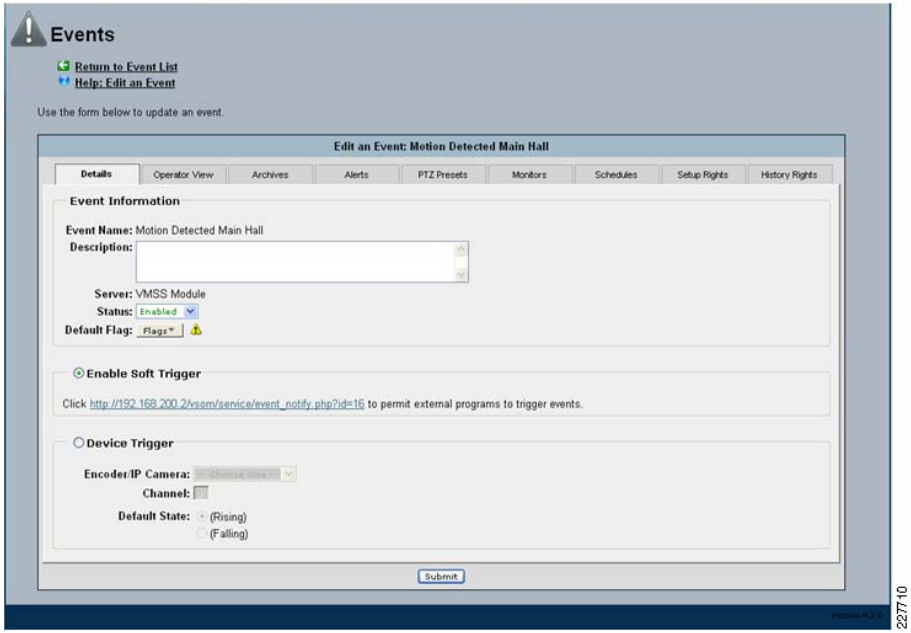
Configure the camera feeds to match the camera setup and verify access to the camera through the Operations Manager. Once this step is complete, triggers for motion detection may be configured.

From the Administration screen in VSOM, complete the following steps:

1. Select **Events** under the System section.
2. Select **Add a New Event** and specify the following:
   a. For the Event Name, use a short meaningful name since this will be displayed on the Ops console when an event is triggered (i.e., Motion Detected Main Hall).
   b. Select the VSMS server where the cameras are defined.
   c. Enable the trigger.
   d. Change the default flag if desired. This is used in the Event List display on the Ops screen.
   e. Select **Enable Soft Trigger**.
   f. DO NOT select **Enable Motion Detection**.
   g. Click **Submit** to save the changes.

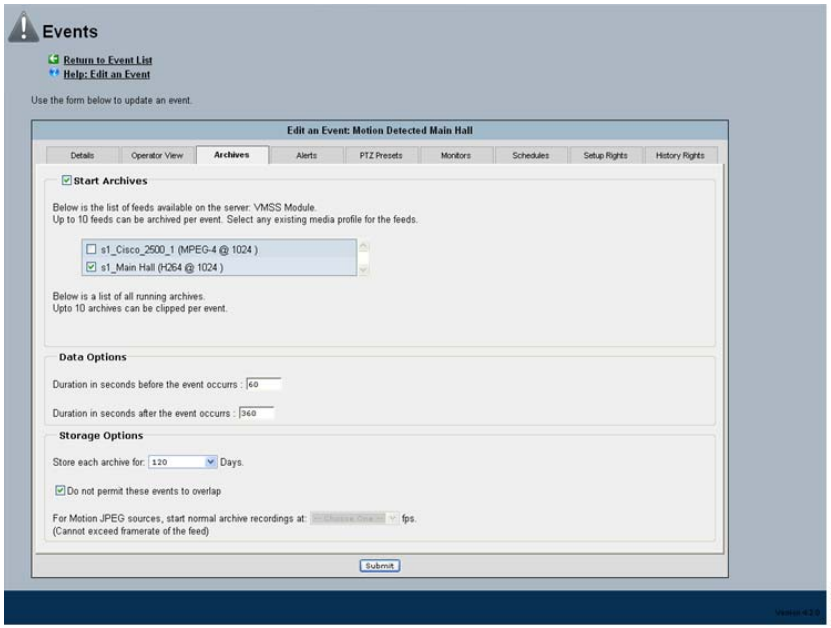
Once submitted, a new screen will display with the **Enable Soft Trigger** selected, with a URL that is used to permit external programs to trigger events. At the end of the URL, there is an ID=*xx*, where *xx* is the number of the soft trigger. This number should be used when configuring the 4000 Series camera under the **Basic Setup >ID field** tab. For the 2500 Series cameras, this number is used when configuring the Augusta EdgeFrontier trigger for motion. See Figure 39 for an example of the URL from VSOM.

Figure 39 VSOM Event Configuration



3. At this point, select the **Archives** tab, and setup the actions that will be taken when the trigger occurs. See Figure 40.

Figure 40 VSOM Event Archive Configuration



For this solution testing, the following were specified:

- Select Start Archives—This creates an archive loop that is used to create clips when a trigger is initiated. The only portions of this archive that is saved are the parts that are identified for a trigger event.
- Select the archive that correlates to the camera feed you are working with.
- Under **Data Options**, select a period of time before and after that you want to include in the video archive that is retained. Using 60 before and 360 after allows for activity for 1 minute prior to the incident, and 6 minutes after. This ensures the capture of the event in the archive. Change these settings as necessary.
- Under **Storage Options**, select the duration that you would like to save any events that occur as part of this archive. This will allow you to go back and select that event from the event list in that archive to review the incident.

Setting Up the 2500 Camera for Motion Detection

There are multiple configuration options for the 2500 Series camera. This section only deals with those options that are relevant to the solution.

Basic Setup is minimal. The most important value on the Basic Setup screen is the use of the NTP server to manage the time on the camera. If time is not synchronized, finding incidents in the VSOM console becomes difficult.

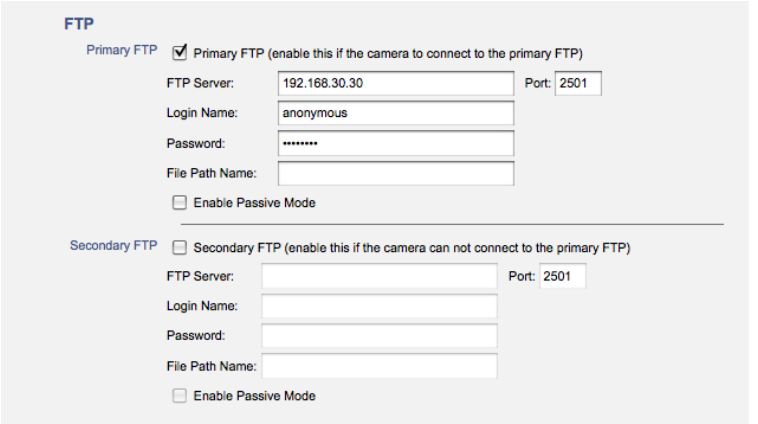
Under the **Administration** menu, create a user for the VSMS server to access the camera with Administrator access.

Under the **Audio/Video > Video**, the following settings were used in the test environment:

- Streaming Mode—Single MPEG-4 Stream
- Resolution—720 x 480
- Video Quality Control—Constant Bit Rate set to 1 Mbps
- Max Frame Rate—15 fps
- **Options > Enable Time Stamp**—Enabled
- **Options > Enable Text Display**—Free-form text set to location of the camera (i.e., front hall)

1. Under the **Applications** menu, select Mail and FTP. The Mail option is not used. See Figure 41 for the FTP configuration.

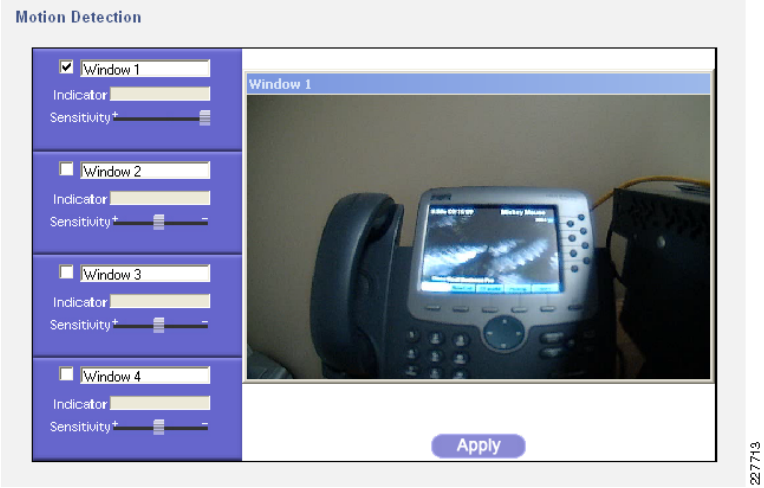
Figure 41 Cisco 2500 FTP Configuration



- FTP Server—IP address of the Augusta EdgeFrontier Server
- Port—Port configured on the Augusta EdgeFrontier Server to listen for 2500 Series camera connections (see section on Augusta EdgeFrontier for details)
- Login name—Not used but required; anonymous is sufficient
- Password—Not used but required; anonymous is sufficient

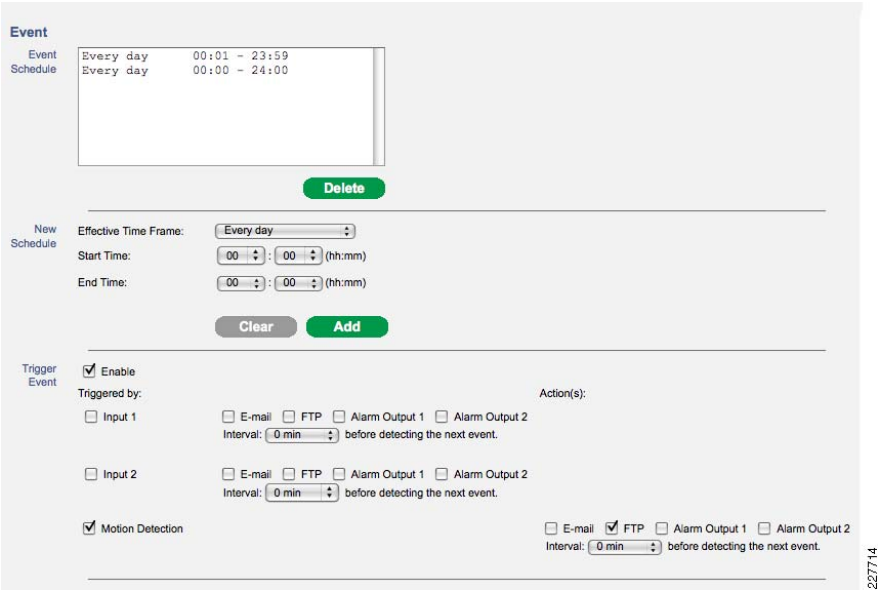
2. Select Motion Detection. See Figure 42.

Figure 42 Cisco 2500 Motion Detection Setup



3. Check the box for **Window 1** and select the entire window. Alternatively, multiple selections could be made with unique sensitivity settings. Any motion in any window will result in the motion event being triggered.
4. Select **Event**. See Figure 43.

Figure 43 Cisco 2500 Schedule and Trigger Event Setup



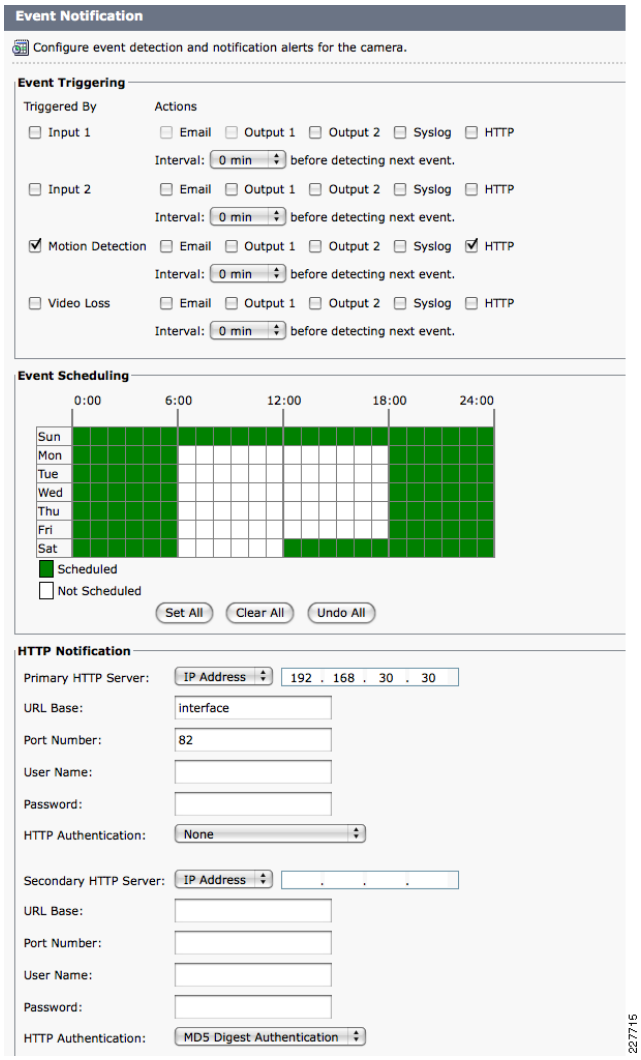
5. Create the **Event** schedule appropriately. This will determine if the event triggers the Augusta EdgeFrontier server. For the trigger event, select the following:
   a. The **Enable** check box.
   b. The **Motion Detection** check box.
   c. The **FTP** check box.

Setting Up the 4000 Series Camera for Motion Detection

There are multiple configuration options for the 4000 Series camera. This section only deals with those options that are relevant to the solution.

1. Select **Setup > Administration** and create a user with Administrator privileges for the VSMS server to access the camera stream.
2. Select **Network Setup**.
3. Select **Basic** and ensure the following settings are specified:
   - *ID*—The number in the ID box should be the same as the ID number assigned to the soft trigger in the VSOM Admin screen. See the VSOM setup for more details.
   - *Name*—Name should be set to a descriptive name that indicates the location (i.e., Main Hall). This name is used in the message built and sent to Singlewire InformaCast for notification to the phones.
   - Other fields are optional and not used for this solution.
4. Select **Time** and set the following values:
   - *Time Mode*—Use NTP server to update time.
   - Primary NTP server should be valued to the NTP server used for all devices in this solution.
5. Select **Feature Setup**. Select streaming as follows; your requirements may be different.
   - Current Channel—Channel 1 – Enable Channel
   - Video—Video Standard – NTSC
   - Video—Video Resolution – 1280 x 720
   - Video—Video Quality Control – Constant Bit Rate – 2 Mbps
   - Video—Maximum Frame Rate – 15 fps
6. Select **Video Overlay**.
   a. Select **Enable Time Stamp** (useful in video forensic activity).
   b. Select **Enable Text Display** (use the same name as configured in Step 3 above).
7. Select **Event**. See Figure 44.

Figure 44 Cisco 4000 Series Event and Schedule setup



c. Select **Motion Detection** check box and select **HTTP** as the notification type.

d. Create the Event Schedule (this indicates what times that events will be triggered and sent to the Augusta EdgeFrontier Server).

e. Primary HTTP Server—IP address of the Augusta EdgeFrontier Server

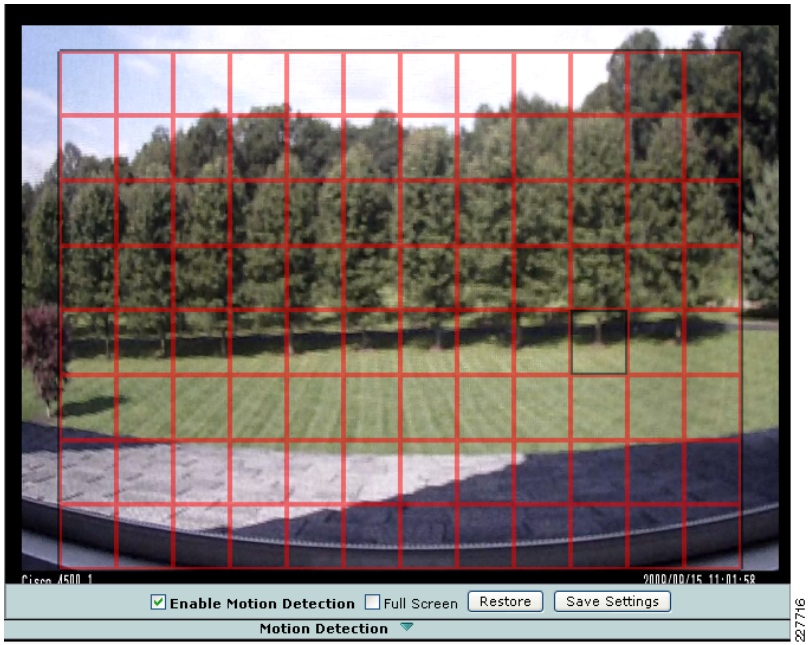
f. URL Base—Must be set to interface as shown. This is a case sensitive parameter required for the interaction with the Augusta EdgeFrontier server.

g. Port Number—Port number configured on the Augusta EdgeFrontier server to listen for activity from 4000 Series cameras. See the Augusta EdgeFrontier server setup section for more details

h. Secondary HTTP server is not used, but could be configured to point to an additional Augusta EdgeFrontier server for HA considerations.

8. Select **View Video** from the menu bar at the top. See Figure 45.

Figure 45 Cisco 4500 Series Motion Detection Setup



a. Select the **Motion Detection** arrow at the bottom of the screen to display the Motion Detection controls.

b. Select the **Enable Motion Detection** box.

At this point, you can select each individual box and adjust the sensitivity settings for each selection, or, select **Full Screen** mode.

Cisco Unified Communications

This solution relies on the Singlewire InformaCast application communicating with Cisco Unified Communications Manager and the phones. The Cisco Unified Communications system must be configured to support that communications. Below are the configurations required for the various call control platforms.

Cisco Unified Communications Manager

On the CUCM cluster, the following must be configured:

1. Configure and enable SNMP.
2. Set up a CTI port.
3. Set up a CTI user for Recording.
4. Set up a CTI user for Broadcasts.

Older versions of CUCM require the "Include Encoding Information in AXL response" to be set to true.

Singlewire InformaCast only supports G.711µ, therefore, if the system uses other codecs, you must create a region and calling search space with G.711µ as the codec.

The configuration required for each version of supported CUCM software is well documented in the Singlewire InformaCast documentation, so it will not be replicated here. The Singlewire InformaCast documentation can be found at the following URL:

http://www.singlewire.com/s_informacast.html

Cisco Unified Communications Manager Express

In order for Singlewire InformaCast to communicate with CUCME via XML, first the router must be configured to:

- Enable the web browser user interface on the router
- Set the local password for XML queries sent to the router
- Specify that the HTTP payload for XML queries be interpreted in the "form" format

Finally, in CUCME the phone URLs must be configured for use with Singlewire InformaCast.

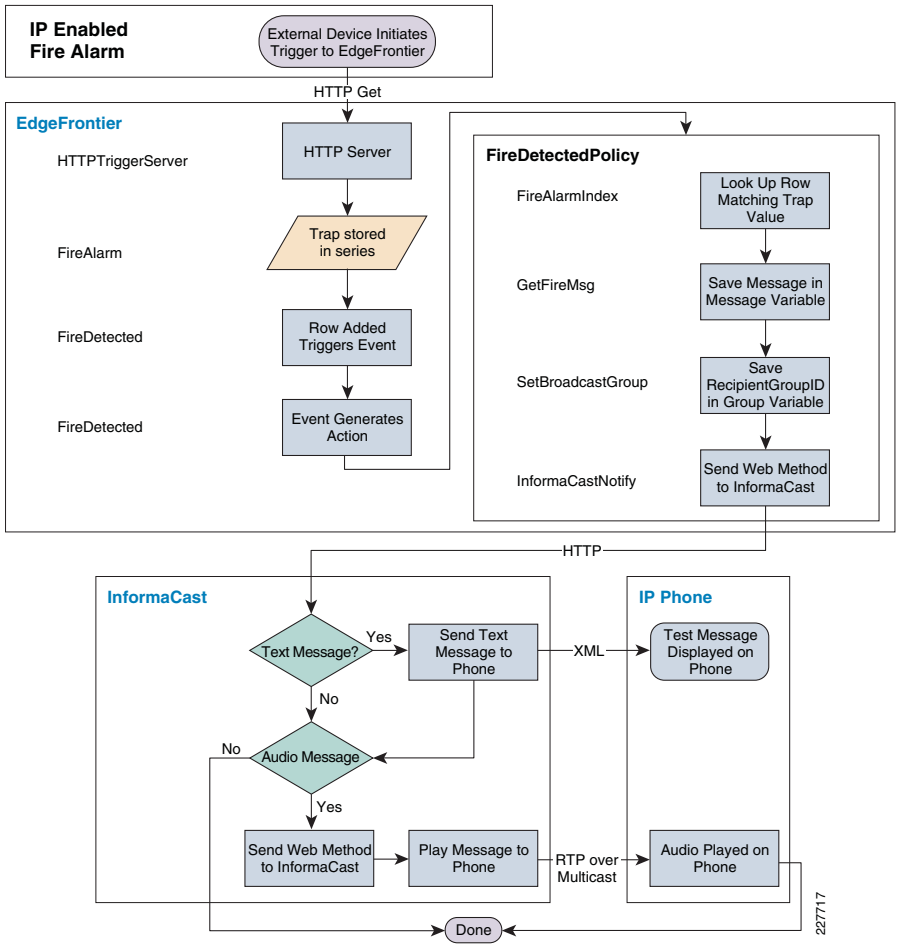
This process is thoroughly documented in the Singlewire InformaCast documentation referenced above.

Partner Products Setup

Following are the detailed steps required to implement the various use cases on the Singlewire InformaCast and Augusta EdgeFrontier. The two applications should be properly installed and the basic configuration completed as outlined in the applications' installation guides.

Figure 46 shows a sample signal flow of what occurs when an alarm is triggered.

Figure 46 Sample Event Trigger Signal Flow



Singlewire InformaCast

On Singlewire InformaCast, configure groups for each unique user group. In this example, two groups were configured using instructions of the document at the following document:

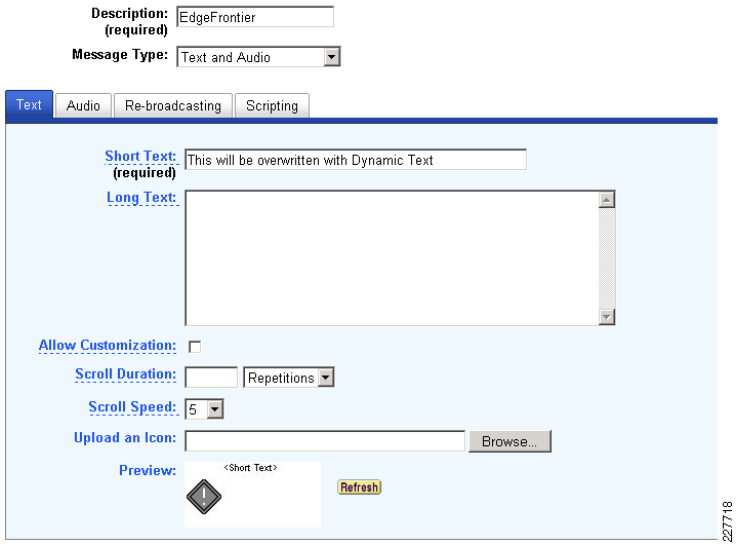
http://www.singlewire.com/pdf/InformaCastCME-7.0.pdd.

These were a Security group consisting of the wireless phones, and a Classroom group consisting of the hard wired phones. The group number is required so the Augusta EdgeFrontier system can direct messages to the appropriate phone. This number can be determined by selecting **Edit Recipient Group**s from the main Singlewire InformaCast administrative page and moving the mouse over the Edit button. See Figure 47. The broadcast group is -1.

In this system, a single message using *Text to Speech* is configured. The text and recipient group are dynamically changed by the SOAP message from Augusta EdgeFrontier.

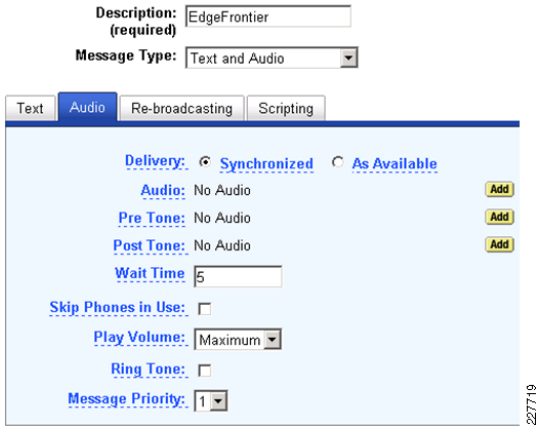
1. On the main administration page, select **Send or Edit Messages**.
2. On the top, select the **Add** button.

Figure 47 Add Message



3. Enter a name and enter text into the short message field. This message will be overwritten by dynamic text from the Augusta EdgeFrontier system.
4. Select the Audio tab. See Figure 48.

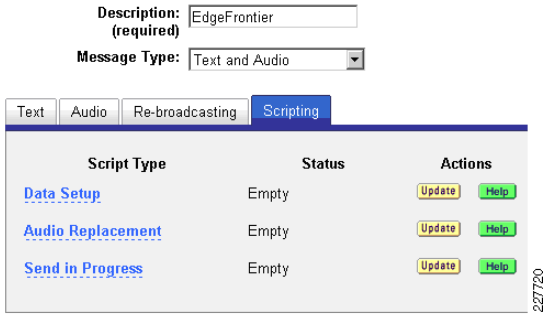
Figure 48 Specify Audio Setting of the Message



   a. Ensure **Message Priority** is **1**.
   b. Set **Play Volume** to maximum. These are emergency messages that will be sent.

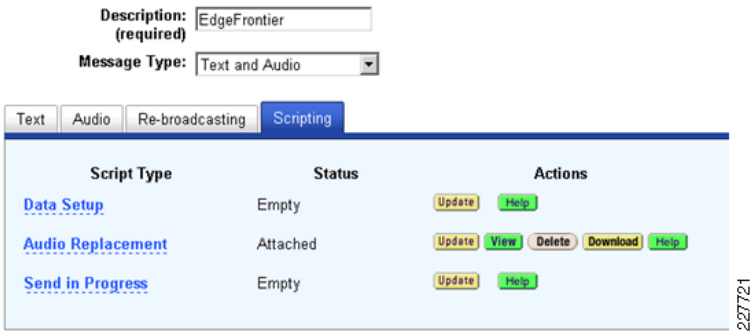
5. Select the **Scripting** tab. See Figure 49, Figure 50, and Figure 51.

Figure 49 Script Setting



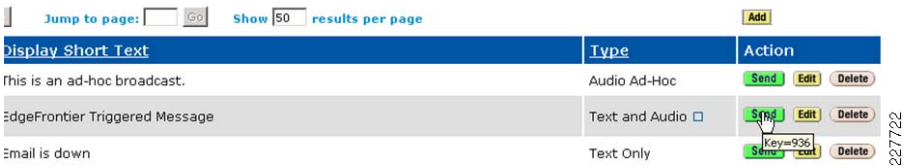
   c. In the Audio Replacement line select **Update**.
   d. When prompted for a file name, browse to **C:Program Files/Singlewire/InformaCast/webapp/sampleScripts** and select the **AudioReplacement.js** file.

Figure 50 Create Replacement Message



   e. The screen should now look like the screen in Figure 50 above. Select **Add**.
   f. The message is now added and set up for text replacement.
   g. The message number for the call from Augusta EdgeFrontier will be required. The process is like looking up the group number.
   h. Move the cursor over the Send button and the message number will be displayed.

Figure 51 Messages



Since Singlewire InformaCast uses multicast to send audio to the phones, multicast must be enabled in the network. Refer to the appropriate switch documentation to determine the requirements and the configuration.

Augusta EdgeFrontier

In general, Augusta EdgeFrontier will gather information from the sensor or camera sending the alert and take actions based on that device. Under certain circumstances (i.e., SNMP alerts), the message associated with the various alarms will be looked up on the Augusta EdgeFrontier server and communicated to Singlewire InformaCast. Once communicated to Singlewire InformaCast, the message may be text, audio, or both.

The Augusta EdgeFrontier server has several sections that require configuration. Additionally, certain values or sections requiring configuration will change based on changes made in other sections. For instance, if Series is selected as an Input parameter, the drop down list will only show values for series already created. This dynamic change makes it very easy to select the proper values and minimizes problems that may occur because of mis-typed values. As a result, creating components in a particular order is sometimes required.

Not all components are required to be created uniquely for each particular use case. For example, it is only necessary to create a single communications component for sending messages to Singlewire InformaCast. By valuing the fields properly before calling that method, it is possible to send unique messages using the same communications component.

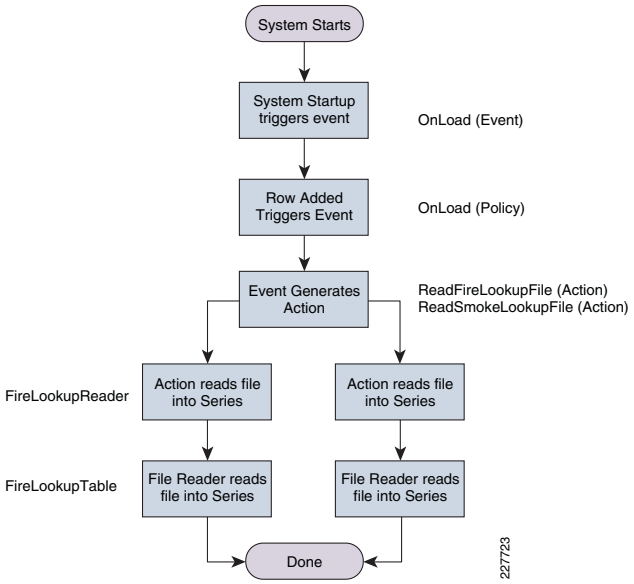
The Augusta EdgeFrontier deployment section is organized such that most steps are in order so that a required step is completed prior to the subsequent step, but some configuration components have been grouped together for organizational purposes. For readability, the order of sections is organized as follows:

- Initialization Steps
- Data Communications Components
- Smoke Alarm use case
- Fire Alarm use case
- Motion Detection with Cisco 2500 Series Camera
- Motion Detection with Cisco 4000 Series Camera
- Notifications based on time of day

Create the Lookup Table Required for SNMP Traps

The lookup table required for the SNMP interface is stored on the Augusta EdgeFrontier server and must be loaded at system initialization. See Figure 52 for the steps necessary to perform the initialization.

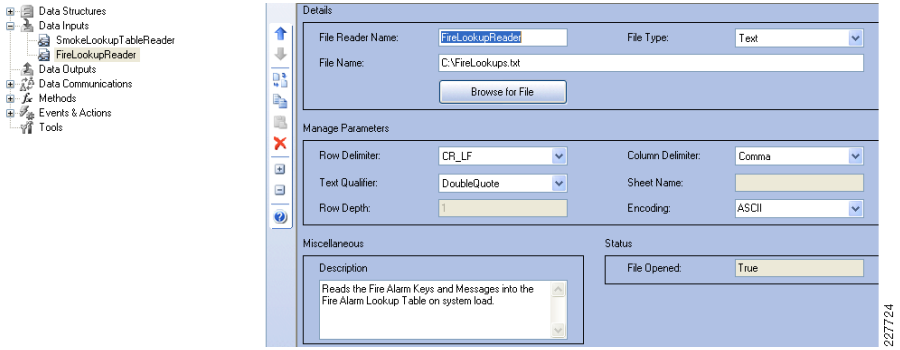
Figure 52 Lookup Table Initialization Flow



A series must be created to store the message that will be received indicating a fire alarm. A second series must be created to store the messages that will be played as audio when a fire alarm is received. These will be stored in files, so begin by creating a file reader.

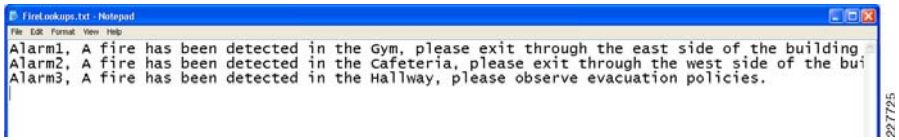
1. Right click on **Data Input** and select **Add File Reader** as shown in Figure 53.

Figure 53 Add File Reader



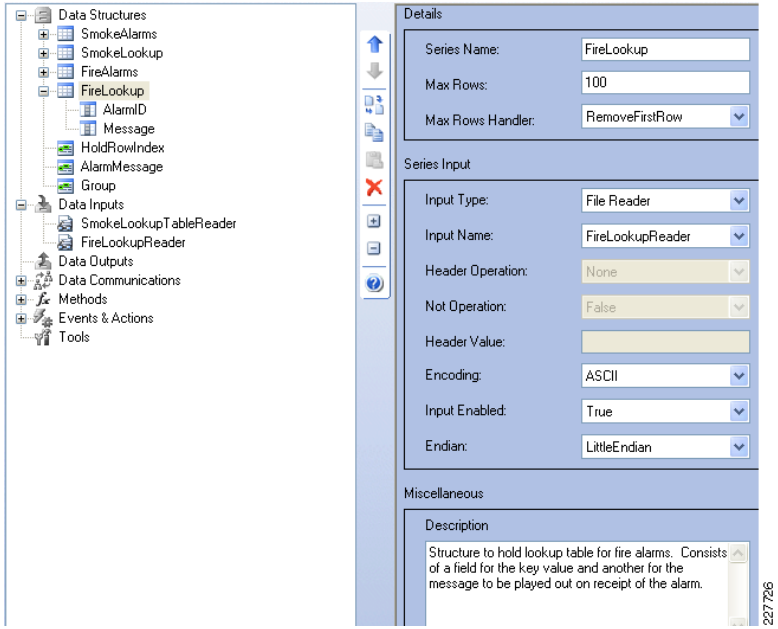
2. Change the File Reader Name to **FileLookupTableReader**. Browse for the name of the lookup file (see Figure 54 for an example). Finally, add a description for readability as shown in Figure 54.

Figure 54 File Reader Text File



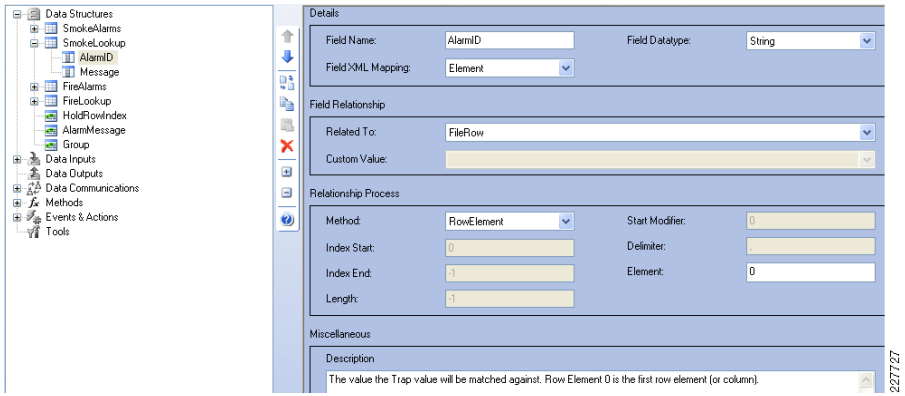
The first field in the line is the value to be matched. **Alarm1** is the text value the Fire Alarm will send in an HTTP get parameter. That should be followed by a comma and the text that should be played by Singlewire InformaCast when the alarm is triggered. This text will be sent to Singlewire InformaCast and displayed as a text on the phone and as audio over the phone's speaker.

Figure 55 Add Series



3. Change Series Name to **FireLookup**. In the Input Type drop down menu select **File Reader**. In the Input Name drop down menu select **FireLookupTableReader**. For readability add a description.
4. The last step in creating the lookup table is to add two fields to the FireLookup series to hold the keys and messages. Right click on the **FireLookup** series and select **Add Field**. See Figure 56.

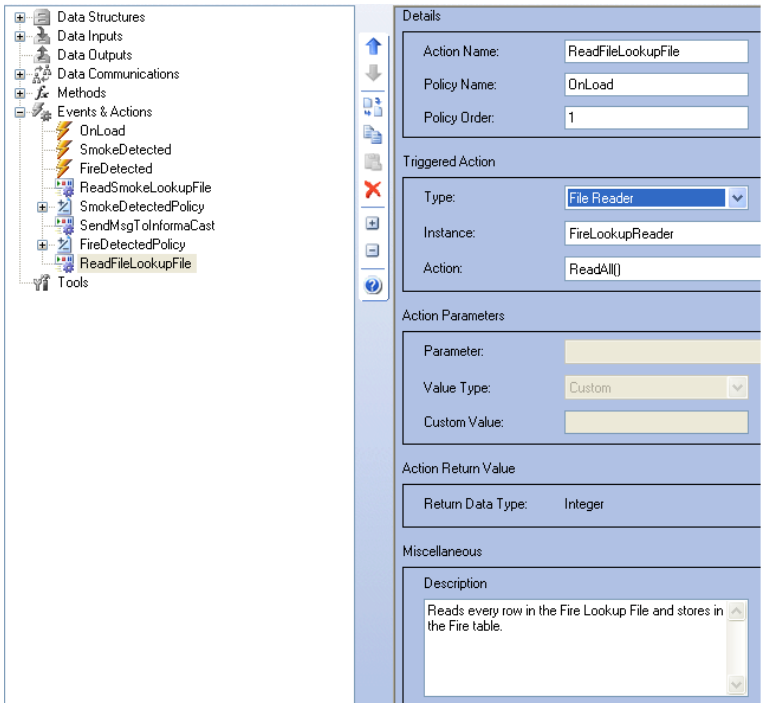
Figure 56 Add Field



Change the Field Name to AlarmID. This will hold the value that will match the Value parameter in the trap. Ensure the Datatype is String.

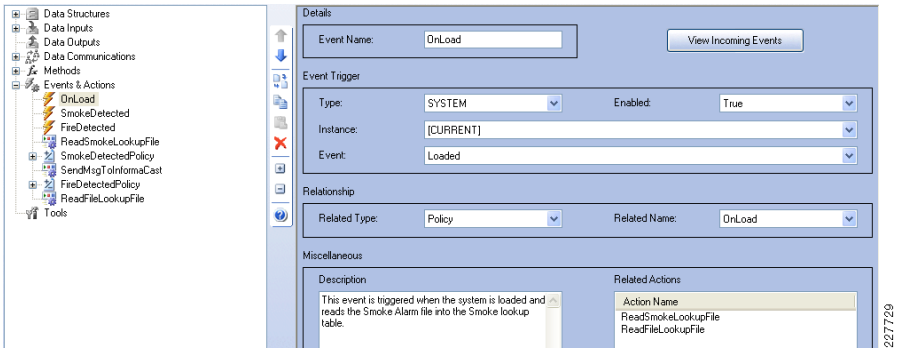
5. In the Related To parameter drop down menu select **FileRow**. In the Method drop down menu, select **RowElement**. For readability add a description.
   a. Right click on the *AlarmID* field and select **Clone Field**. Select the newly cloned field and change the name to **Message**. A second series and file reader need to be added to hold the Smoke Alarms. In *Data Inputs*, right click on **FileLookups** and select **Clone File Reader**.
   b. Select the newly cloned reader and change the name to **SmokeLookupReader**.
   c. Browse for the file with the **Smoke Lookup Table**. This should be the same format as described above for the Fire Lookup Table except, instead of receiving a text string, smoke alarms are SNMP variables and the key value should be a number.
   d. Right click on the **FireLookup** series and select **Clone Series**. Select the newly created series and change the name to **SmokeLookup**. In the *Input Name*, select **SmokeLookupReader**.
   e. There are now file readers for the fire alarm system and the smoke detection system and data structures to store the information read. An action must be created to cause the file reader to read the file into the associated data structure. Right click on *Events & Actions* and select **Add Action**. See Figure 57.

Figure 57 Add Action



6. Change the name to **ReadFireLookupFile**.
7. Add a Policy Name of **OnLoad**. In the *Type* drop down menu, select **FileReader.** In the *Instance* drop down menu, select **FireLookupReader**. In the *Action* drop down menu, select **ReadAll()**. For readability add a description.
8. Create an action to read the **Smoke Alarm LookupFile**.
9. Right click on the **ReadFireLookupFile** action and select **Clone Action**.
10. Change the name to **ReadSmokeLookupFile** and the *Instance* to **SmokeLookupReader.**
11. Create an event to trigger the actions to read the files. This event will run once when the system is first loaded. Right click on **Events and Actions** and select **Add Event**. See Figure 58.

Figure 58 Add Event

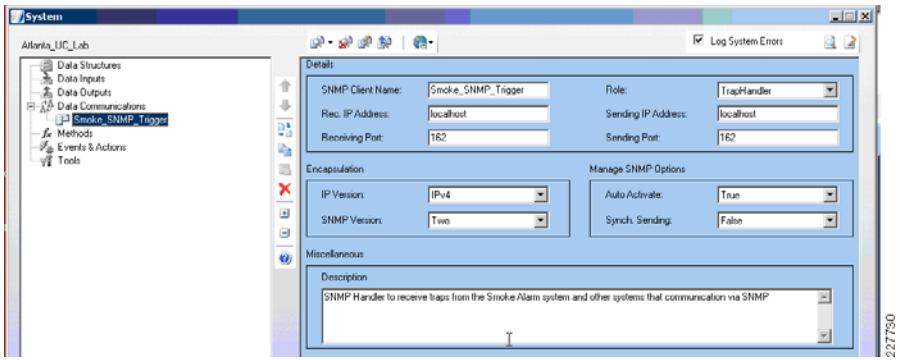


12. Change the name to **OnLoad**. On the *Type* drop down menu, select **SYSTEM**. In the *Instance* drop down menu, select **[CURRENT]** and in the *Event* drop down menu, select **Loaded**. In the *Related Type* drop down menu, select **Policy**, and in the *Related Name*, select **OnLoad**.

Configure the Required Data Communications Components

1. Create the necessary communication components to support the various use cases as described below.
2. Configure Trigger Communications Mechanism—SNMP Client as shown in Figure 59. This is used to receive traps from the smoke detector system and other systems using SNMP to communicate an alarm.

Figure 59 Add SNMP Client

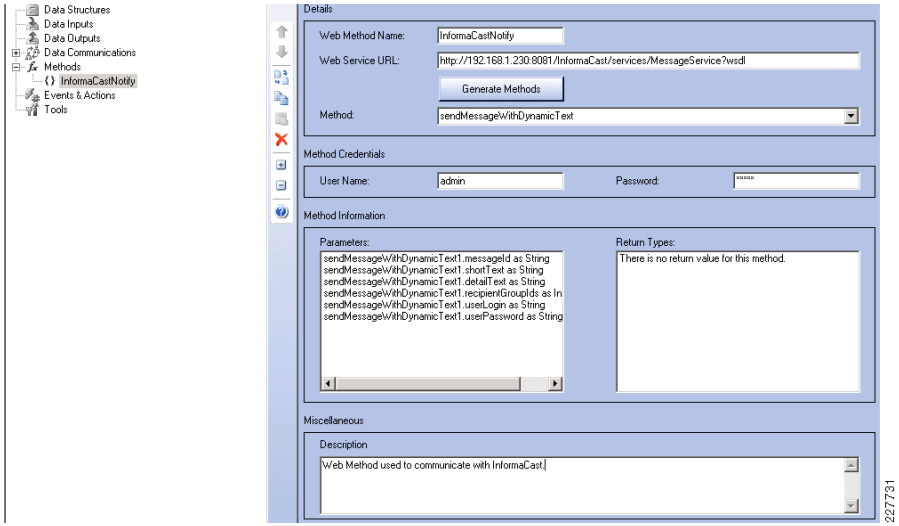


The following table lists the setting for Figure 59.

Data Communications/SNMP Client		
· SNMP Client Name	· Role	· Port
Smoke_SNMP_Trigger	TrapHandler	182

3. Configure a Web Method to Communicate with Singlewire InformaCast system as shown in Figure 60.

Figure 60 Add Web Method

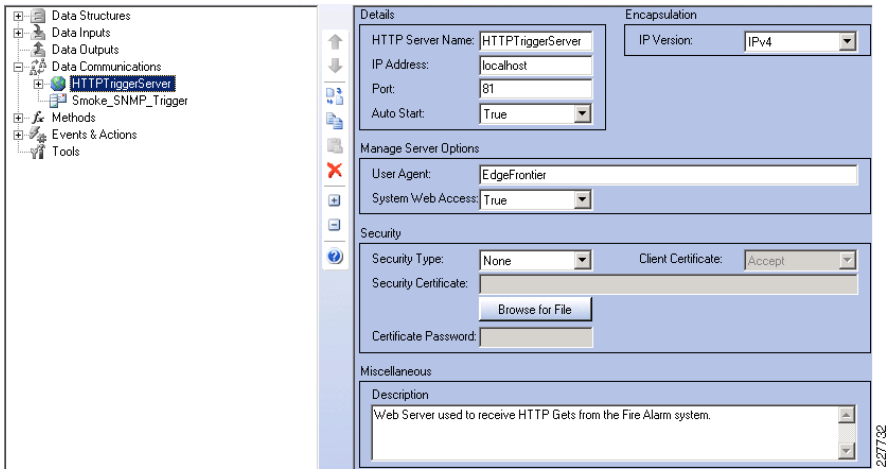


The following table lists the setting for Figure 60:

Methods/Web Method			
Web Method Name	WebService URL	User Name/Password	Method
InformaCastNotify	https://<InformaCast_Server>:8444/InformaCast/services/MessageService?wsdl	InformaCast credentials	sendMessageWithDynamicText

4. Configure an HTTP Server Trigger Communications Mechanism. This is used to receive traps from the Fire Alarm System and other systems using HTTP Gets to port 81 in the case of an alarm. Figure 61 shows the detailed configuration.

Figure 61 Add HTTP Server

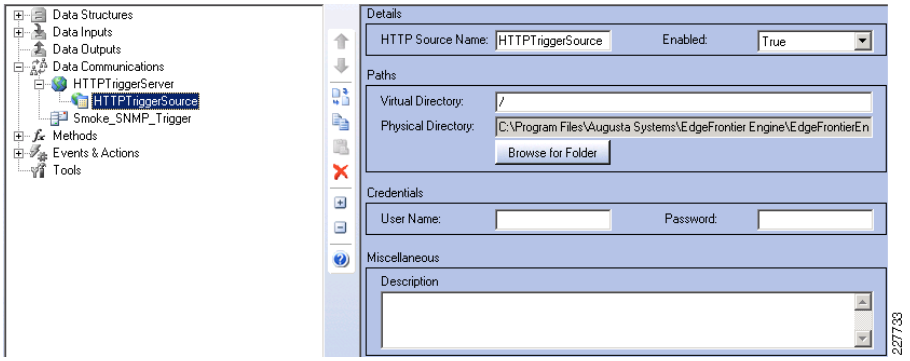


The following table lists the setting for Figure 61.

Data Communications/ HTTP Server			
HTTP Server Name	IP Address	Port	System Web Access
HTTPTriggerServer	Localhost	81	True

5. Add an HTTP Source to the HTTP Server as shown in Figure 62.

Figure 62 HTTP Source

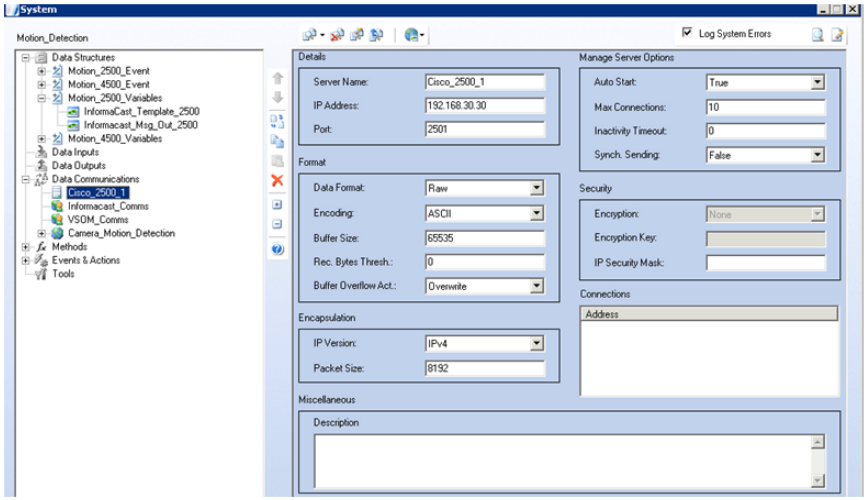


The following table lists the setting for Figure 62:

Data Communications/ HTTP Server / HTTP Source		
HTTP Source Name	Enabled	Virtual Directory
HTTPTriggerSource	True	/

6. Right click on Data Communications and click on **Add TCP Server** to create a communications port for the 2500 Series cameras to contact when motion is detected, as shown in Figure 63.

Figure 63 Add Data Communications

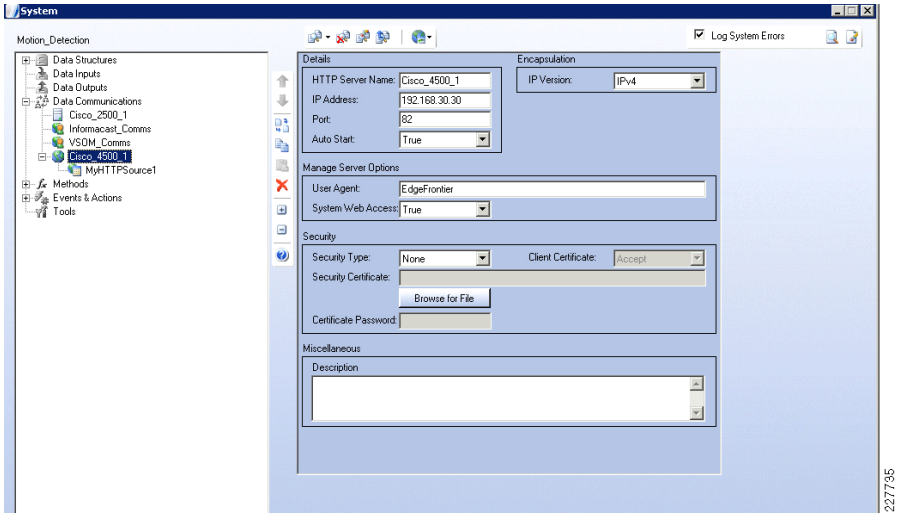


The following table lists the setting for Figure 63:

Data Communications/TCP Server				
Server Name	**IP Address**	**Port**	**Remaining Values**	**Note**
Cisco_2500_1	IP Address of Ethernet interface	2501	Default values	IP Address is typically the server address Port is unique on this server and must match the port number configured in the FTP interface on the 2500 Camera

7. Right click on Data Communications and click on **Add HTTP Server** to provide an HTTP listener where the 4000 Series cameras can post messages when motion is detected, as shown in Figure 64.

Figure 64 Add HTTP Server

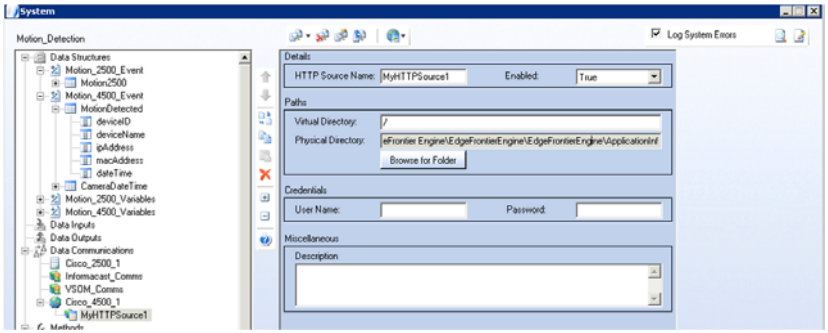


The following table lists the settings for Figure 64:

Data Communications/HTTP Server					
Server Name	**IP Address**	**Port**	**System Web Access**	**Securit y Type**	**Notes**
Cisco_4500_1	IP Address of Ethernet interface	82	True	None	IP Address is typically the server address Port is unique on this server and must match the port number configured in the HTTP interface on the 4000 series camera

8. Right click on the HTTP Server just created and click on Add HTTP Source, as shown in Figure 65.

Figure 65 Add HTTP Source



The following table lists the settings for Figure 65:

HTTP Source					
HTTP Source Name	**Enabled**	**Virtual Directory**	**Physical Directory**	**Credentials**	**Password**
MyHTTPSource1 (You can take the default, it is not referenced later)	True	(Relative to Physical Directory)	Specify a Physical Directory or take default. Nothing is actually deposited here.	(Optional) You can optionally supply an ID and Password if the camera supports authentication	(Optional) You can optionally supply an ID and Password if the camera supports authentication

Smoke Alarm

The smoke alarm system generates an SMNP trap with a value in a specific leaf node in the smoke alarm system MIB. For testing purposes, the snmpSetSerialNo was used in the SNMPv2 MIB. See Figure 66.

Figure 66 SNMP MIB Used for Testing

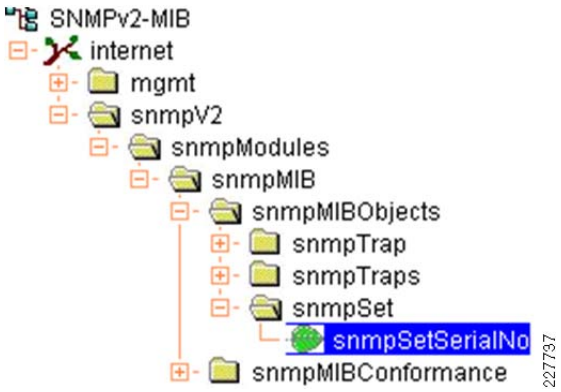
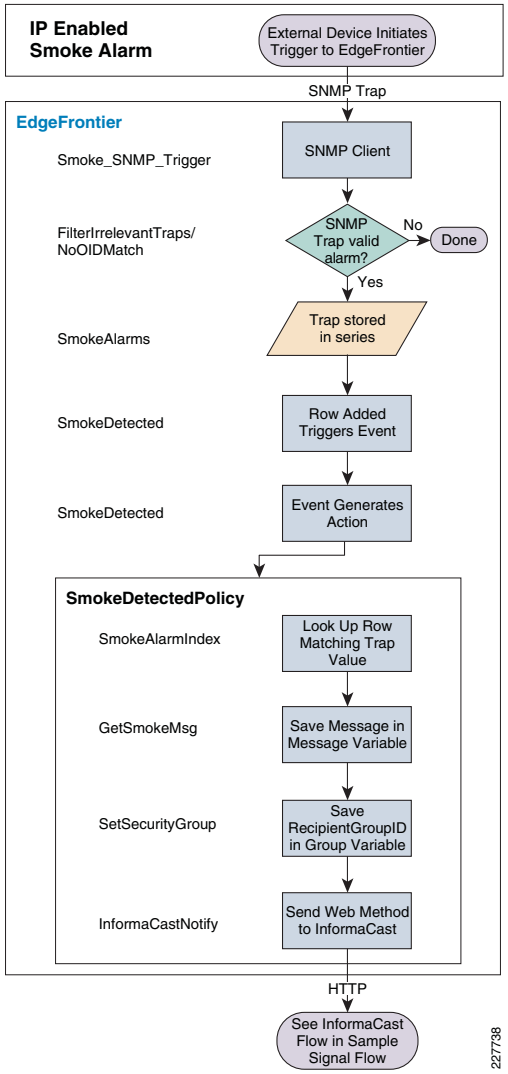


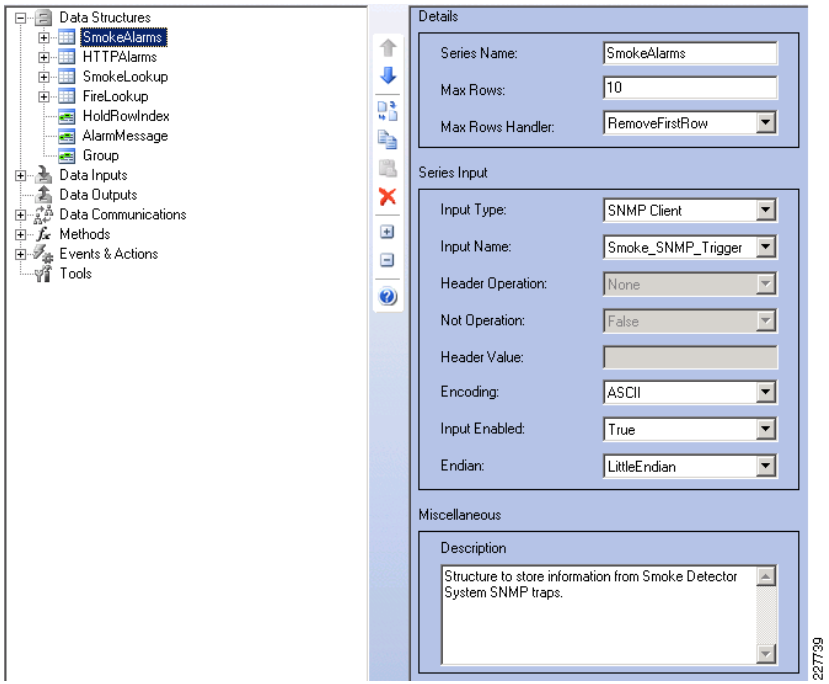
Figure 67 shows the flow for a smoke alarm trap.

Figure 67 Smoke Alarm Flow



1. To build a system for smoke alarms, add a series to hold the information received in the trap, as shown in Figure 68.

Figure 68 Add Data Structure

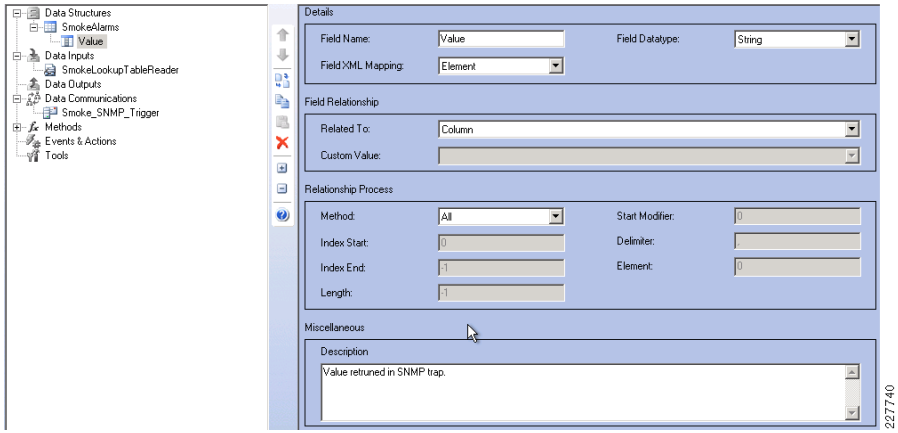


The following table lists the settings for Figure 68:

Data Structures/Series		
Series Name	**Input Type**	**Input Name**
SmokeAlarms	SNMP Client	Smoke_SNMP_Trigger

2. Add a field to the Data Structure that correlate to each SNMP fields (Value, ObjectIdentifier, and RequestID), as shown Figure 69.

Figure 69 Add Field

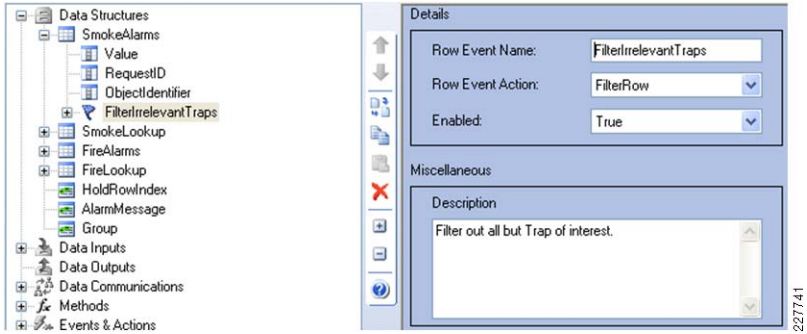


The following table lists the settings for Figure 69:

Data Structures/Fields		
Field Name	**Field Datatype**	**Related To:**
Value	String	Column
RequestID	Int32	Column
ObjectIdentifier	String	Column

3. Add row event to **Filter Irrelevant Traps** of the series by right-clicking on the series name created in the previous step, as shown in Figure 70.

Figure 70 Add Row Event

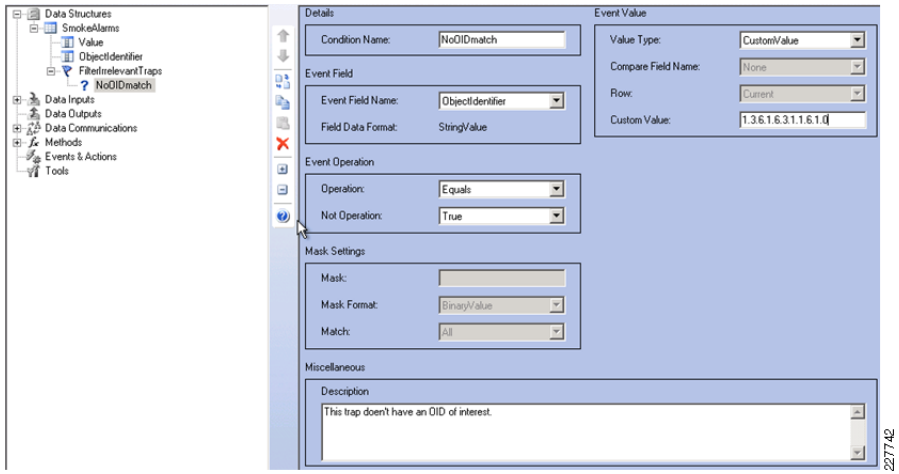


The following table lists the settings for Figure 70:

Data Structures/Series/Row Event	
Row Event Name	**Row Event Action**
FilterIrrelevantTraps	FilterRow

4. Add condition to Identify Irrelevant Traps by clicking on the row event in the previous step, as shown in Figure 71.

Figure 71 Add Condition

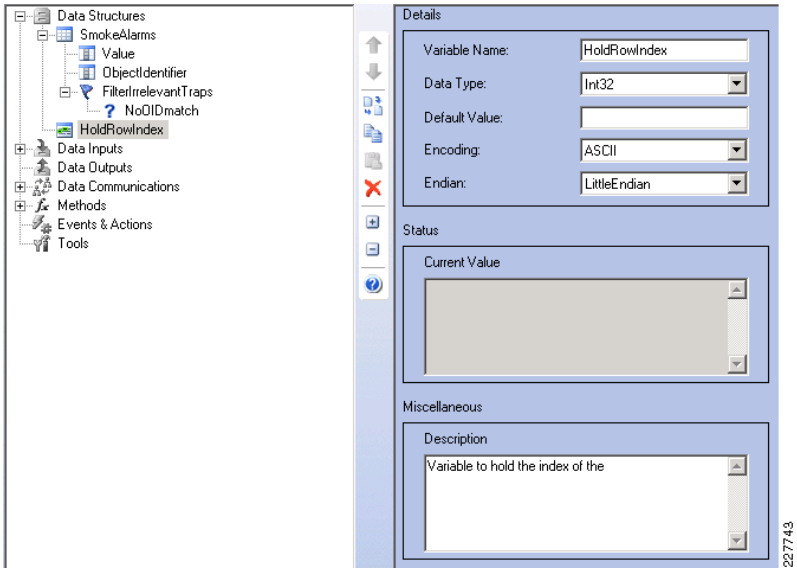


The following table lists the settings for Figure 71:

Data Structures/Series/Row Event/Condition				
Condition Name	**Event Field Name**	**Value Type**	**Custom Value**	**Not Operation**
NoOIDmatch	ObjectIdentifier	CustomValue	Trap's OID	True

5. Add a variable to hold the **Row Index** when looking up the message, as shown in Figure 72.

Figure 72 Add Variable



The following table lists the settings for Figure 72:

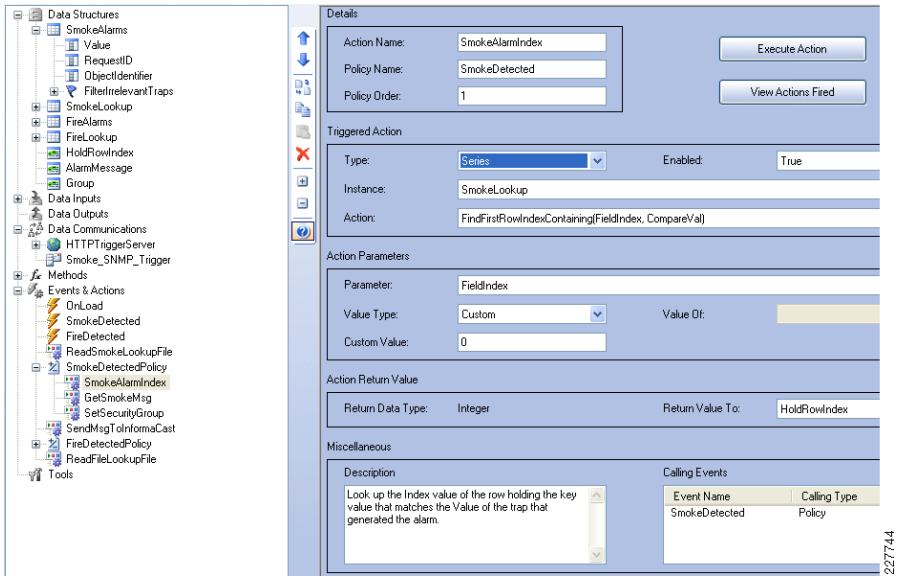
Data Structures/ Variables		
Variable Name	**Data Type**	**Default Value**
HoldRowIndex	Int32	
AlarmMessage	String	
Group	Int64	

6. Create the following actions under an action to look up the Row Index of the trap value when an alarm is received:

- SmokeAlarmIndex
- *GetSmokeMsg*—Used to get the message to be transmitted to Singlewire InformaCast
- *SetSecurityGroup*—Used to store the Security Recipient Group in the group variable

Details are shown in Figure 73.

Figure 73 Add Action



The following table lists the settings for Figure 73:

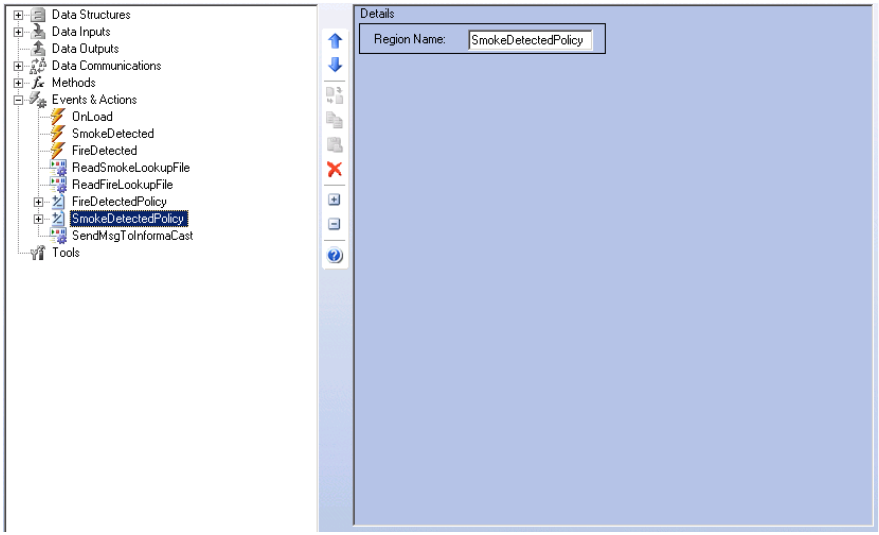
Events & Actions/Actions					
Action Name	**Policy Name**	**Type**	**Instance**	**Action**	**Return Value To**
SmokeAlarmIndex	SmokeDetected	Series	SmokeLookUP	FindFirstRowIndexContaining (FieldIndex,CompareVal)	HoldRowIndex
GetSmokeMsg	SmokeDetected	Series	SmokeLookUp	GetSeriesFieldValue (FieldName, RowIndex)	HoldRowIndex
SetsecurityGroup	SmokeDetected	Variable	Group	Set Value(Value)	

7. For the previous three actions, configure the action parameters as shown in the following table:

Events & Actions/Actions Action Parameters				
Action Name	**Parameter**	**Value Type**	**Custom Value/Value Of**	**Notes**
SmokeAlarmIndex	FieldIndex	Custom	0	First field in the series (field 0).
SmokeAlarmIndex	CompareVal	SeriesField	SmokeAlarms.Value	Series field holding the value of the alarm sent in the trap. This will be matched in the Smoke Lookup Table.
GetSmokeMsg	FieldName	Custom	Message	Name of the field holding the messages to be played out for alarms in the Smoke Lookup Table
GetSmokeMsg	RowIndex	Variable	HoldRowIndex	Index of row corresponding to the alarm received. Looked up in previous step.
SetsecurityGroup	Value	Custom	942	Value of the Group created in InformaCast associated with Security phones. It can be determined by mousing over the Edit button in InformaCast for the Security Group you created.
SetsecurityGroup	CompareVal	SeriesField	SmokeAlarms.Value	Series field holding the value sent in the trap.

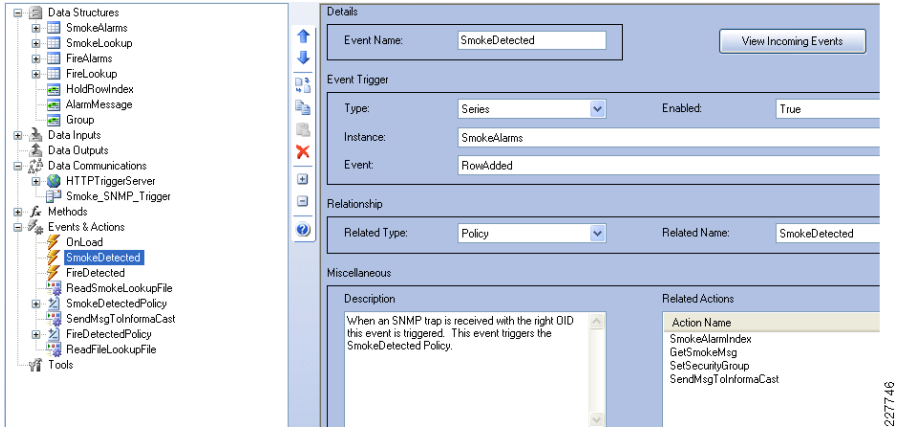
Regions are optional in the configuration, but allow for improved readability of the system by grouping. Figure 74 shows a region with a name related to the smoke alarm settings (**SmokeDetectedPolicy**).

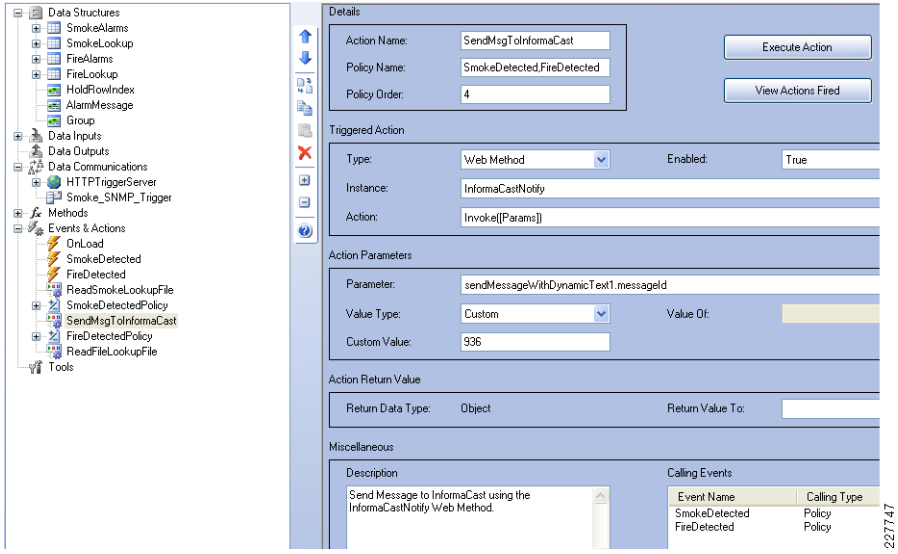
Figure 74 Add Region



8. Once the region is created, move all related actions into the new region.
9. Create an event that will be invoked by an alarm being received to trigger the SmokeDetected action previously defined. Figure 75 shows the detailed steps.

Figure 75 Add Event





The following table lists the settings for Figure 75:

Events & Actions/Events					
Event Name	**Type**	**Instance**	**Event**	**Related Type**	**Related Name**
SmokeDetected	Series	SmokeAlarms	RowAdded	Policy	SmokeDetected

10. Create an action to transmit the information just looked up to Singlewire InformaCast as shown in Figure 76.

Figure 76 Add Action

The following table lists the settings for Figure 76:

Events & Actions/Actions				
Action Name	**Policy Name**	**Type**	**Instance**	**Action**
SendMsgToInformaCast	SmokeDetected	Web Method	Group	Invoke(Params)

11. For the previous action, configure the action parameters as shown in the following table:

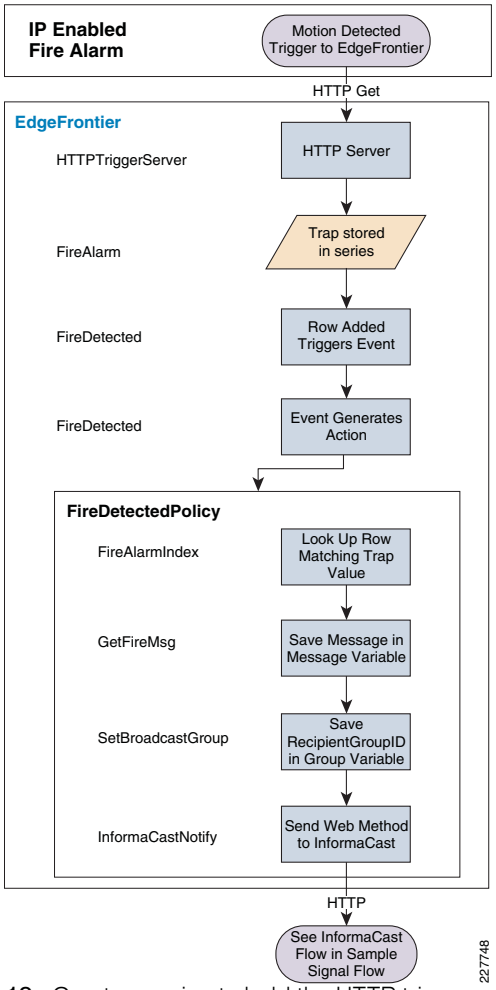
Events & Actions/Actions Action Parameters			
Parameter	**Value Type**	**Custom Value/Value Of**	**Notes**
messageID	Custom	936	ID of the message created in InformaCast with Text to Speech for broadcasting.
shortText	Variable	Message	Variable created to hold the message to be played out to the phones. This variable is populated in the *GetSmokeMsg* action for a smoke alarm, and the *GetFireMsg* action for a fire alarm.
detailText	Custom	Test Message	Not used in this application.
recipientGroupIDs	Variable	Group	Variable created to hold the InformaCast group to receive this message. This variable is populated in the *SecurityGroup* action for a smoke alarm, and in the *BroadcastGroup* action for a fire alarm.
userLogin	Custom	admin	Login Name for the InformaCast system
userPassword	Custom	cisco	Login Password for the InformaCast system

Fire Detection

The fire alarm system generates an HTTP Get with a parameter named Event on port 81. That value is arbitrary. Use the same port configured by the fired alarm system.

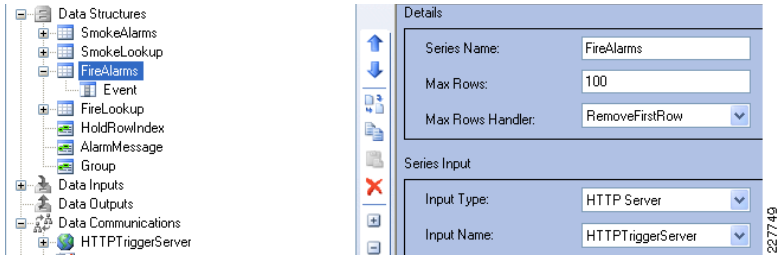
Figure 77 shows the data flow for a fire alarm.

Figure 77 Fire Alarm Flow



12. Create a series to hold the HTTP triggered alarms as shown in Figure 78.

Figure 78 Add Series —FireAlarms

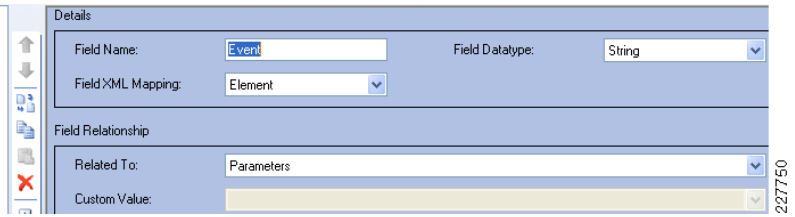


The following table lists the settings for Figure 78:

Data Structures/Series		
Series Name	**Input Type**	**Input Name**
FireAlarms	HTTP Server	HTTPTriggerServer

13. Add a field to store the parameter in the HTTP Get, indicating the alarm type as shown in Figure 79.

Figure 79 Add Field - Fire Event

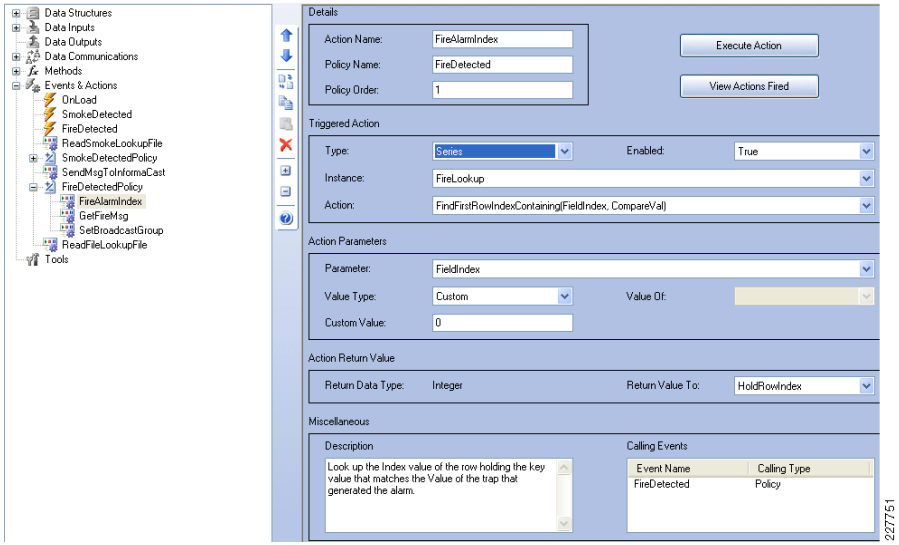


The following table lists the settings for Figure 79

Data Structures/Fields		
Field Name	**Field Datatype**	**Related To:**
Event	String	Parameters

Create an action to look up the row index where the key matches the received alarm as shown in Figure 80.

Figure 80 Add Action - Fire Alarm



The following table lists the settings for Figure 80:

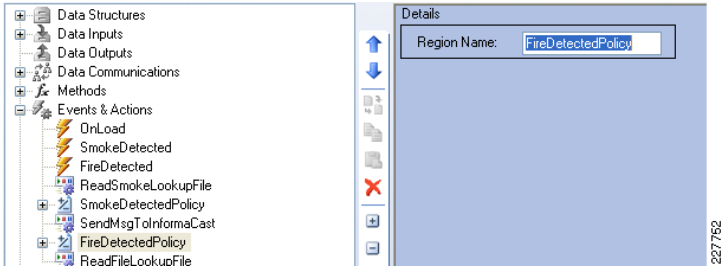
Events & Actions/Actions					
Action Name	**Policy Name**	**Type**	**Instance**	**Action**	**Return Value To**
FireAlarmIndex	FireDetected	Series	FireLookup	FindFirstRowIndexContaining (FieldIndex,CompareVal)	HoldRowIndex
GetFireMsg	FireDetected	Series	FireLookup	GetSeriesFieldValue(FieldName,RowIndex)	HoldRowIndex
SetBroadcastGroup	SmokeDetected	Variable	Group	Set Value(Value)	

14. For the previous three actions, configure the action parameters as shown in the following table:

Events & Actions/Actions Action ParametersEvents & Actions/Actions Action Parameters				
Action Name	**Parameter**	**Value Type**	**Custom Value/Value Of**	**Notes**
FireAlarmIndex	FieldIndex	Custom	0	First field in the series (field 0).
FireAlarmIndex	CompareVal	SeriesField	FireAlarms.Event	Series field holding the value of the alarm sent in the HTTP Get. This will be matched in the Fire Lookup Table.
GetFireMsg	FieldName	Custom	Message	Name of the field holding the messages to be played out for alarms in the Smoke Lookup Table
GetFireMsg	RowIndex	Variable	HoldRowIndex	Index of row corresponding to the alarm received. Looked up in previous step.
SetBroadcastGroup	Value	Custom	-1	Value of the Group created in InformaCast associated with Security phones. It can be determined by mousing over the Edit button in InformaCast for the Security Group you created.
SetBroadcastGroup	CompareVal	SeriesField	FireAlarms.Value	Series field holding the value sent in the trap.

15. Create a region with a name indicating this is setting up the parameters for the fire alarm (**FireDetectedPolicy**). Creating a region is optional, but improves readability of the system. Figure 81 shows the new region.

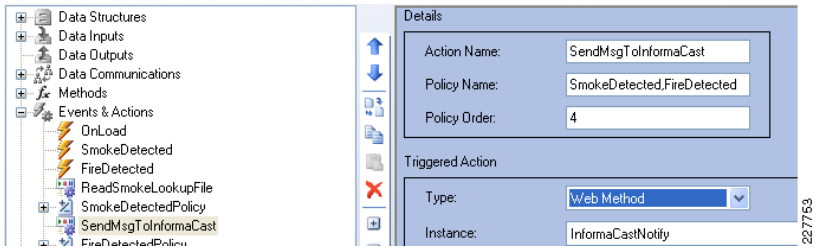
Figure 81 Add Policy - FireDetected



16. Once the region is created, move all related actions into the new region.
17. Add the FireDetected Policy to the **SendMsgToInformaCast** action created in the SNMP section above. See Figure 82.

Figure 82 Add Policy to SendMsgToInformaCast

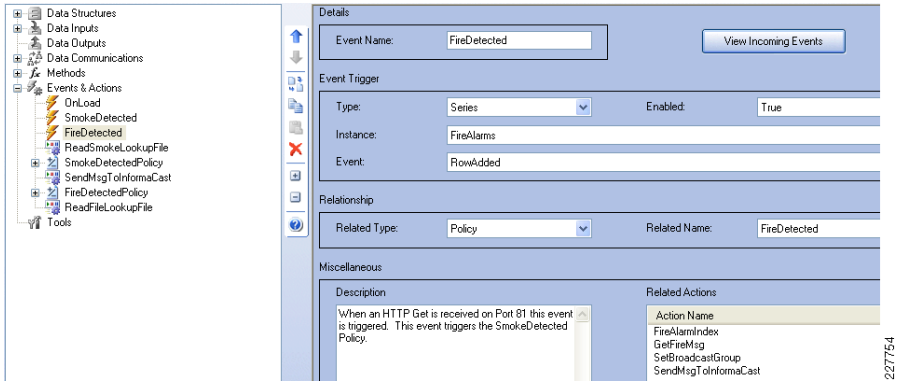
The following table lists the settings for Figure 82:



Events & Actions/Actions			
Action Name	**Policy Name**	**Type**	**Instance**
SendMsgToInformaCast	SmokeDetected,FireDetected	Web Method	InformaCastNotify

18. Create fire detected event as shown in Figure 83.

Figure 83 Add Event - Fire Detected



The following table lists the settings for Figure 83:

Events & Actions/Events					
Event Name	**Type**	**Instance**	**Event**	**Related Type**	**Related Name**
FireDetected	Series	FireAlarms	RowAdded	Policy	FireDetected

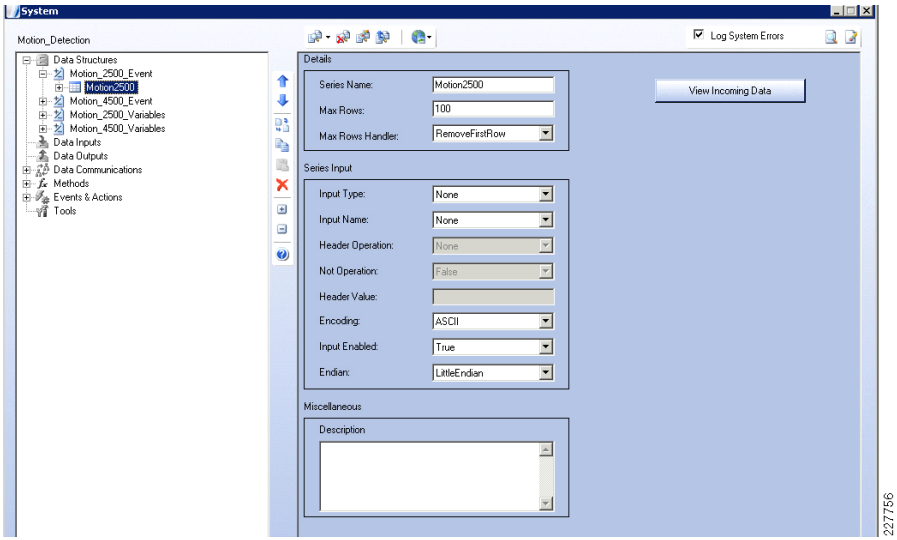
Motion Detection with a Cisco 2500 Camera

The data flow for the Cisco 2500 Series camera is shown in Figure 84.

Figure 84 Motion Detection with 2500 Series Camera

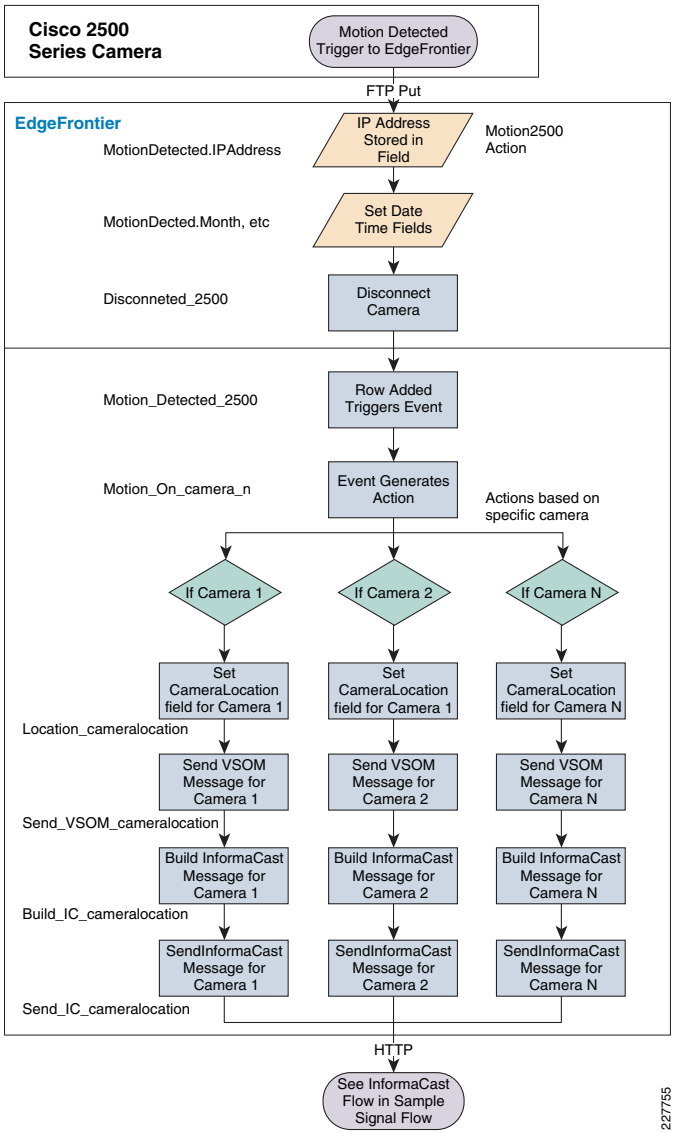
19. Add a series to hold the key values and text for the alarm. See Figure 85.

Figure 85 Add Series



The following table lists the settings for Figure 85:

Data Structures/Series			
Series Name	**Input Enabled**	**Remaining Values**	**Notes**
Motion2500	Yes	Use Default Values for all other fields	Use a Series Name that has meaning, it will make it easier later in the configuration

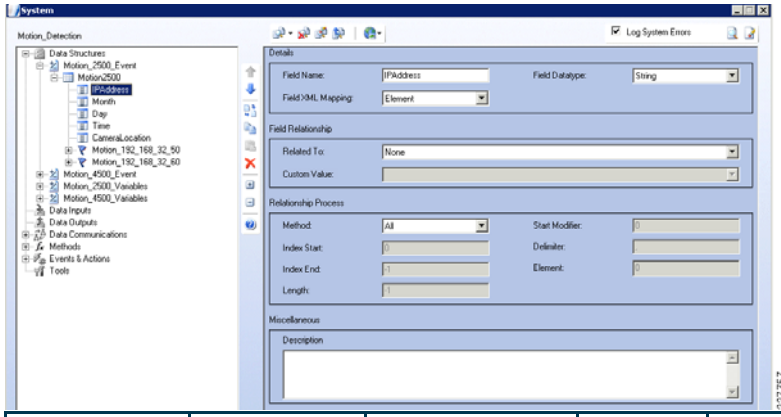


20. Add the fields to hold the key values and text for the alarm. See Figure 86.

Figure 86 Add Fields to Series

The following table lists the settings for Figure 86:

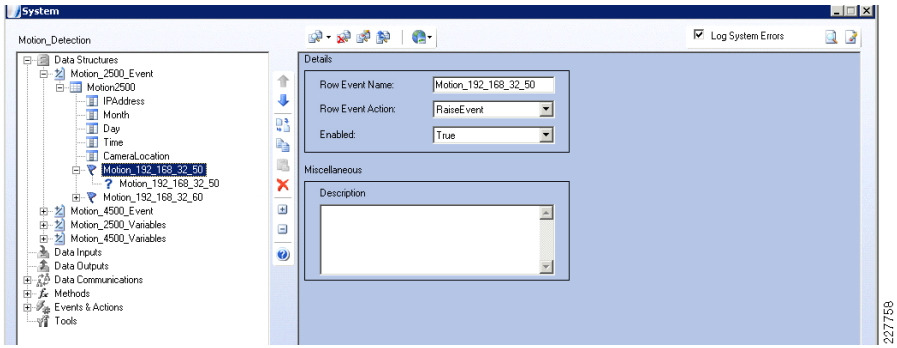
Data Structures/Series/Fields				
Field Name	**Field Data Type**	**Field XML Mapping**	**Related To**	**Method**
IP Address	String	Element	None	All



Month	String	Element	Custom	DateTime(MM)
Day	String	Element	Custom	DateTime(dd)
Time	String	Element	Custom	DateTime(HH:mm)
CameraLocation	String	Element	None	All

21. Right click the series just created and select Add Row Event to handle motion for each of the 2500 Series cameras on the network. See Figure 87 and the table that follows for the values. Repeat for each 2500 Series camera with motion detection.

Figure 87 Add Row Event

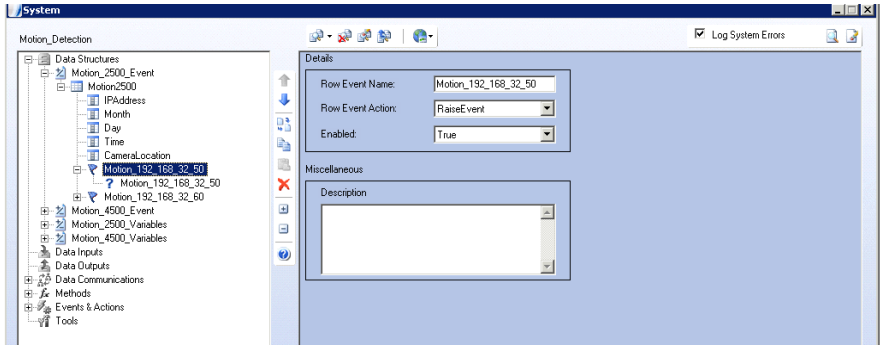


The following table lists the settings for Figure 87:

Data Structures/Series/RowEvent				
Row Event Name	**Row Event Action**	**Enabled**	**Description**	**Notes**
Motion_192_168_32_50	RaiseEvent	True	Optional	Use a Row Event Name that has meaning and uniquely identifies that camera that pertains to.

22. Right click the row event just created and select **Add Condition** to handle motion for each of the 2500 Series cameras on the network. See Figure 88 and the table that follows for the values.

Figure 88 Add Condition



The following table lists the settings for Figure 88:

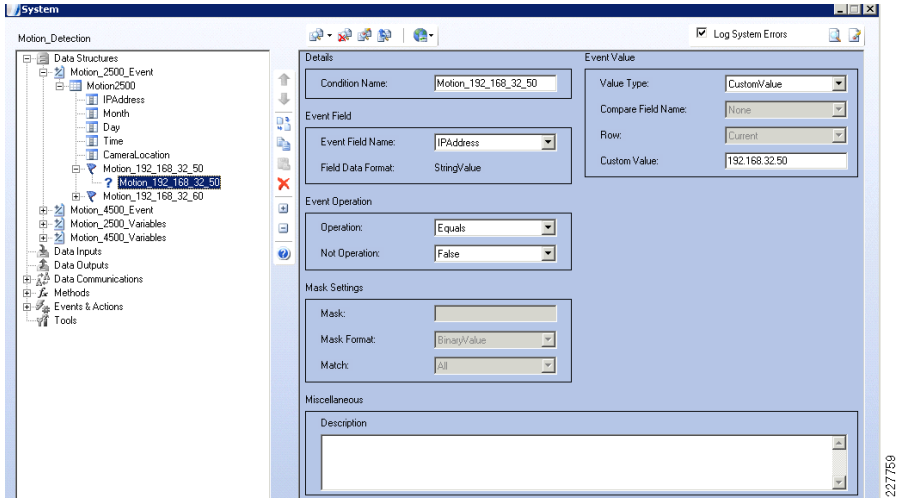
Data Structures/Series/Row Event/Condition					
Condition Name	**Value Type**	**Custom Value**	**Event Field Name**	**Operation**	**Not Operation**
Select True	Custom Value	IP Address of the associated camera	Select IP address from the drop down	Equals	False

23. Rich click on **Data Structures** and click on **Add Variables** to create variables to be used for 2500 Series camera motion detection. See Figure 89 and the table that follows for details.

Figure 89 Add Variables

The following table lists the settings for Figure 89:

Data Structures/Variables				
Variable Name	**Data Type**	**Default Value**	**Encoding**	**Notes**



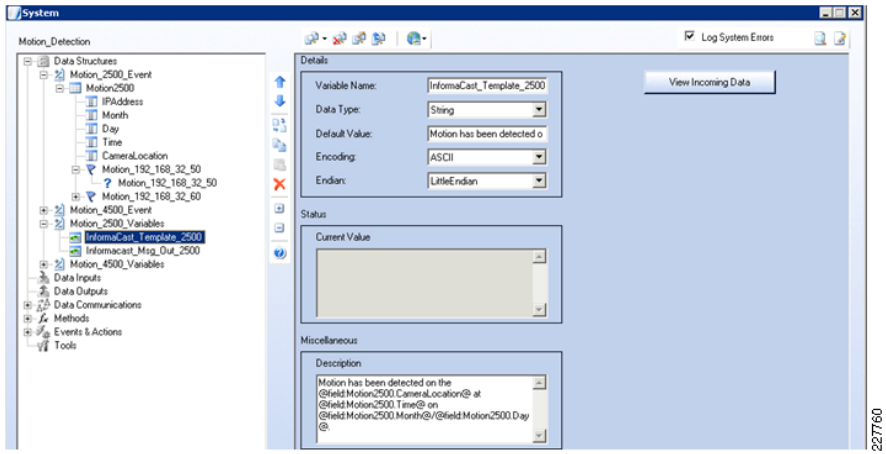
InformaCast_Template_2500	String	Motion has been detected on the @field:Motion2500.CameraLocation@ at @field:Motion2500.Time@ on @field:Motion2500.Month@/@field:Motion2500.Day@.	ASCII	The default value uses substitution parameters to insert values into the message. Format of the parameter is: @keyword:SeriesName.FieldName@
InformaCast_Msg_Out_2500	String	Leave Blank	ASCII	

24. Right click on **Events & Actions** and select **Add Action** to create a series of actions when motion is detected on all 2500 cameras. See Figure 90 and the tables that follow for details.

Figure 90 Add 2500 Actions

The following tables list the settings for Figure 90:

Action (Populates IP Address Field in Motion2500 Series)					
Action Name	**Policy Name**	**Policy Order**	**Type**	**Enabled**	**Instance**
Motion_2500	Motion_2500	1	Series	True	Motion_2500
Action	Parameter	Value Type	Value Of	Custom Value	Return Value to
AddSeriesRows([FieldParams])	IP address (value from Motion2500 series)	EventArgument	IPAddress (selects the actual IP address of the device connecting)	Blank	Blank



Action (Disconnects the FTP Connection Request from the 2500 Camera)					
Action Name	**Policy Name**	**Policy Order**	**Type**	**Enabled**	**Instance**
Dicsonnect_2500	Motion_2500	2	TCP Server	True	Cisco_2500_1
Action	Parameter	Value Type	Value Of	Custom Value	Return Value to
CloseAllConnections ()	Blank	Blank	Blank	Blank	Blank

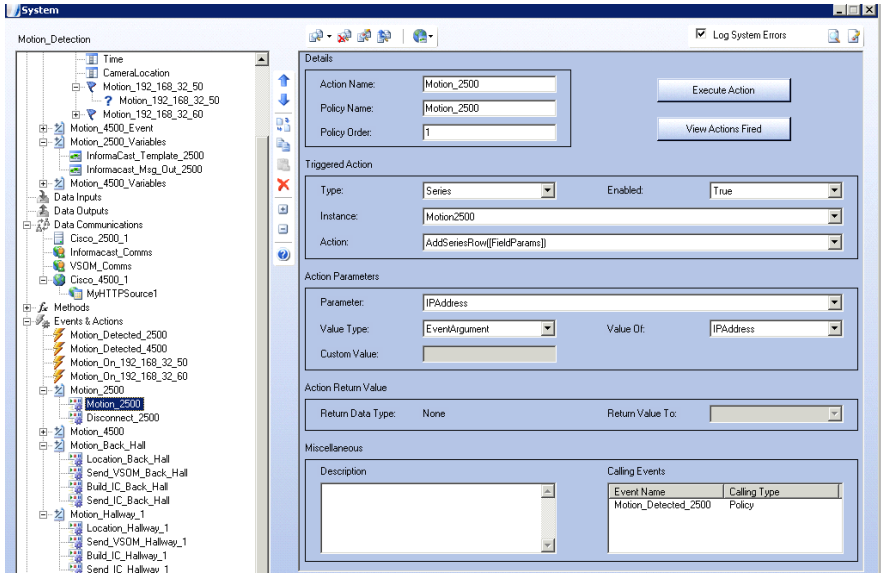
25. Right click on **Events & Actions** and select **Add Action** to create a series of actions when motion is detected on a specific camera. See Figure 91 and the tables that follow for details. This series of actions is repeated for each 2500 Series camera.

Figure 91 Add Specific 2500 Camera Actions

The following tables list the settings for Figure 91:

Add Action to value CameraLocation field in Motion2500 Series		
Action Name	Policy Name	Policy Order
Location_Back_Hall	Motion_192_168_32_50	1

Type	**Enabled**	**Instance**	**Action**
Series	True	Motion2500 (Relates to Motion2500 Series)	SetSeriesFieldLastValue(FieldName, Value)



Note	**Parameter**	**Value Type**	**Value Of**	**Custom Value**
Multiple Parameters have to be valued – Use Parameter Drop Down menu to select each	FieldName	Custom	Blank	CameraLocation (refers to CameraLocation Field in Motion2500 Series
	Value	Custom	Blank	Back Hall Camera (actual text value of location of camera)

Add Action to send soft trigger to VSOM Server		
Action Name	**Policy Name**	**Policy Order**
Send_VSOM_Back_Hall	Motion_192_168_32_50	1

Type	**Enabled**	**Instance**	**Action**
HTTP Client	True	VSOM_Comms (refers to Data Communications entry for VSOM	Execute(NewURI)

Parameter	Value Type	Value Of	Custom Value
NewURI	Custom	Blank	http://ipaddr/vsom/service/event_notify.php?id=13 Replace ipaddr with VSOM IP address Replace id=13 with actual soft trigger id for this camera

Add Action to build InformaCast message for Back Hall Camera		
Action Name	**Policy Name**	**Policy Order**
Build_IC_Back_Hall	Motion_192_168_32_50	2

Type	Enabled	Instance	Action
COMMON	True	STRING	GernerateStringFromText(TemplateText)

Parameter	Value Type	Value Of	Custom Value
Template Text	Variable	InformaCast_Template_2500 (Refers to variable field created)	Blank

Return Data Type	Return Value To
String	InformaCast_Msg_Out_2500 (Refers to variable field created to hold InformaCast Msg)

Add Action to send message to InformaCast Server		
Action Name	**Policy Name**	**Policy Order**
Send_IC_Back_Hall	Motion_192_168_32_50	3

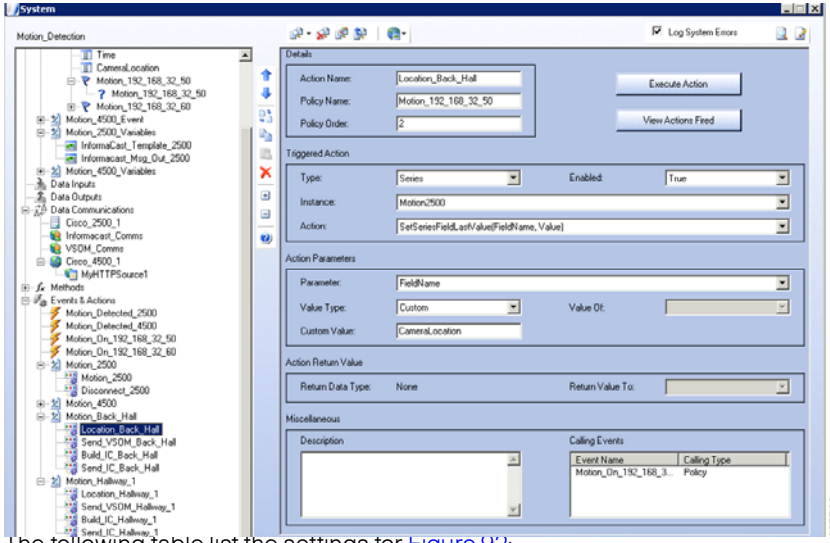
Type	Enabled	Instance	Action
Web Method	True	InformaCast_Dynamic_Msg (Refers to the Method created communicating with InformaCast Server	Invoke([Params])

Note	Parameter	Value Type	Value Of	Custom Value
Multiple Parameters have to be valued – Use Parameter Drop Down menu to select each	sendMessage WithDynamicText1.messageId	Custom	Blank	931 (Refers to shell message id created on InformaCast Server
	sendMessageWithDynamicText1.shortText	Variable	InformaCast_Msg_Out_2500 (Refers to variable created to hold InformaCast message)	Blank
	sendMessageWithDynamicText1.detailText	Custom	Blank	Optional text for detail message in InfomaCast message
	sendMessageWithDynamicText1.recipientGroupIds	Custom	Blank	-1 (Refers to Distribution group ID in InformaCast
	sendMessageWithDynamicText1.userLogin	Custom	Blank	ID created for sending messages in InformaCast
	sendMessageWithDynamicText1.userPassword	Custom	Blank	Password that goes with specified ID

26. Right click on Events & Actions and select Add Event to add the events necessary to track the motion on the 2500 Series cameras. The IP address is used to identify which camera has activity, and then a unique action for each camera because of the way the action is tracked. An alternative would be to use a look-up table similar to the SNMP setup in the fire and smoke detection scenarios.

See Figure 92 and the table that follows for details.

Figure 92 Add 2500 Events



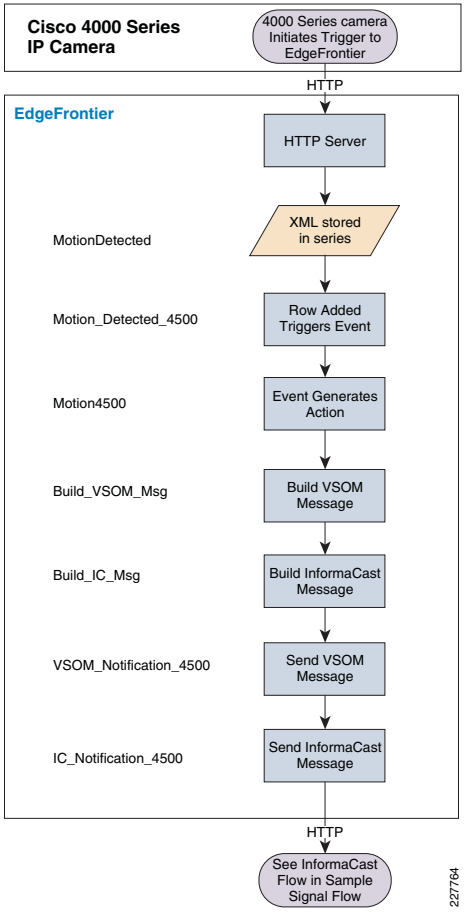
The following table list the settings for Figure 92:

Events						
Event Name	**Type**	**Enabled**	**Instance**	**Event**	**Related Type**	**Related Name**
Motion_Detected_2500	TCP Server	True	Cisco_2500_1 (Refers to Data Communications name created	Connection Established	Policy	Policy name for the Motion_2500 action
Motion_On_192_168_32_50	Row Event	True	Motion2500.motion_192_168_32_50 (Refers to Row Event created for this camera)	RowEvent Fired	Policy	Select the Policy used for motion on this camera
Unique event name for each camera used	Row Event	True	Select Row Event created for this camera	RowEvent Fired	Policy	Select the Policy used for motion on this camera

Motion Detection with a Cisco 4000 Series Camera

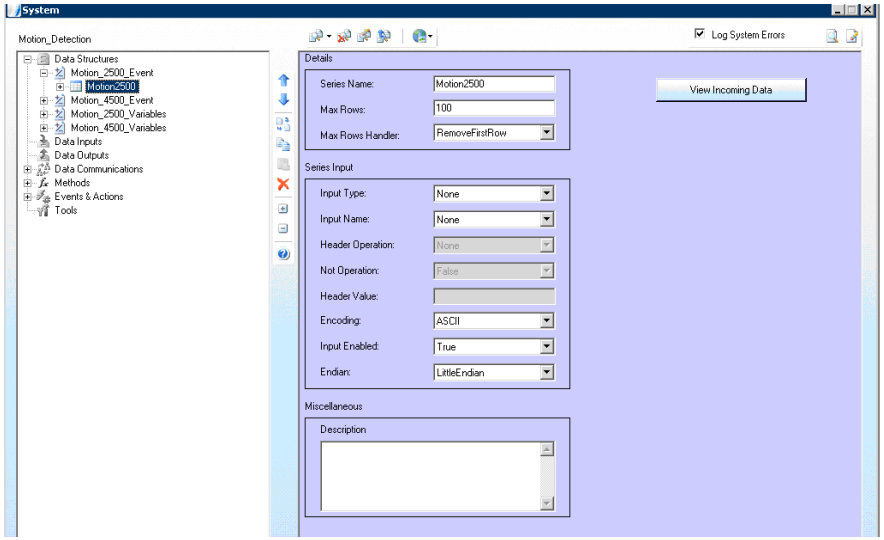
Figure 93 shows the flow of data with the 4000 Series camera.

Figure 93 Motion Detection with 4000 Series Camera



1. Right click on the **Data Structures** and select **Add a Series** to hold the key values and text for the alarm and for a series to hold fields to reformat the date and time from the camera. See Figure 94 and the table that follows for the values.

Figure 94 Add Series

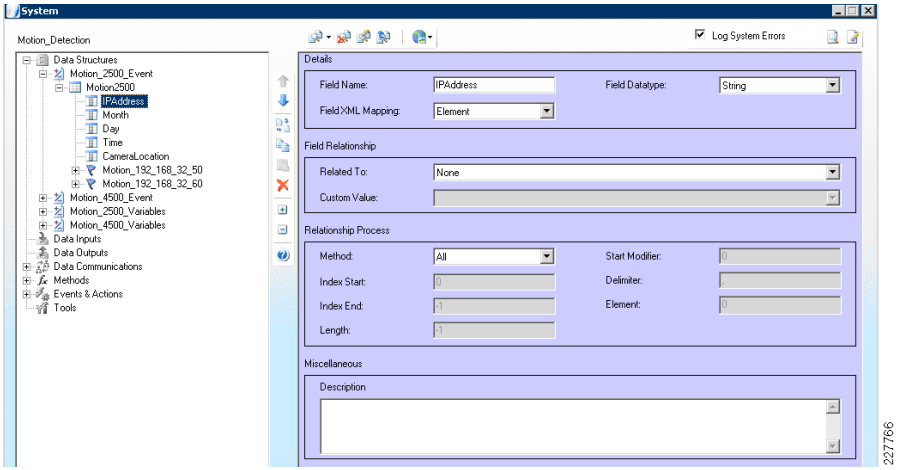


The following table list the settings for Figure 94:

Data Structures/Series			
Series Name	**Input Enabled**	**Input Type**	**Input Name**
MotionDetected	True	HTTP Server	Cisco_4500_1 (Refers to the HTTP Server created to listen for connections from the 4000 series cameras)
CameraDateTime	True	Series	MotionDetected (Refers to Series created above)

2. Right click the **MotionDetected** series just created and select **Add Fields** to hold the key values and text for the alarm. Then, right click the **CameraDateTime** series and select **Add Fields** to hold the key values for reformatting the camera date and time. See Figure 95 and the tables that follows for the values.

Figure 95 Add Fields to Series



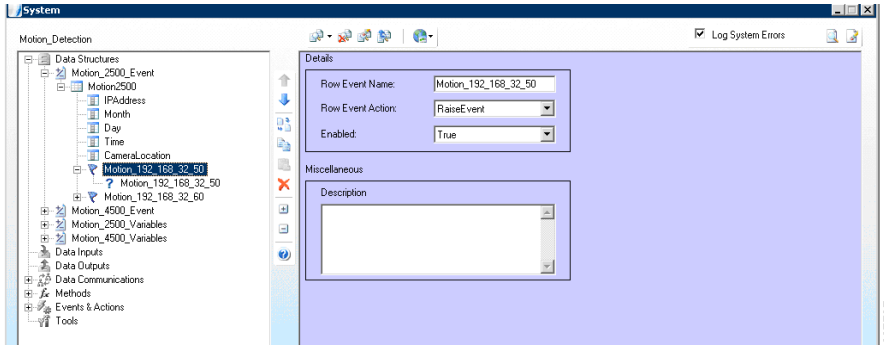
The following tables list the settings for Figure 95:

MotionDetected Fields					
Field Name	**Field Data Type**	**Field XML Mapping**	**Related To**	**Method**	**Element** **(Refers to the xml field defined in the string on the 4000 series camera)**
deviceID	String	Element	Document	XPathElement	//deviceID
deviceName	String	Element	Document	XPathElement	//deviceName
ipAddress	String	Element	Document	XPathElement	//ipAddress
macAddress	String	Element	Document	XPathElement	//macAddress
dateTime	String	Element	Document	XPathElement	//dateTime

CameraDateTime Fields							
Field Name	**Field Data Type**	**Field XML Mapping**	**Related To**	**Method**	**Start Modifier**	**Index Start**	**Length**
deviceID	Object	Element	DeviceID	All			
CameraMonth	Object	Element	dateTime	Start_Length	0	0	2
CameraDay	Object	Element	dateTime	Start_Length	0	2	2
CameraYear	Object	Element	dateTime	Start_Length	0	4	4
Cameratime	Object	Element	dateTime	Start_Length	0	9	5

3. Right click the series you just created and select **Add Row Event** to handle motion for the 4000 Series cameras. See Figure 96 and the table that follows for the values.

Figure 96 Add Row Event

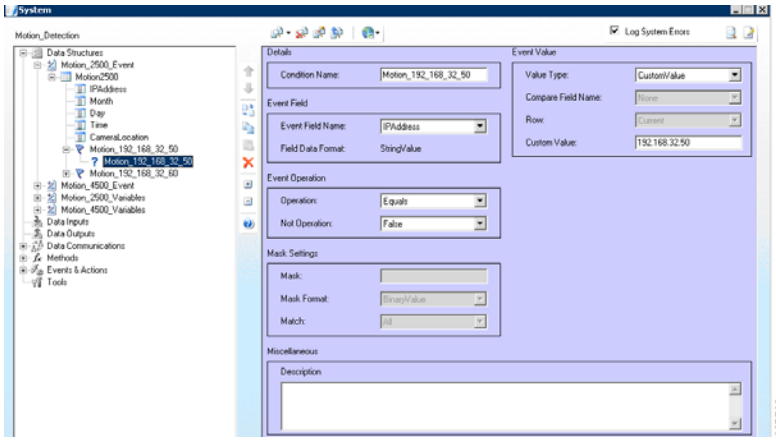


The following table list the settings for Figure 96:

Data Structures/Series/RowEvent				
Row Event Name	**Row Event Action**	**Enabled**	**Description**	**Notes**
Motion_Detected	RaiseEvent	True	Optional	Use a Row Event Name that has meaning and uniquely identifies that camera that pertains to.

4. Right click the **Row Event** just created and select **Add Condition** to handle motion for the 4000 Series cameras. See Figure 97 and the table that follows for the values.

Figure 97 Add Condition

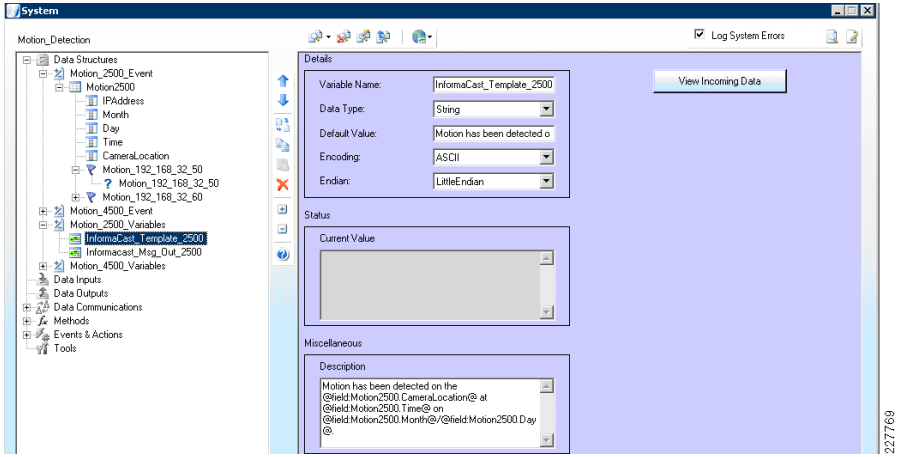


The following table list the settings for Figure 97:

Data Structures/Series/Row Event/Condition					
Condition Name	**Value Type**	**Custom Value**	**Event Field Name**	**Operation**	**Not Operation**
Motion	Custom Value	Blank	None	Equals	False

5. Right click on **Data Structures** and click on **Add Variables** to create variables to be used for 4000 Series camera motion detection. See Figure 98 and the table that follows for details.

Figure 98 Add Variables



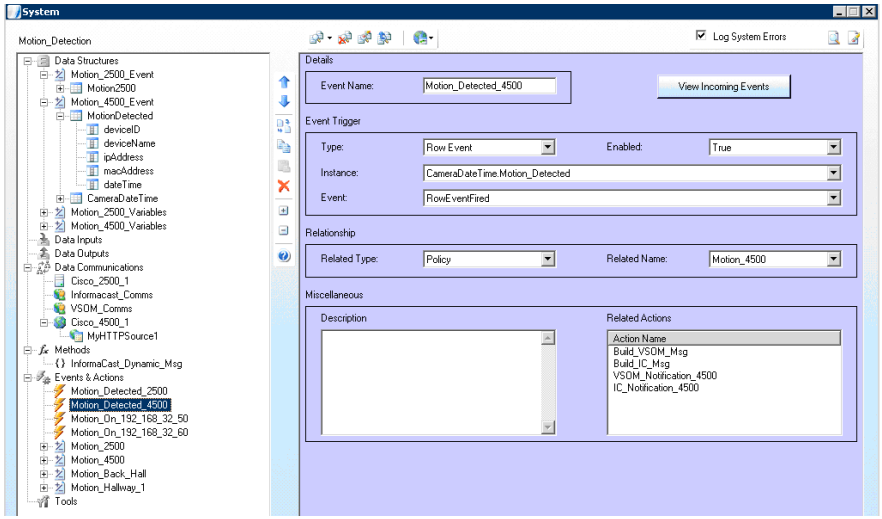
The following table list the settings for Figure 98:

Variable Name	Data Type	Default Value	Notes
InformaCast_Template_4500	String	Motion has been detected on the @field:MotionDetected.deviceName@ at @field:CameraDateTime.CameraTime @ on @field:CameraDateTime.CameraMonth@/@field:CameraDateTime.CameraDay@.	The Default value uses substitution parameters to insert values into the message. Format of the parameter is: @keyword:SeriesName.FieldName@
InformaCast_Msg_Out_4500	String	Leave Blank	

VSOM_MSG_IN_4500	String	http://192.168.200.2/vsom/service/event_notify.php?id=deviceID	An action will occur that will change the deviceID value to that contained in the xml string submitted by the camera
VSOM_MSG_OUT_4500	String	Blank	Holds the convertes VSOM Message

6. Right click on **Events & Actions** and select **Add Event** to create an event to handle motion detected on the 4000 Series cameras. See Figure 99 and the table that follows for details.

Figure 99 Add 4500 Motion Event

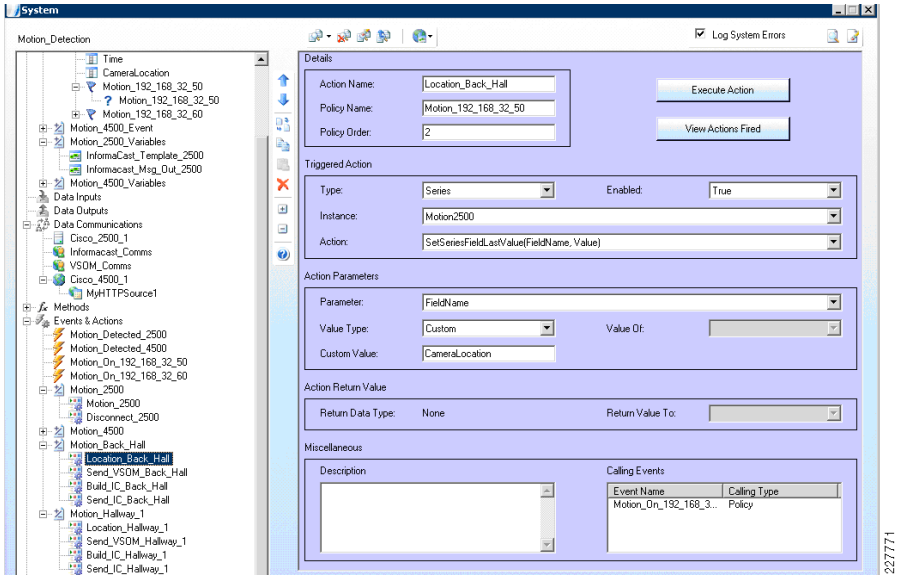


The following table list the settings for Figure 99:

Events						
Event Name	**Type**	**Enabled**	**Instance**	**Event**	**Related Type**	**Related Name**
Motion_Detected_4500	Row Event	True	CameraDateTime.Motion_Detected	RowEventFired	Policy	Policy name for the Motion_4500 action

7. Right click on **Events & Actions** and select **Add Action** to create a series of actions when motion is detected on the 4000 Series cameras. See Figure 100 and the tables that follow for details.

Figure 100 Add 4000 Series Camera Actions



The following tables list the settings for Figure 100:

Add Action to build VSOM message for 4000 Series cameras		
Action Name	**Policy Name**	**Policy Order**
Build_VSOM_Msg	Motion_4500	1

Type	**Enabled**	**Instance**	**Action**
Common	True	STRING	Replace(Text, OldCharacters, NewCharacters

Note	**Parameter**	**Value Type**	**Value Of**	**Custom Value**
Multiple Parameters have to be valued – Use Parameter Drop Down menu to select each	Text	Variable	VSOM_MSG_IN_4500	Blank
	OldCharacters	Custom	Blank	deviceID
	NewCharacters	SeriesField	MotionDetected.deviceID	blank

Return Value To
VSOM_MSG_OUT_4500

Add Action to build InformaCast message for 4000 Series cameras		
Action Name	**Policy Name**	**Policy Order**
Build_IC_Msg	Motion_4500	1

Type	Enabled	Instance	Action
Common	True	STRING	GenerateStringFromText(TemplateText)

Parameter	Value Type	Value Of	Custom Value
TemplateText	Variable	InformaCast_Template_4500	Blank

Return Value To
InformaCast_Msg_Out_4500

Add Action to send soft trigger to VSOM Server		
Action Name	**Policy Name**	**Policy Order**
VSOM_Notification_4500	Motion_4500	2

Type	Enabled	Instance	Action
HTTP Client	True	VSOM_Comms (references Data Communications entry for VSOM)	Execute(NewURI)

Parameter	Value Type	Value Of	Custom Value
NewURI	Custom	VSOM_MSG_OUT_4500	Blank

Add Action to send message to InformaCast Server		
Action Name	**Policy Name**	**Policy Order**
IC_Notification_4500	Motion_4500	2

Type	Enabled	Instance	Action
Web Method	True	InformaCast_Dynamic_Msg (References the Method created for communicating with InformaCast Server)	Invoke([Params])

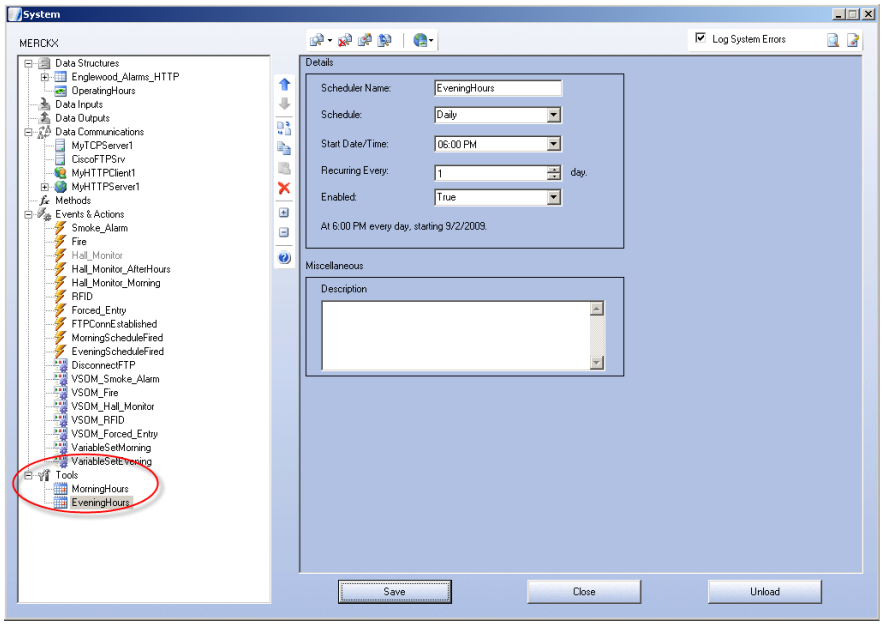
Note	Parameter	Value Type	Value Of	Custom Value
Multiple Parameters have to be valued – Use Parameter Drop Down menu to select each	sendMessage WithDynamicText1. messageId	Custom	Blank	931 (Refers to shell message id created on InformaCast Server
	sendMessage WithDynamicText1. shortText	Variable	InformaCast_Msg_ Out_4500 (Refers to variable created to hold InformaCast message)	Blank
	sendMessage WithDynamicText1. detailText	Custom	Blank	Optional text for detail message in InfomaCast message
	sendMessage WithDynamicText1. recipientGroupIds	Custom	Blank	-1 (References distribution group ID in InformaCast)
	sendMessage WithDynamicText1. userLogin	Custom	Blank	ID created for sending messages in InformaCast
	sendMessage WithDynamicText1. userPassword	Custom	Blank	Password that goes with specified ID

Notifications to Augusta EdgeFrontier Based on Time of Day

Augusta EdgeFrontier may be configured to recognize events from IP cameras and, based on the time of the day, trigger an event for VSOM. For example, for some video cameras, recording can be disabled between 6:00am and 6:00pm, when school activity is at its highest and enabled at all other times. Maintenance periods can also be configured follow the same guidelines.

8. To configure Augusta EdgeFrontier to process different events based on the time-of-day, create a Scheduler with the appropriate time definitions. In Figure 101, a scheduler has been created for evening hours starting at 6:00pm. Create a similar Scheduler for the morning hours.

Figure 101 Evening Hours Schedule

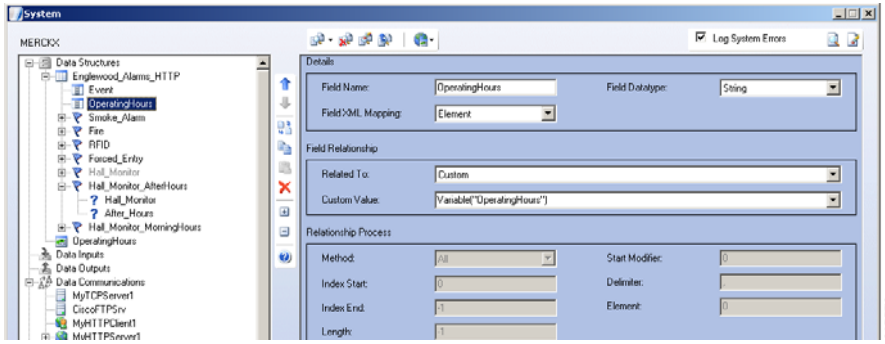


The following table list the settings for Figure 101:

Tools/Scheduler			
Scheduler Name	**Schedule**	**Start Date/Time**	**Recurring Every**
MorningHours	Daily	06:00AMs	1
Evening Hours	Daily	06:00PM	1

9. Create a series named *OperatingHours* and specify the **Custom Value** as shown in Figure 102. Based on the Schedule settings, the *OperatingHours* will be set to Morning or Evening.

Figure 102 OperatingHours Series

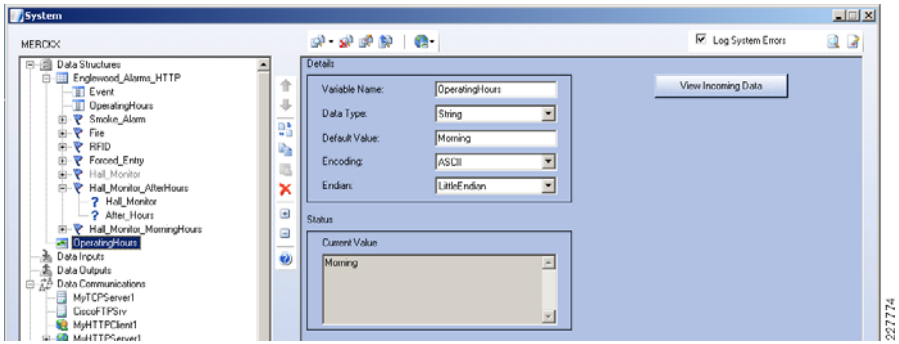


The following table list the settings for Figure 102:

Data Structures/Series				
Field Name	**Field Datatype**	**Field XML Mapping**	**Related To**	**Custom Value**
OperatingHours	String	Element	Custom	Variable("OperatingHours")

10. Create a variable named *OperatingHours* as shown in Figure 103. The variable is configured with a default value of "Morning". The current value of the *OperatingHours* is displayed under the current value status area.

Figure 103 OperatingHours Variable

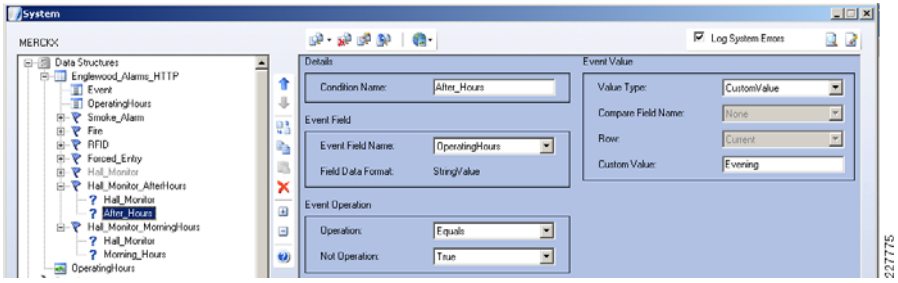


The following table list the settings for Figure 103:

Data Structures/Variable				
Variable Name	**Data Type**	**Default Value**	**Encoding**	**Endian**
OperatingHours	String	Morning	ASCII	LittleEndian

11. Create row events for each time period, MorningHours and AfterHours, as shown in Figure 104. Note the Custom Value setting of Evening.

Figure 104 Row Events for AfterHours

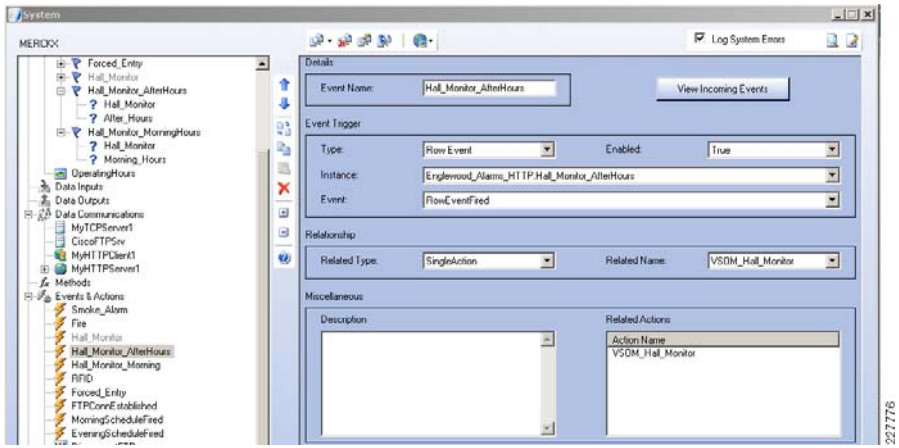


The following table list the settings for Figure 104:

Data Structures/Series/Row Event						
Row Event Name	**Row Event Action**	**Condition Name**	**Event Field Name**	**Value Type**	**Custom Value**	**Not Operation**
Hall_Monitor_AfterHours	RaiseEvent	Hall_Monitor	Event	CustomValue	HALL_MONITOR	FALSE
		After_Hours	Operating_Hours	CustomValue	Evening	FALSE
Hall_Monitor_MorningHours	RaiseEvent	Hall_Monitor	Event	CustomValue	HALL_MONITOR	FALSE
		Morning_Hours	OperatingHours	CustomValue	Morning	TRUE

a. Under **Events & Actions**, create events for each time range. Figure 105 shows an event defined for after hours, linked to the VSOM_Hall_Monitor action.

Figure 105 After Hours Event

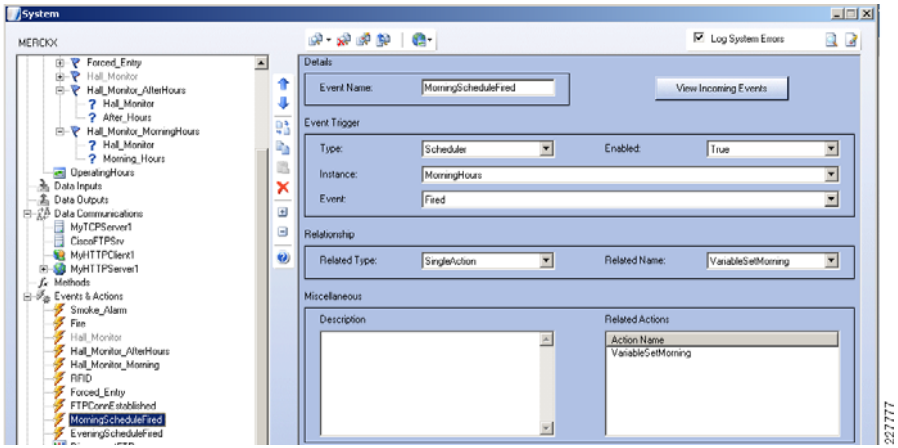


The following table list the settings for Figure 105:

Events & Actions/Events						
Event Name	**Type**	**Enabled**	**Instance**	**Event**	**Related Type**	**Related Name**
Hall_Monitor_AfterHours	Row Event	TRUE	Englewood_Alarms_HTTP.Hall_Monitor_AfterHours	RowEventFired	SingleAction	VSOM_Hall_Monitor
Hall_Monitor_Morning	Row Event	TRUE	Englewood_Alarms_HTTP.Hall_Monitor_MorningHours	RowEventFired	SingleAction	VSOM_Hall_Monitor

12. In order to set the variables, an event must be created and fired when the Scheduler takes place (morning or evenings). Figure 106 shows how the variable is set to *MorningHours* when the Schedule reaches the specified time.

Figure 106 ScheduleFired

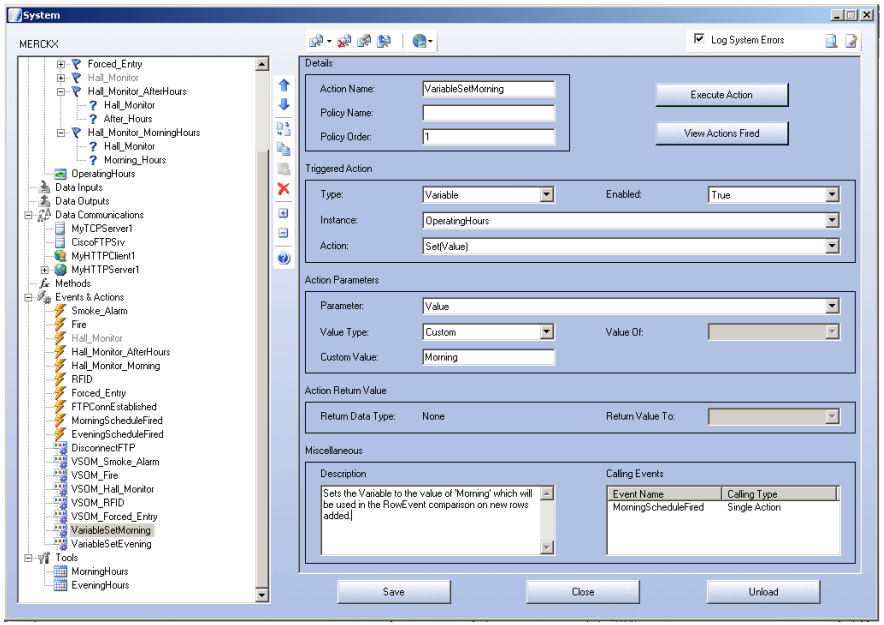


The following table list the settings for Figure 106:

Events & Actions/Events						
Event Name	**Type**	**Enabled**	**Instance**	**Event**	**Related Type**	**Related Name**
MorningScheduleFired	Scheduler	TRUE	MorningHours	Fired	SingleAction	VariableSetMorning
EveningScheduleFired	Scheduler	TRUE	EveningHours	Fired	SingleAction	VariableSetEvening

13. Associate the event with an action. In Figure 107, the *Set (Value) Action* is configured for “Morning”.

Figure 107 Variable Set



The following table list the settings for Figure 107:

Events & Actions/Actions

Action Name	Policy Order	Type	Instance	Action	Parameter	Value Type	Custom Value
VariableSetMorning	1	Variable	OperatingHours	Set(Value)	Value	Custom	Morning
VariableSetEvening	1	Variable	OperatingHours	Set(Value)	Value	Custom	Evening

To define other time periods, such as the maintenance window, follow the same steps specifying a different Scheduler fire time.

Lab and Test Overview

Test Overview

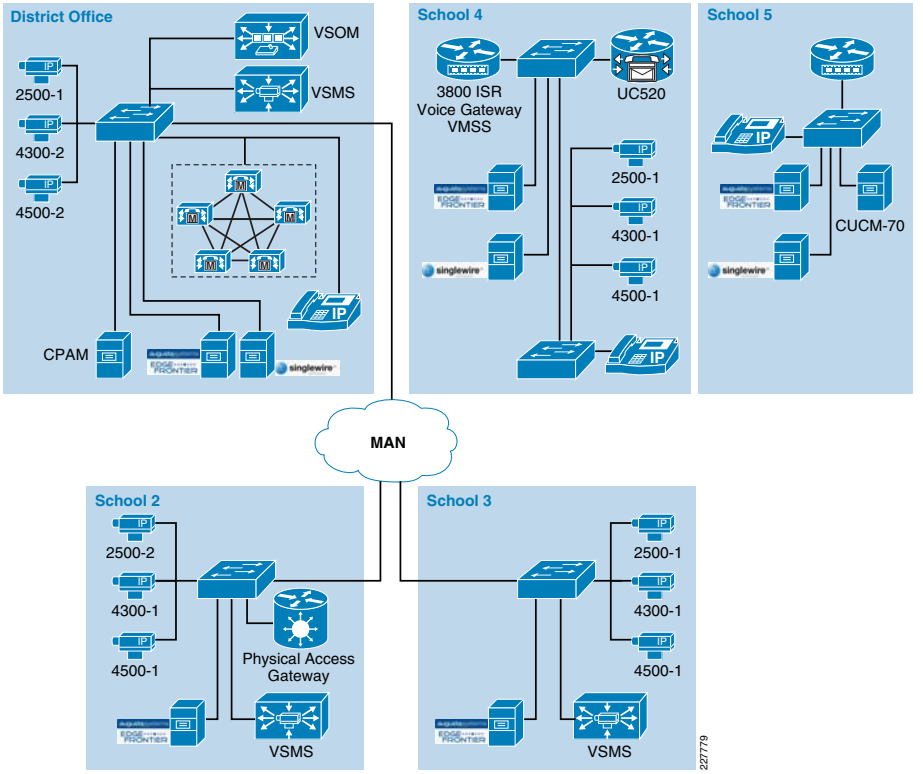
The test goals were to simulate a school environment with different locations and diverse requirements. The emphasis was on configuring different devices to generate events and provide the intelligence to integrate those security events with a correlation engine capable of communicating with different, such as Singlewire InformaCast or the Cisco Video Surveillance Manager.

The lab environment includes a district office and different schools. The goal of the district office was to centralize as much as possible the video surveillance, access control, and the Unified Communications servers. By centralizing the main applications, the deployment scenarios are simplified at the school level.

This application deployment guide testing did not focus on testing Layer-2 or Layer-3 features typical of a campus or branch office deployment, since those have been extensively documented in other solutions.

Figure 108 shows the five different locations configured for the test environment.

Figure 108 Lab Environment



Cisco Video Surveillance

A single Cisco video Surveillance Operations Manager server was deployed at the district office in order to manage the Media Servers deployed at the schools. A single VSOM server is capable of managing cameras, events and media servers located at different schools. The Media Servers were also deployed locally at each school in order to archive video from local cameras and to reduce bandwidth requirements across the MAN.

Each Media Server acts as a proxy to the local IP cameras and possible viewers. Video can still be viewed by any location if required and the proper user permissions are in place.

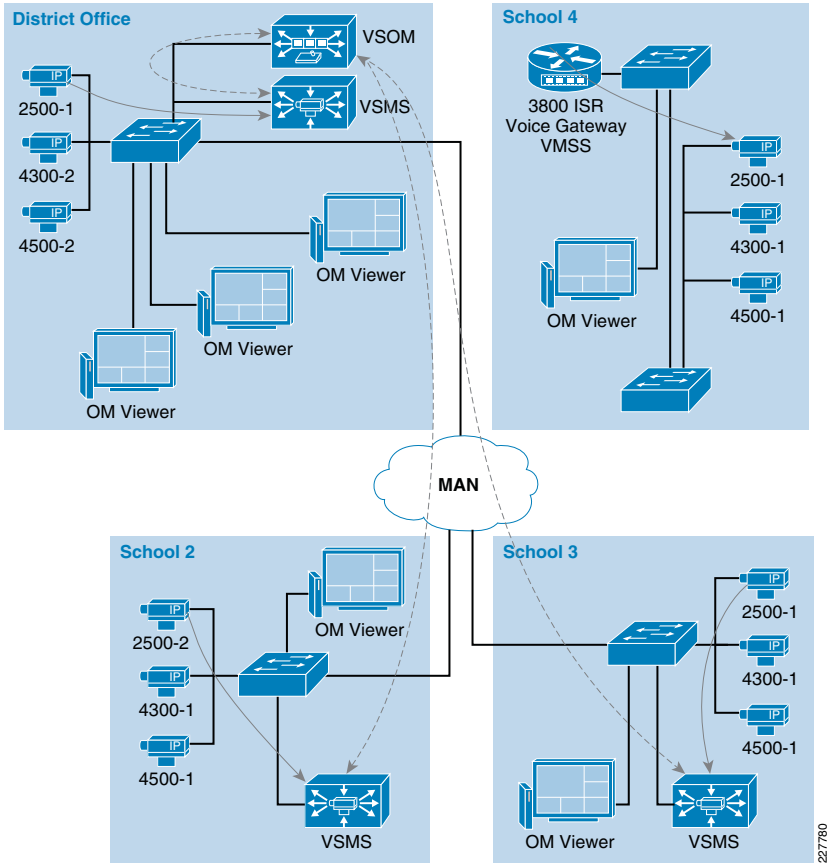
School 2 and School 3 are directly connected to the District Office while School 4 and School 5 are completely standalone. The Cisco ISR router in School 4 is responsible for providing voice gateway capabilities, routing within the school, and for hosting the Video

Management and Storage Module (VMSS). School 4 and 5 provide event messaging between Singlewire InformaCast, Augusta EdgeFrontier, and the Cisco Unified Communications. School 5 does not include video surveillance devices.

Figure 109 shows the interaction between the VSOM at the district office and a three Media Servers local to the district office, School 2, and School 3. The VSOM provides proper access to all cameras and provides a consistent interface for all of viewers.

Figure 109 also shows how viewers are deployed at each location and how cameras interface with the local VSMS which acts like a proxy for live and archived video.

Figure 109 Cisco Video Surveillance



Cisco Physical Access Control

A single CPAM server was deployed at the district office to manage the access gateways at different schools. An access gateway and door hardware were installed at School 2. Since the testing focused on on integrating different components, rather than scalability, access gateways were not installed at each school. The door hardware includes a card reader, a lock, a door sensor, a button used to request for exit, and an alarm. Using forced entry as an example, the access gateway reports the incident to CPAM, CPAM notifies Augusta EdgeFrontier, and Augusta EdgeFrontier triggers VSOM and Singlewire InformaCast. These interactions are shown in Figure 110.

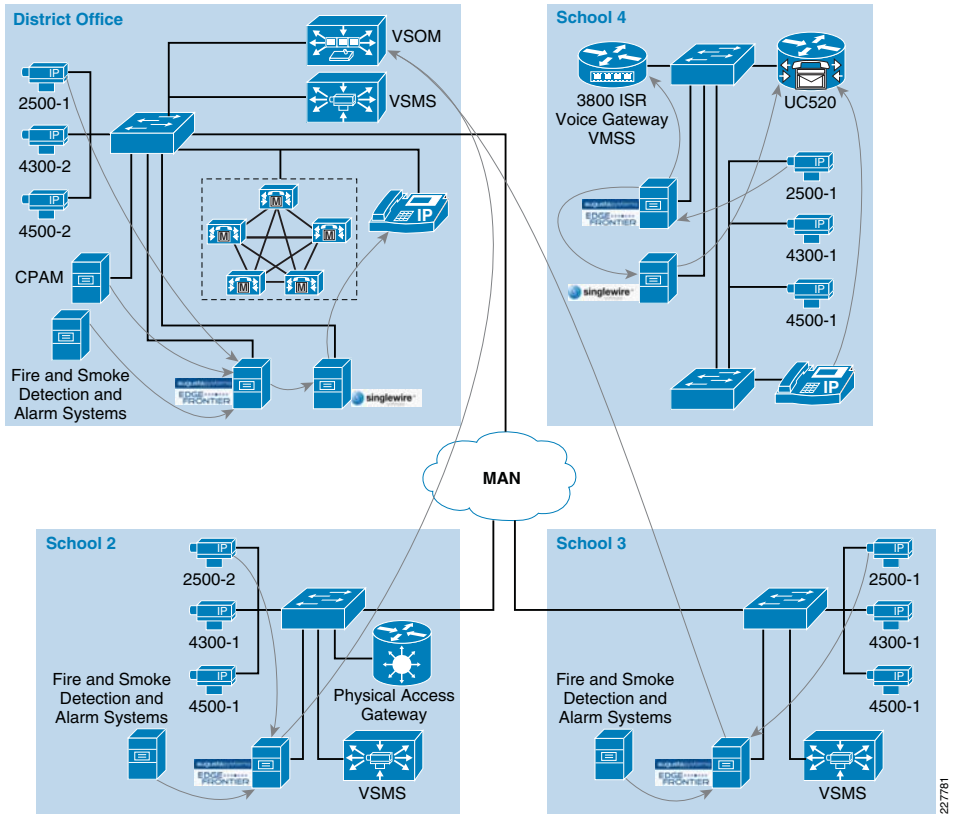
Augusta EdgeFrontier and Singlewire InformaCast

An Augusta EdgeFrontier engine was deployed at each school location in order to provide localized device configuration and processing of alarms and events. Each Augusta EdgeFrontier engine received alarms from IP cameras, access control systems, and fire and smoke detection systems.

Based on the alarm type, notifications were sent to VSOM, Singlewire InformaCast, or CPAM and in turn those systems acted according to predefined actions, such as paging, video archiving, etc.

Figure 110 shows the interaction between these systems and how Augusta EdgeFrontier receives alarms at each location.

Figure 110 Augusta EdgeFrontier Interaction



Hardware/Software

Table 1 and Table 2 show the different devices and releases used during the solution testing.

Table 1 Device and Software versions for Multi-Site Deployment

Device	Location	Software Release
Cisco VSOM	School District Office	4.2.0-12
Cisco VS Media Server	School District Office/Schools	6.2.0-15d
Cisco VSBase	School District Office	6.2.0-15d
Cisco 2500 IP Camera	School District Office/Schools	Firmware version 2.1.2
Cisco 4300 IP Camera	School District Office/Schools	Firmware version 1.0.1
Cisco 4500 IP Camera	School District Office/Schools	Firmware version 1.0.1
Cisco CPAM	School District Office	1.1.0(0.2.416)
Augusta EdgeFrontier	Client and Engine	4.3.0.1
Cisco Access Gateway	Schools	1.1.0(0.2.416)
Cisco Unified Communications Manager	School District Office	7.0.1.10000-19
Singlewire InformaCast Server Installed as VM guest	School District Office	7.0

Table 2 Device and Software Versions for Single-Site Deployment

Device	Location	Software Release
NME-VMSS2-HP32	School 4	SW-VMSS-K9-2.2
NME-ISS	School 4	SW-ISS-K9-1.0
Cisco 3845	School 4	C3845-entservices-mz.124-15.T3
Cisco WS-C3750G-24PS	School 4, Core switch	C3750-advipservicesk9-mz.122-46.SE
Cisco WS-C3750G-24PS	School 4, Distribution Switch	C3750-ipbase-mz.122-35.SE5
Cisco UC520-16U-4FXO-K9	School 4 – Cisco Unified Communications Manager Express	Uc500-advipservicesk9-mz.124-20.T2
Cisco 2500 IP Camera	School 4	Firmware version 2.1.2
Cisco 4300 IP Camera	School 4	Firmware version 1.0.1
Cisco 4500 IP Camera	School 4	Firmware version 1.0.1
Cisco CP-7961G-GE	School 4	SCCP41.8.4-2S
Cisco CP-7970G	School 4	SCCP70.8-4-2S
Cisco MCS7835 Intel Xeon 3.4 Ghz 3.5 GB RAM	School 4	MS Windows Server 2003 R2 Service Pack 2 VMWare Server V6.5 – win32-x86
Augusta EdgeFrontier Server Installed as VM guest	School 4	V4.2.0.20
Singlewire InformaCast Server Installed as VM guest	School 4	V7.0

Appendix A—Reference Documents

- Service Ready Architecture Design Guide
  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns826/landing_srArchit_edu.html

Cisco Physical Access Control

- Cisco Physical Access Manager Appliance User Guide, Release 1.1.0
  http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpam/1_1_0/english/user_guide/cpam_ug_1_1_0.html
- Cisco Physical Access Gateway User Guide, Release 1.1.0
  http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpag/gateway/1_1_0/english/user_guide/cpag_ug_1_1_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 Unified Communications Manager Express Install and Upgrade Guides
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_installation_guides_list.html

Partner Products

- Singlewire InformaCast Product Information:
  http://www.singlewire.com/informacast.html
- Singlewire InformaCast Support:
  http://www.singlewire.com/s_informacast.html
- Augusta Systems Product Information:
  http://www.augustasystems.com/Products/Overview.htm