CHAPTER 5

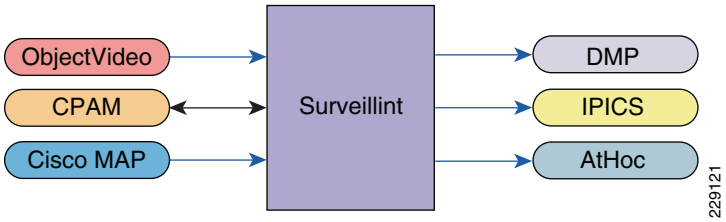
Integrating the Applications

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

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

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

Figure 5-1 Interactions between Surveillint and Other Components



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

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

The following procedures are recommended for integrating multiple technologies:

Step 1 Select the components and an integration application.

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

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

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

Step 5 Integrate each component with the integration application.

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

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

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

Table 5-1 List of Integration Examples

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

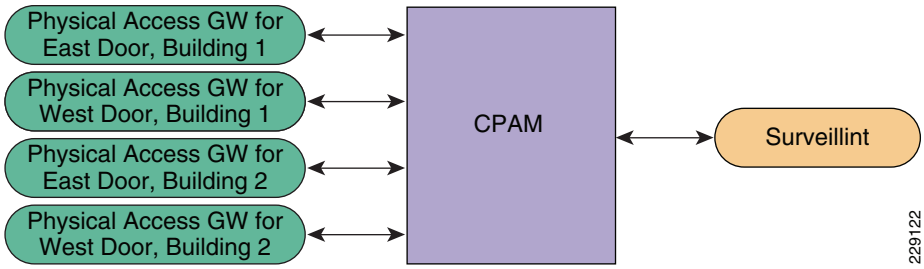
CPAM Integration

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

Integrating CPAM and Surveillint

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

Figure 5-2 Four Doors Connected to CPAM



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

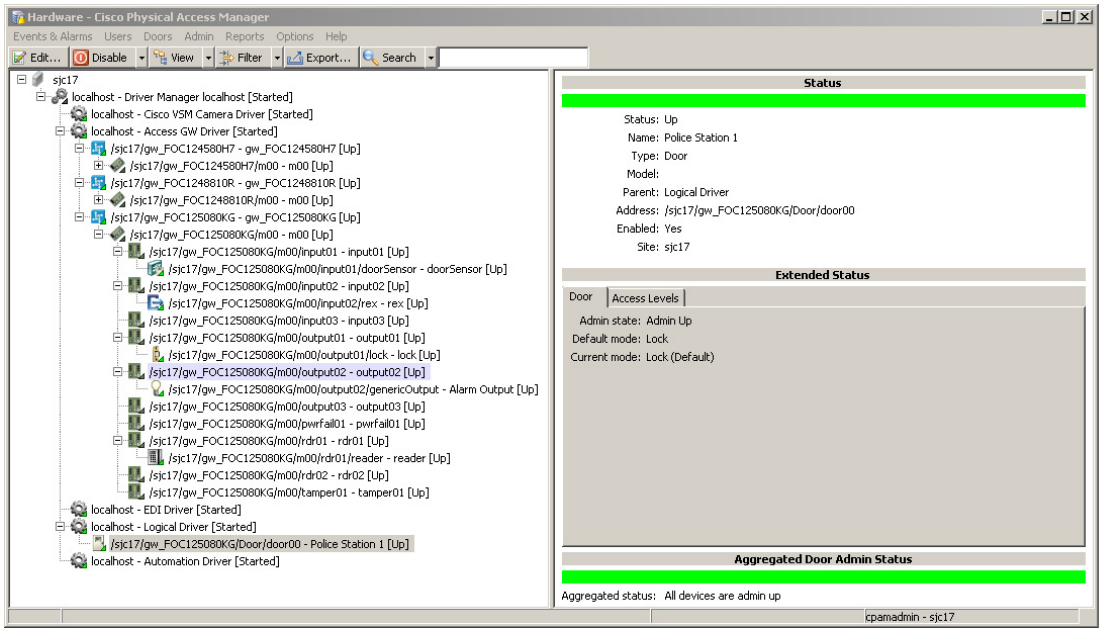
In short, from the perspective of Surveillint, one door equals one Surveillint "sensor".

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

Checkpoints Before Integration

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

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



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

The integration includes the following steps:

Step 1 Establish connection between CPAM and Surveillint.

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

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

Step 4 Configure Surveillint to receive alerts from CPAM.

Step 5 Configure Surveillint to send incident notifications.

Establishing the Connection between CPAM and Surveillint

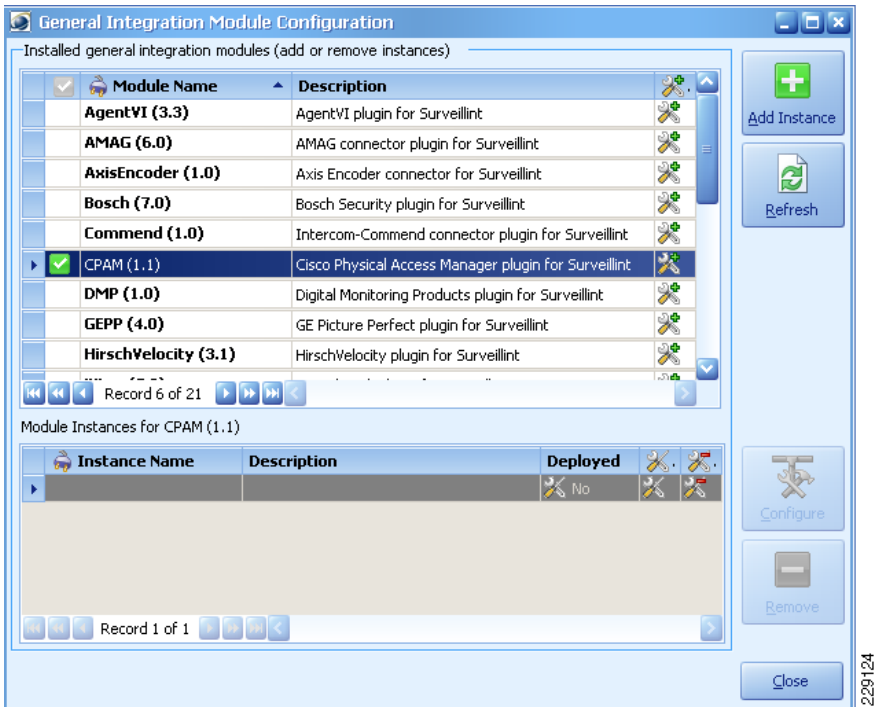
Establishing the connection between CPAM and Surveillint is performed on the Surveillint server through the Event Integration Module. This requires specifying the following information about CPAM: IP address, web service URL, and login. Perform the following steps:

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

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

Note Surveillint supports both CPAM version 1.1 and 1.2.

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



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

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

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

Troubleshooting

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

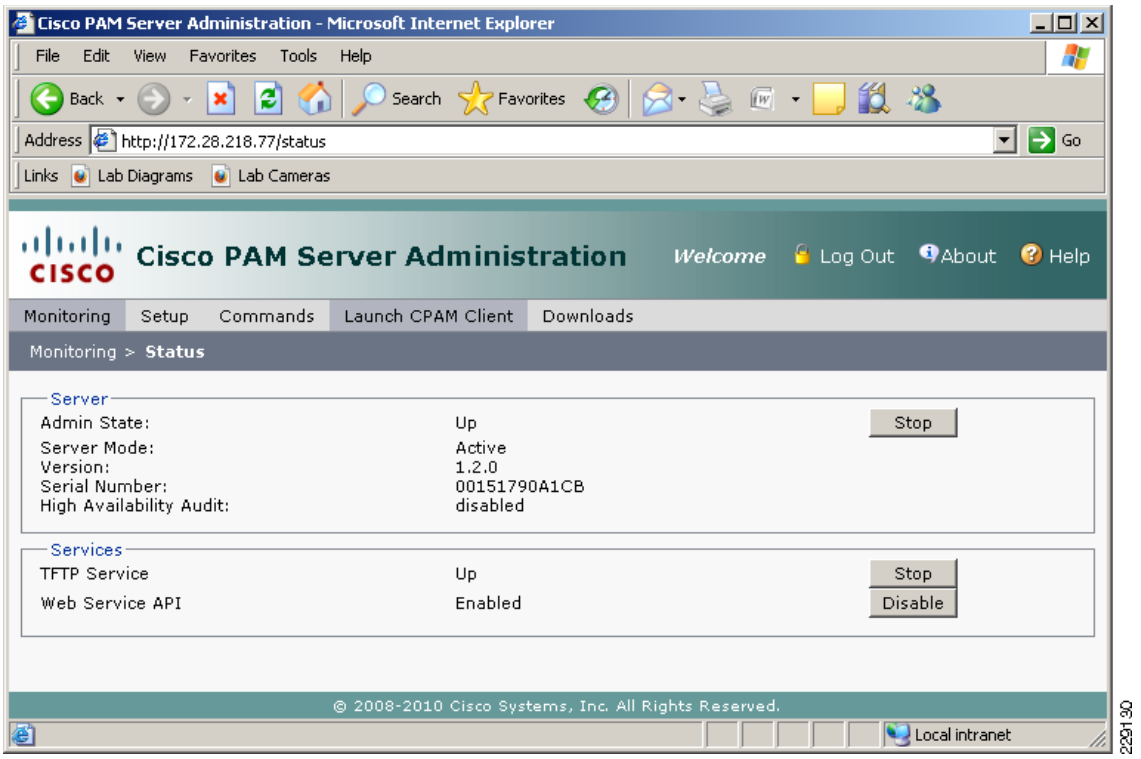
C:\Inetpub\wwwroot\PxConnectorWS\log.

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

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

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

Figure 5-5 Disable and Enable Web Services API



Auto Discovery of Newly Added Sensors

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

To update the value, perform the following steps.

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

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

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

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

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

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

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

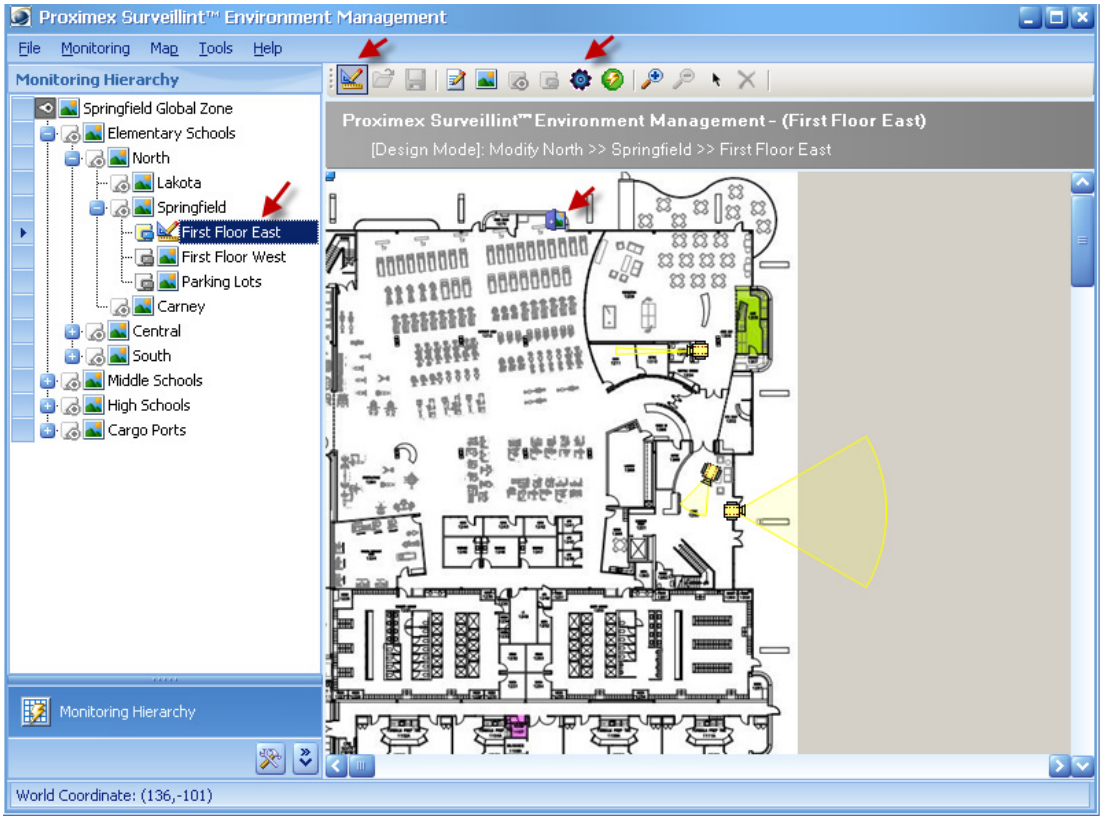
Step 3 Select an entry (such as "entrance door for police station 1") and check the blue box in front of the entry.

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

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

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

Figure 5-6 Place a Sensor on the Map Interface



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

Configuring Receiving Alerts from Doors

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

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

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

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

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

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

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

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

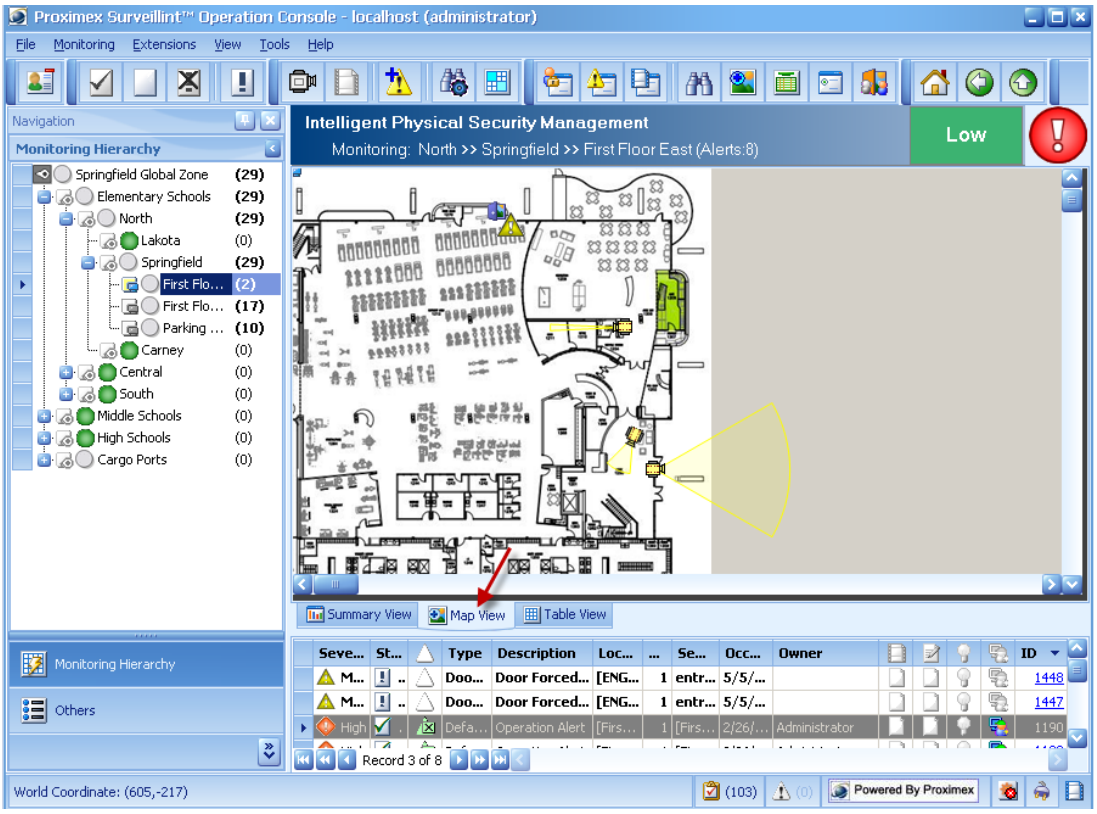
Step 7 Business Logic policies must be applied at the highest level in the hierarchy, select **Global Zone** and click **Next**.

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

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

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

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



Configuring Surveillint to Send Incident Notifications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

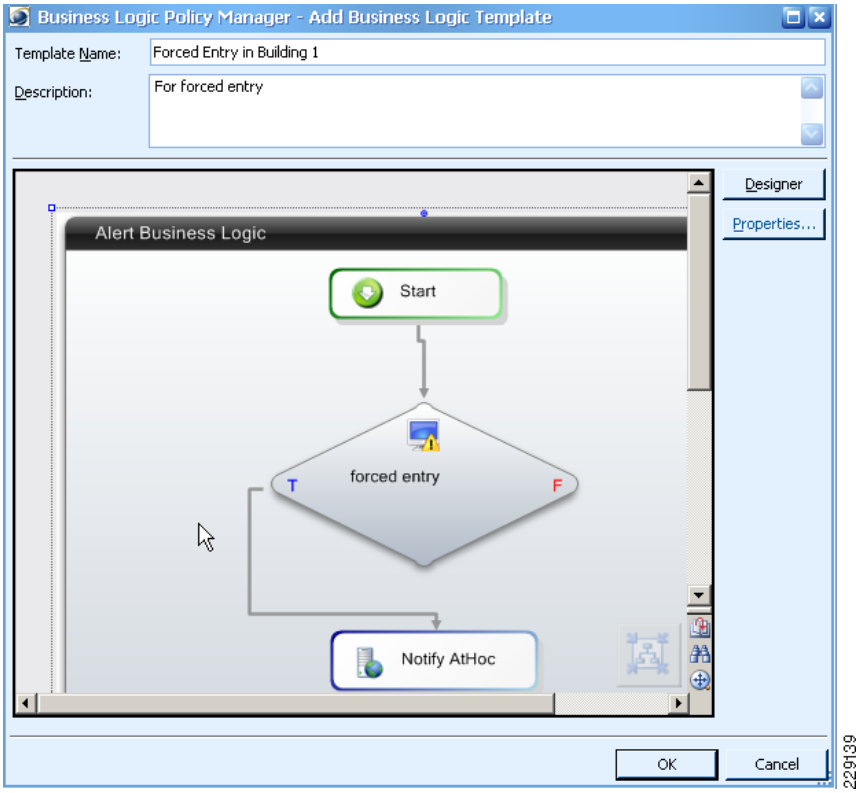
Step 14 Double click **HTTP send** on the left panel and the **HTTP send activity** window opens.

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

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

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

Figure 5-8 Alert Business Logic was Created



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

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

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

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

Step 20 Click **OK > Apply**.

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

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

Troubleshooting

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

CPAM Receives Alerts and Takes the Proper Action

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

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

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

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

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

IPICS Integration

Integration Checkpoints

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

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

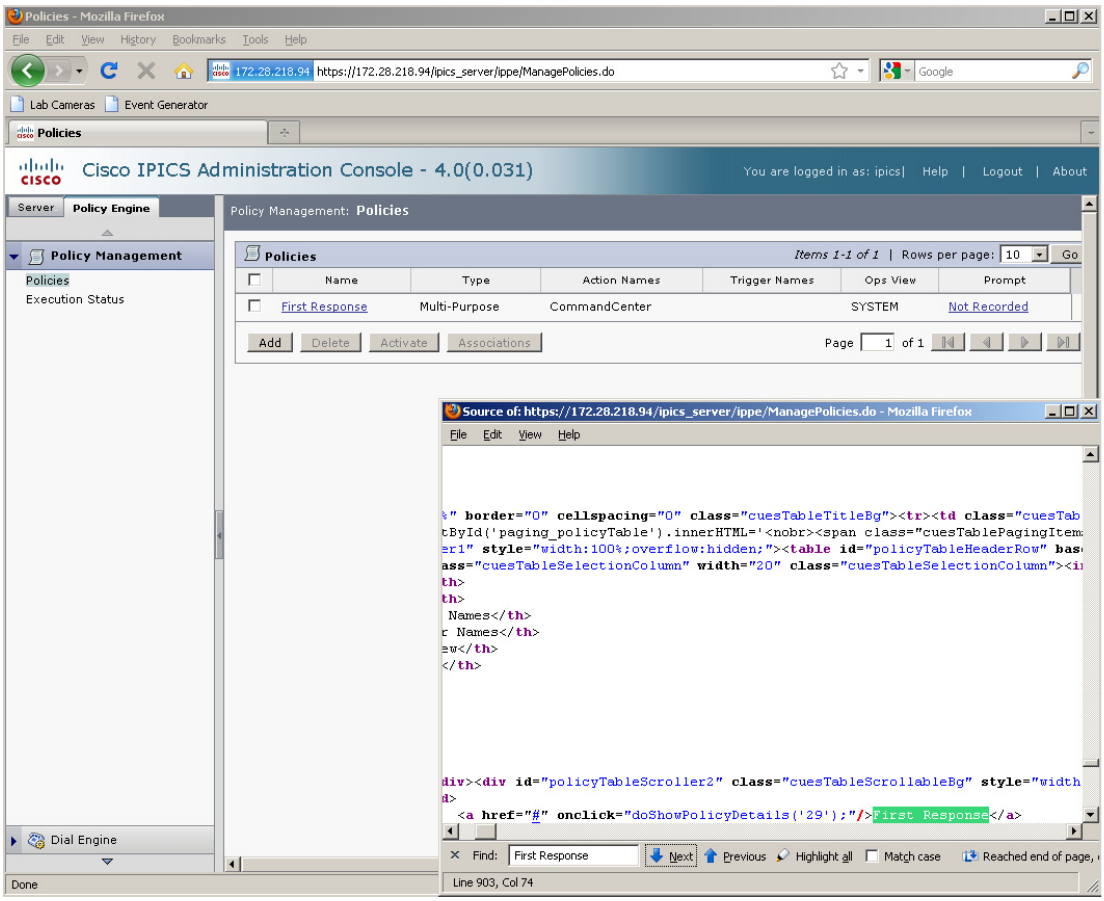
Step 1 Right-click anywhere inside the policy management window (the window on the right).

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

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

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

Figure 5-9 Find Policy ID



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

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

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

The browser asks to enter user ID and password.

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

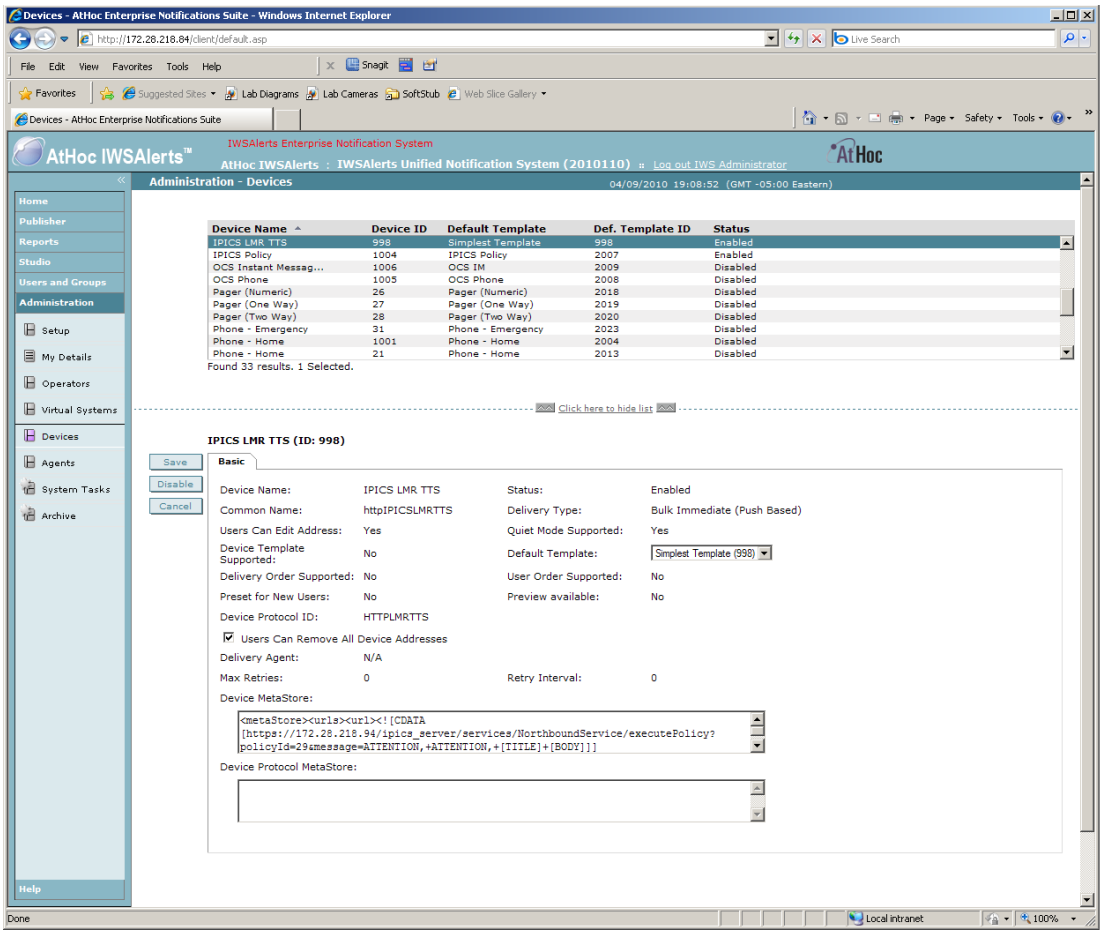
The phone with extension 1000 rings. When a user picks up the phone, the phone announces "This is Cisco IPICS calling. Press any key to continue". This is followed by "*Please enter your User ID and PIN*". Next it plays "*You're invited to join VTG 'first responder'; you're about to join VTG 'first responder';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

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

Integrating IPICS and AtHoc

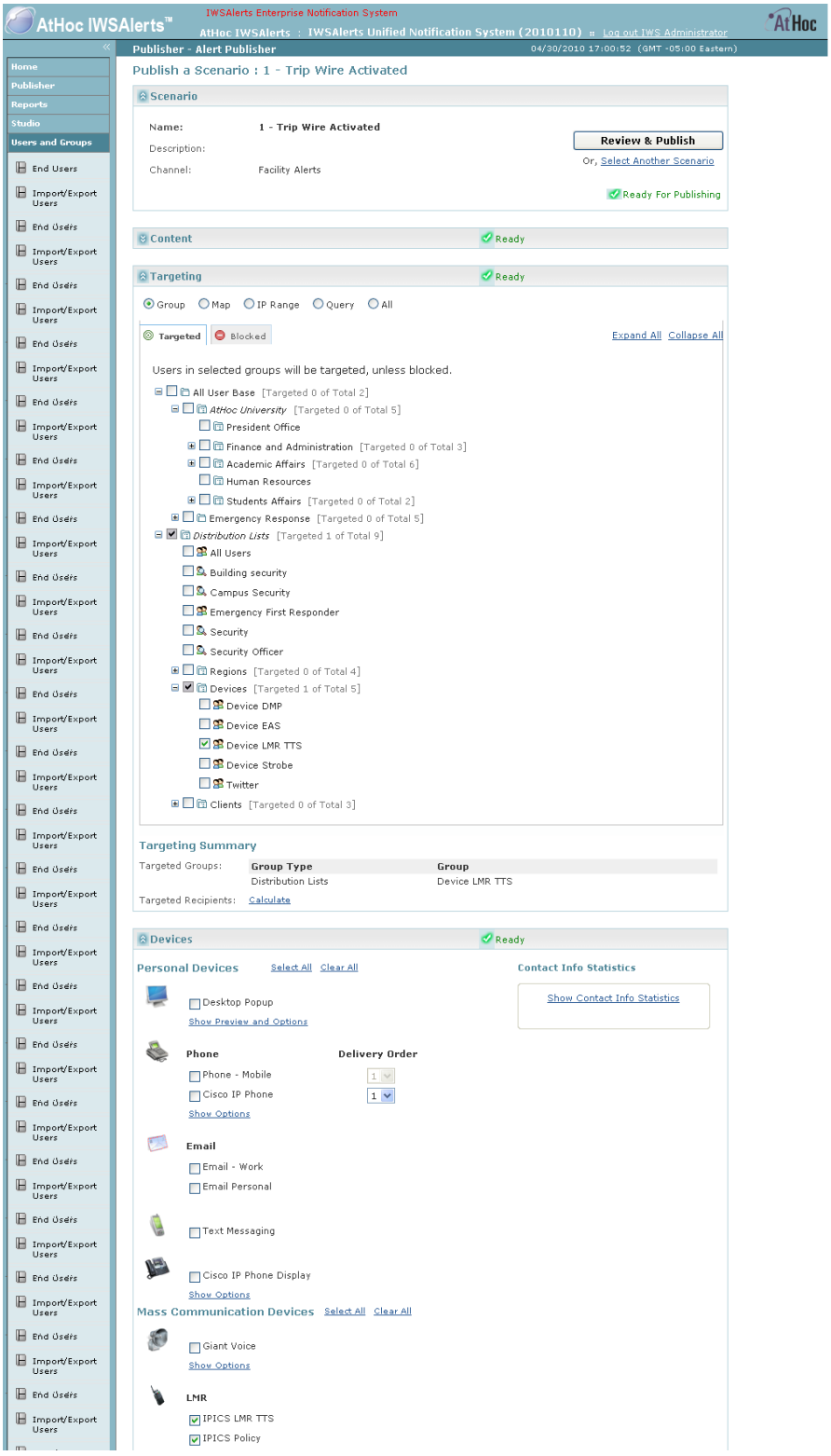
AtHoc has defined the “IPICS LMR TTS” device. Update the “default MetaStore” for this device with the URL for triggering IPICS. See Figure 5-10.

Figure 5-10 Update Default MetaStore for IPICS



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

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



DMP Integration

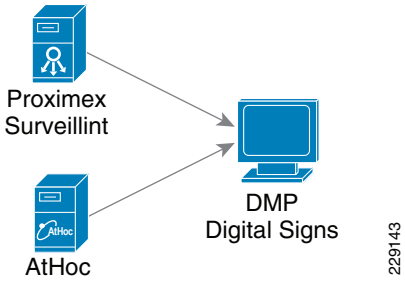
Digital media players are able to decode and display unicast and multicast live video stream as well as Flash content. In large deployments, DMPs are controlled by the Digital Media Manager (DMM), but DMPs can also receive content directly from a web server or other applications.

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

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

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

Figure 5-12 DMP Receiving Alerts



Creating HTML Content for the DMP

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

Figure 5-13 Sample DMP Alert

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

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

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

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

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

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

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

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

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

Invoking Content for the DMP

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

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

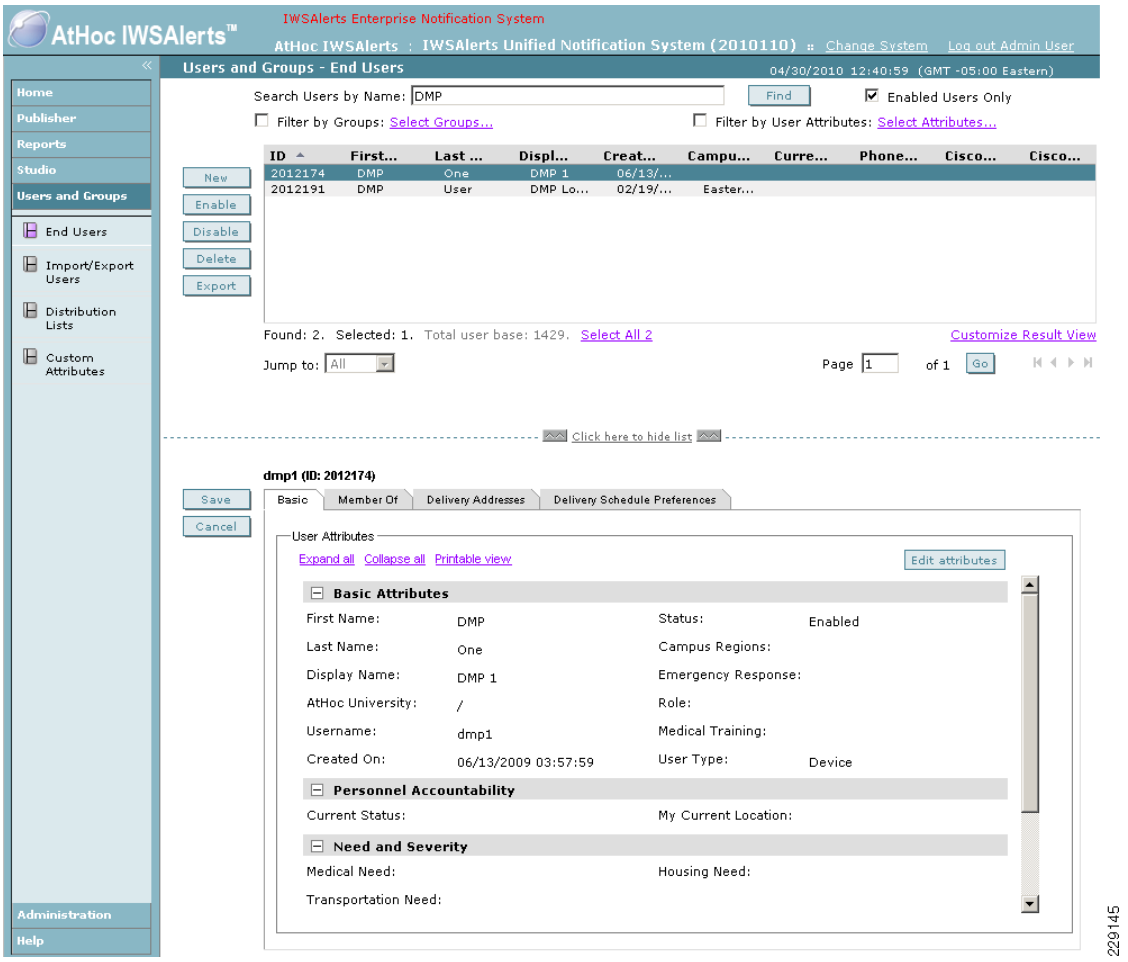
The following example retrieves the chemical.html file from the DMP at IP address 10.94.162.225. The chemical.html page is served by the web server at 10.94.162.233:
http://admin:default@10.94.162.225:7777/set_param?init.BROWSER_CMD=http://10.94.162.233/chemical.html&init.TVZILLA_URL=http://10.94.162.233/chemical.html

Integrating DMP and AtHoc IWSAlerts

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

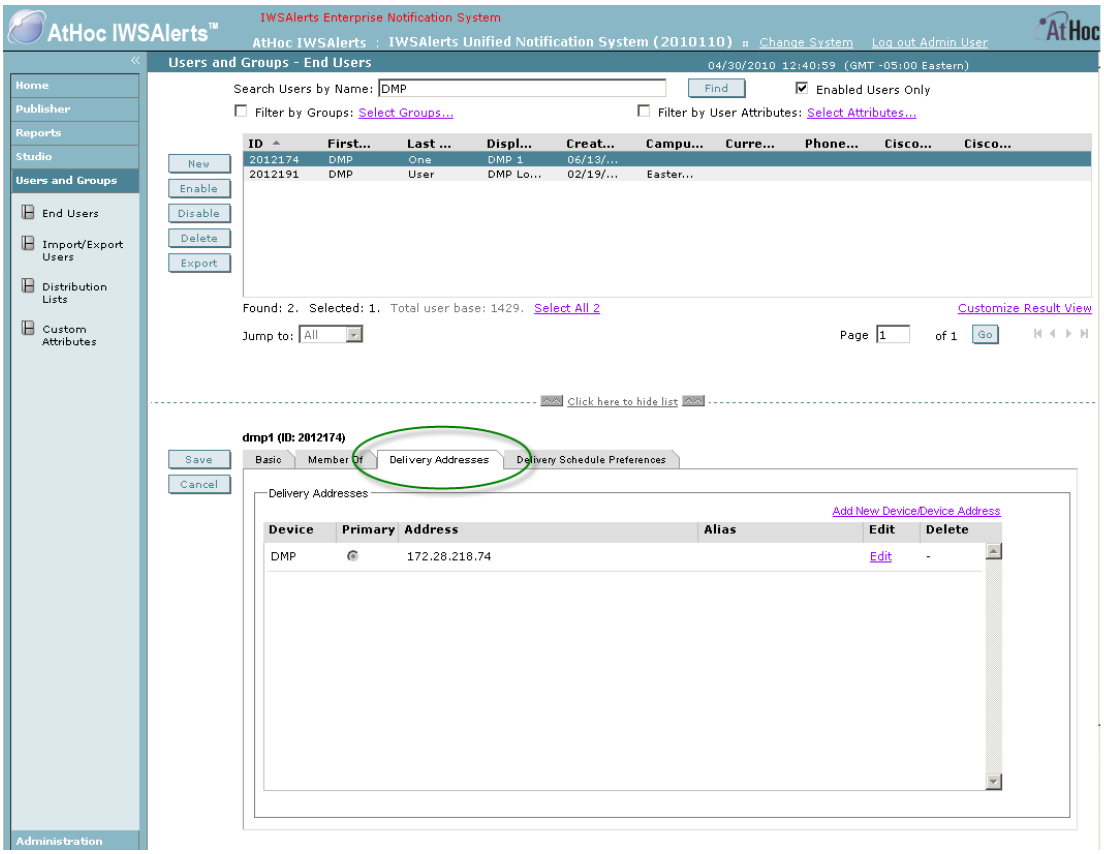
Step 1 The DMP is defined in IWSAlerts under **Users and Groups > End Users**, as shown in Figure 5-14.

Figure 5-14 DMP Definition in IWSAlerts



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

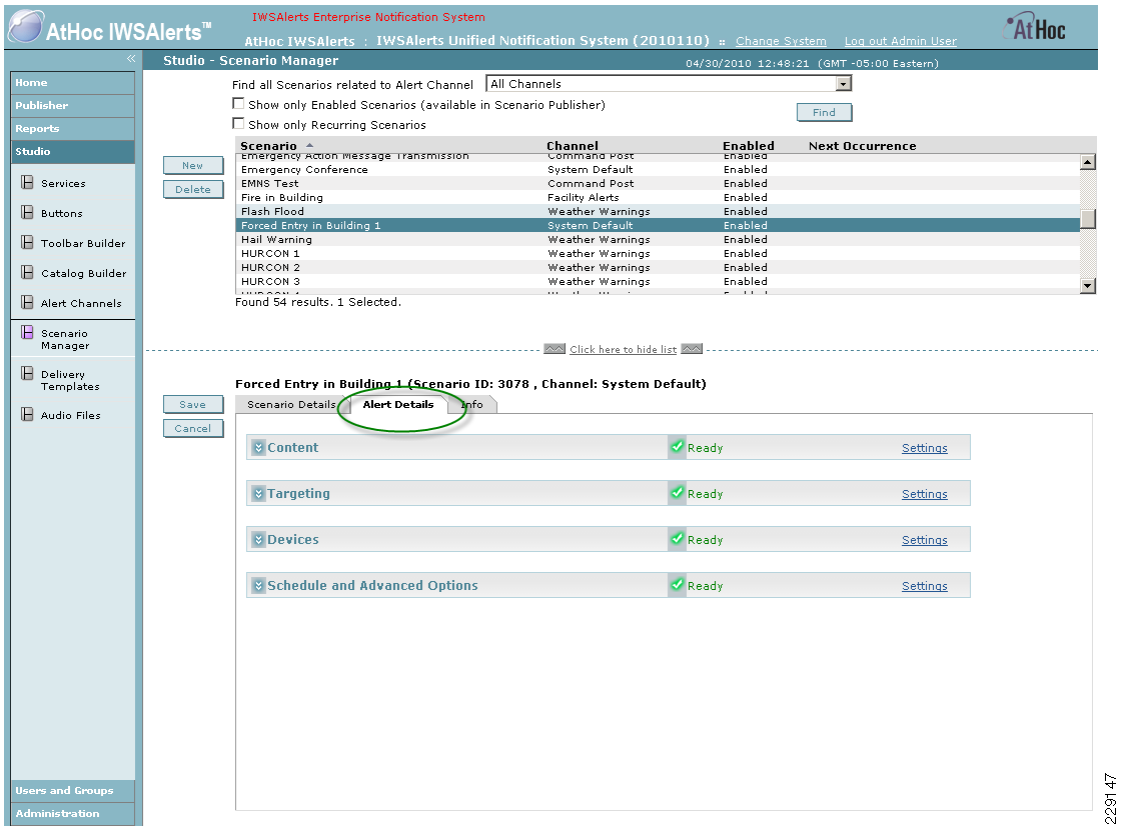
Figure 5-15 DMP IP Address



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

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

Figure 5-16 DMP Scenario



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

Figure 5-17 Target Devices

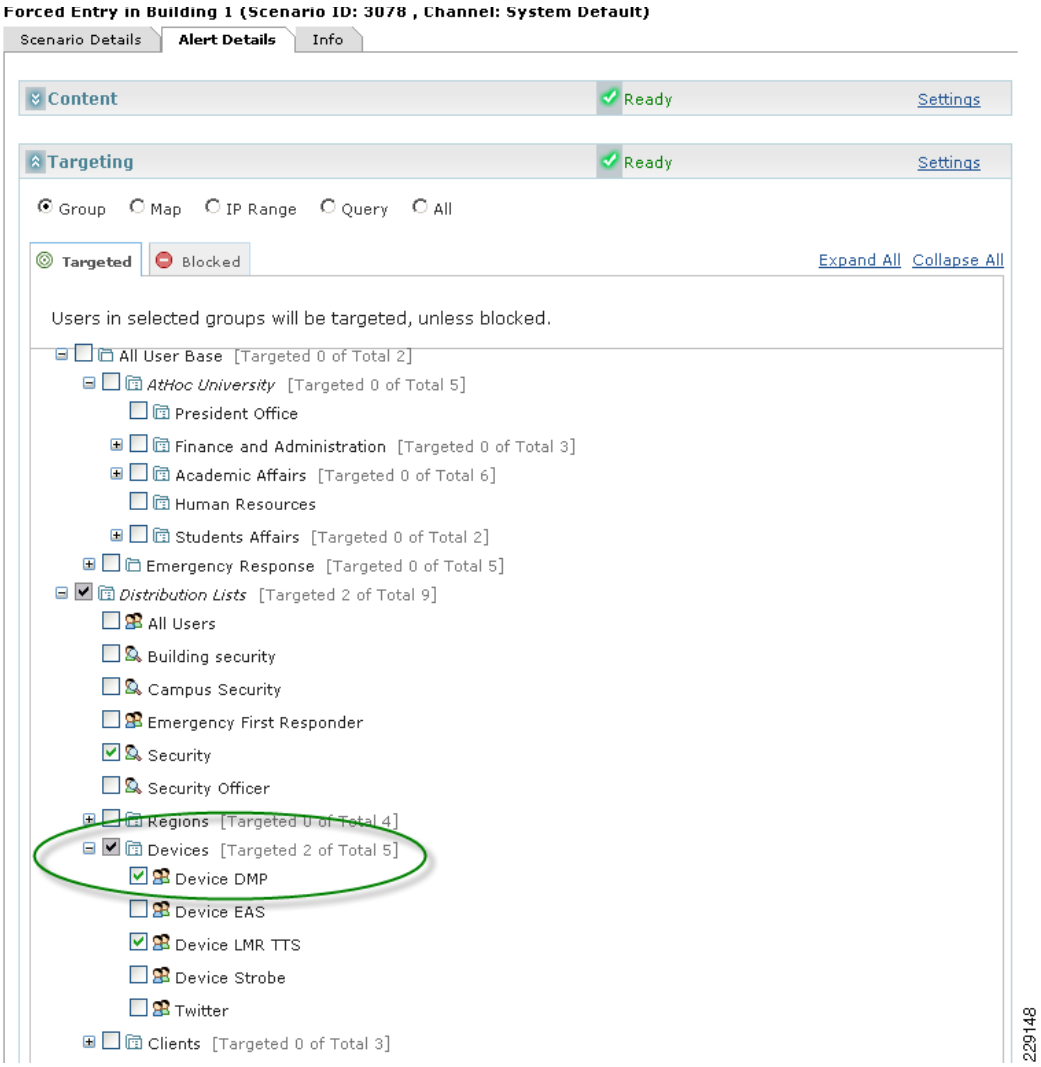
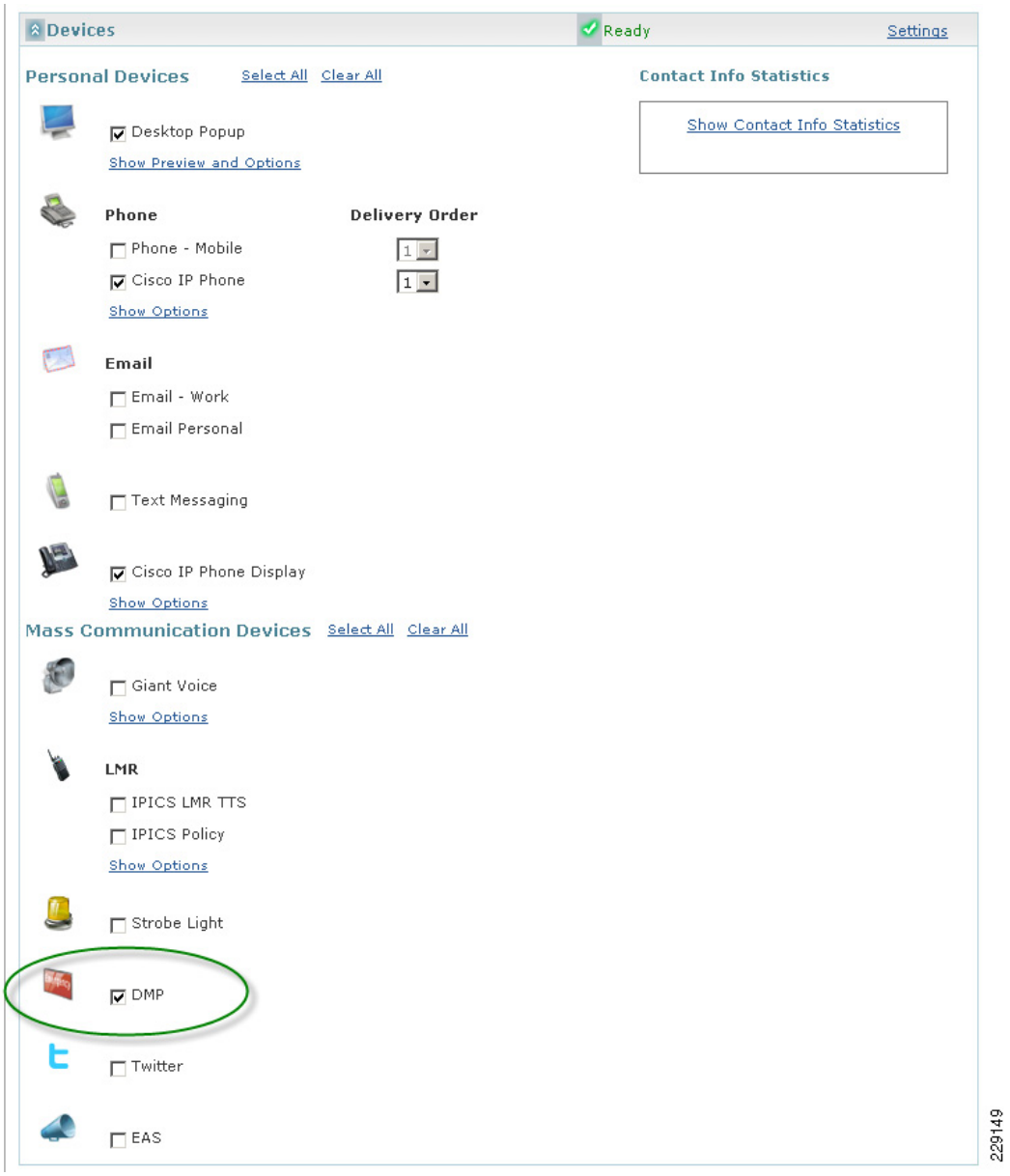


Figure 5-18 Enabled Devices



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

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

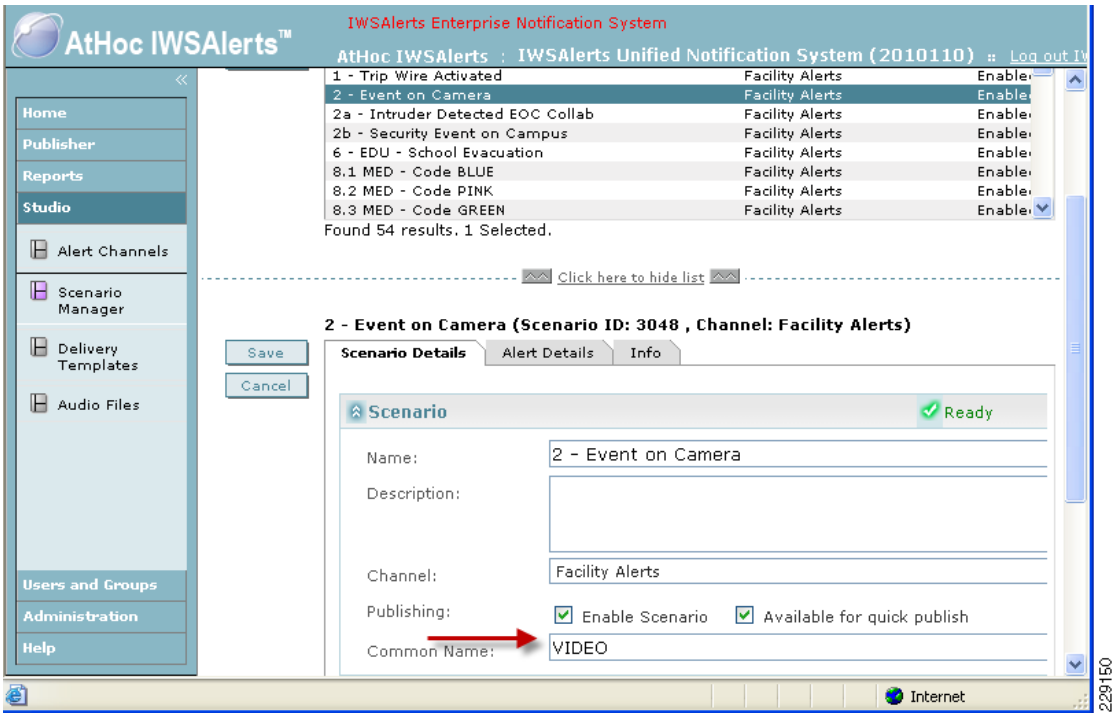
For example, enter the following URL in a browser:

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

It will show a snapshot of a camera.

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

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



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

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

For the above scenario, it will be:

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

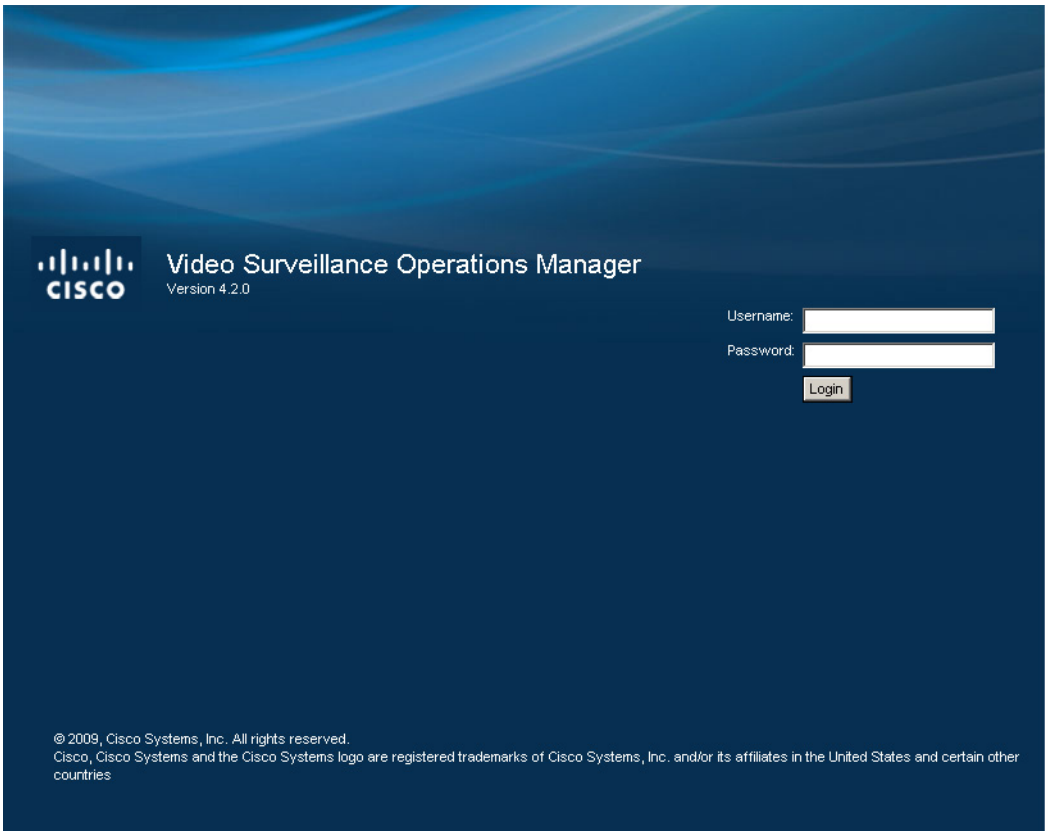
ObjectVideo Integration with Surveillint

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

Configuring ObjectVideo Sensors

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

Figure 5-20 Cisco Video Surveillance Operations Manager



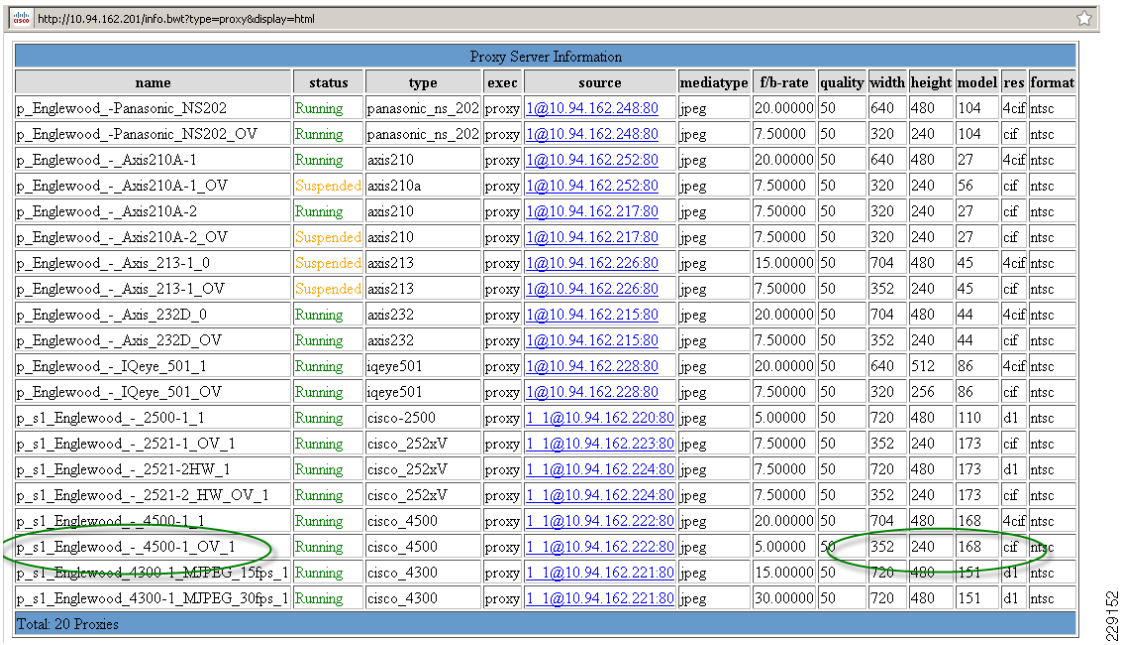
Selecting the Video Source for a Sensor

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

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

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

Figure 5-21 List of Running Proxies



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

Proxy Server Information

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

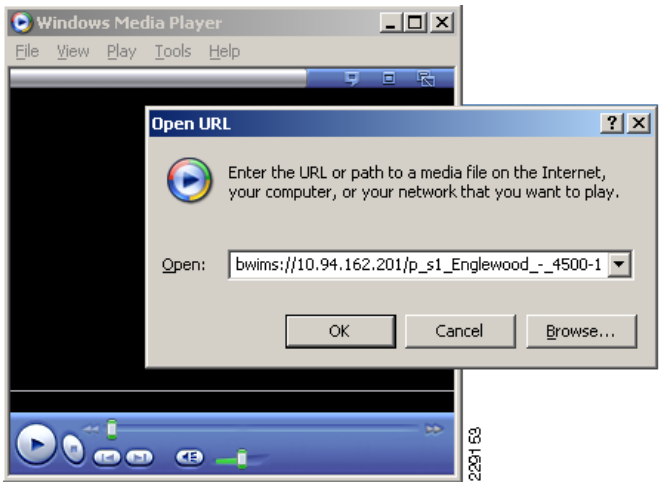
Total: 20 Proxies

229152

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

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

Figure 5-22 Windows Media Player



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

Figure 5-23 Windows Media Player—Streaming

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

Configuring a New Sensor using the ObjectVideo Management Tool

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

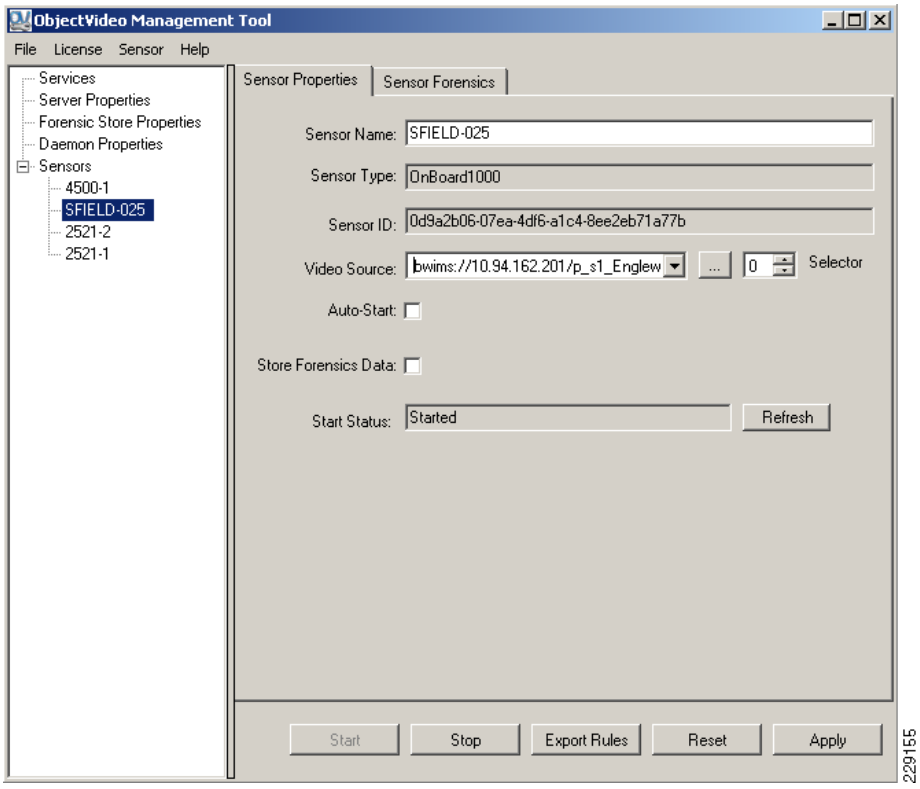
Step 1 Launch the ObjectVideo Management Tool and click on **Sensor > Add.** Specify the sensor type as **OnBoard 1000.**

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

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

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

Figure 5-24 Sensor Defined



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

ObjectVideo Rule Management Tool

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

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

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

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

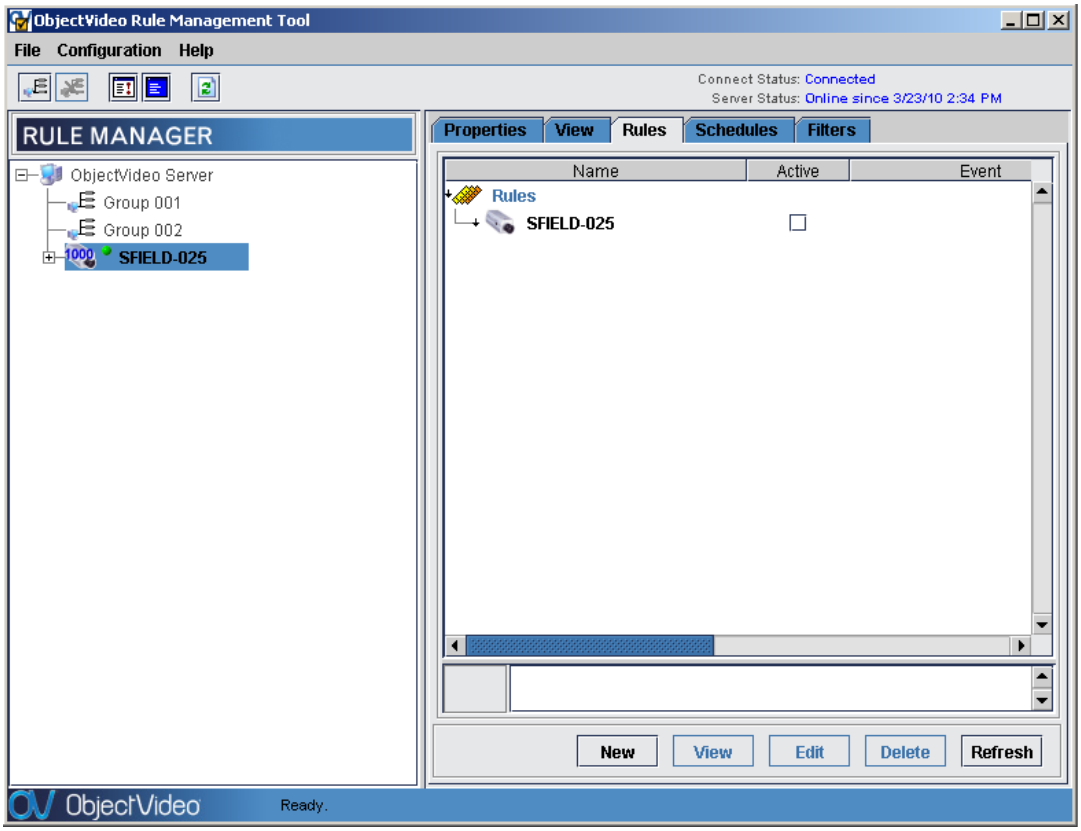
When defining a new event using the Rule Management Tool, one or more objects must be specified for the event. An object is something that either performs an action or is acted upon to trigger a response. The following object types may not be supported by every sensor:

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

To create a new rule, perform the following steps:

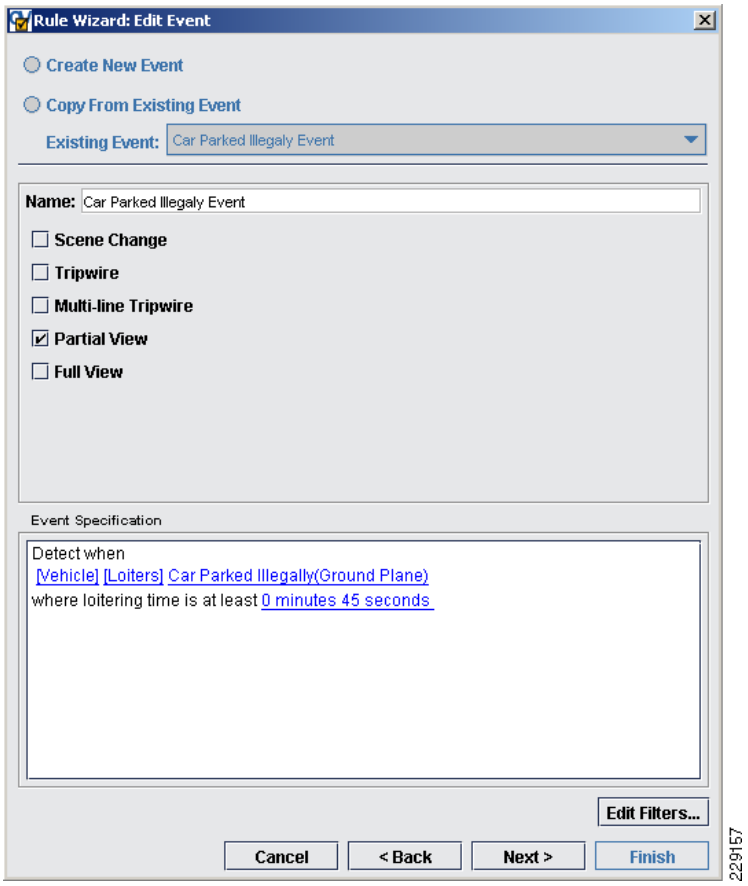
Step 1 Select the newly created sensor and click on **Default View > Rules > New**, as shown in Figure 5-25.

Figure 5-25 New Analytics Rule



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

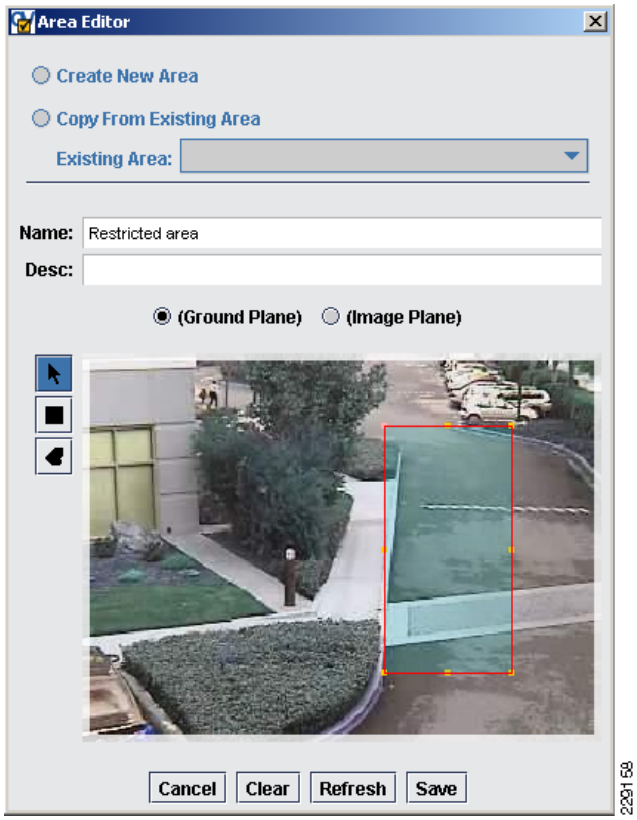
Figure 5-26 Event Details



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

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

Figure 5-27 Restricted Area



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

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

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

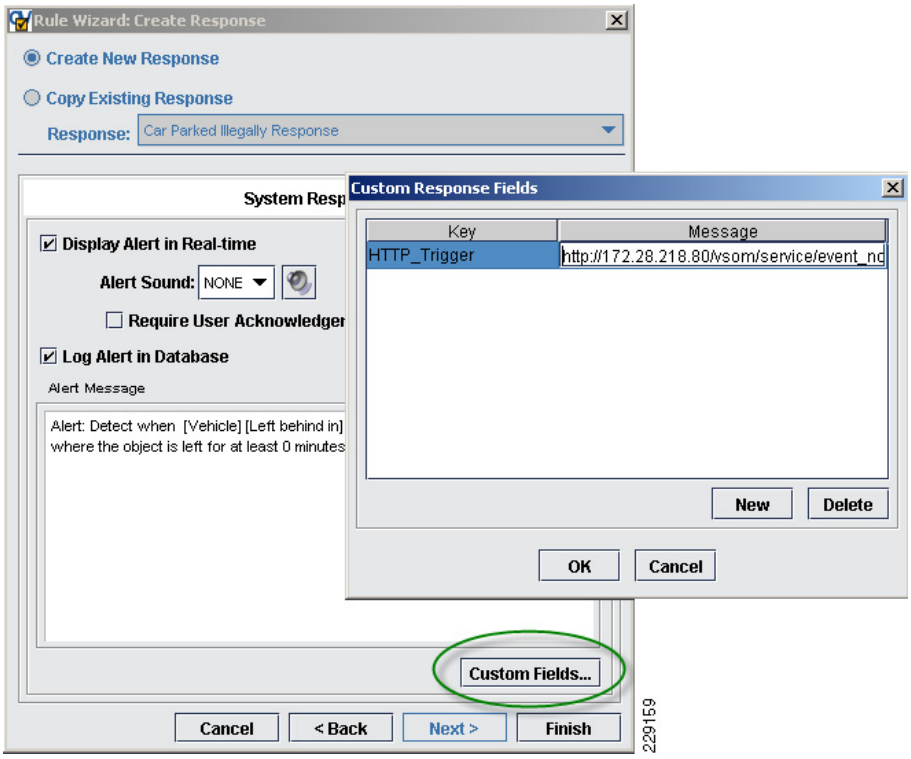
Step 4 To send a specific HTTP message to a third-party system, such as VSOM, define the proper URL in the *Alertbridge.exe.config* file, located in the ObjectVideo server at *C:\Program Files\ObjectVideo\Alert Bridge*.

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

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

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

Figure 5-28 Custom Response Fields

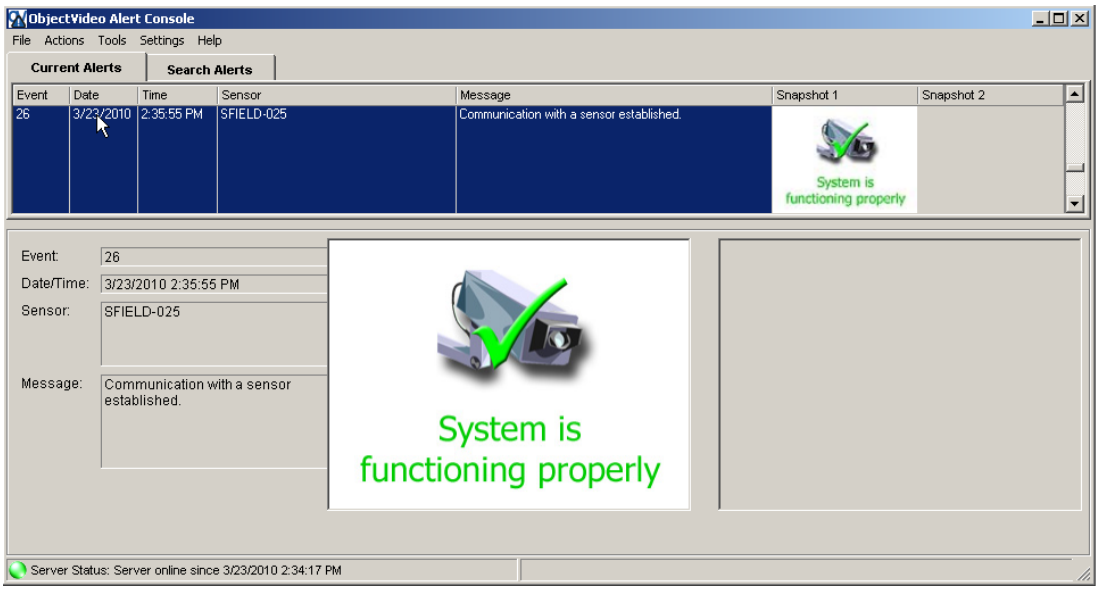


The section Configuring Surveillint to Receive ObjectVideo Alerts, page 5-34 explains how to configure Surveillint to receive alerts from ObjectVideo.

ObjectVideo Alert Console

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

Figure 5-29 Communicating with a Sensor

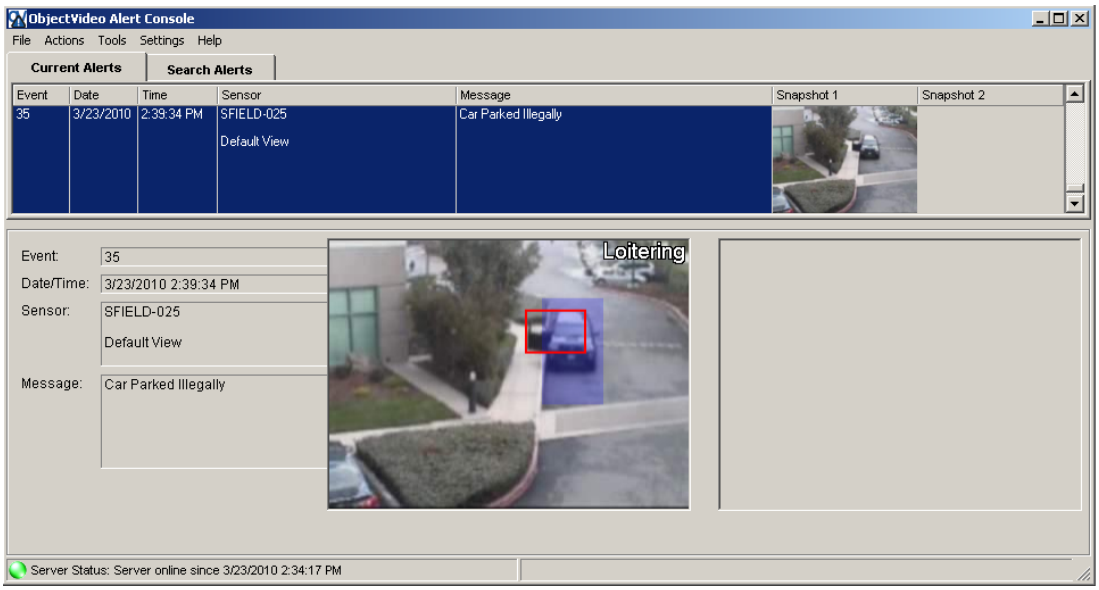


The Alert Console also logs the alerts generated by the video analytics engine. If the system is configured to send an HTTP notification to an external system, an HTTP notification takes place concurrently.

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

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

Figure 5-30 Car Parked Illegally Alert



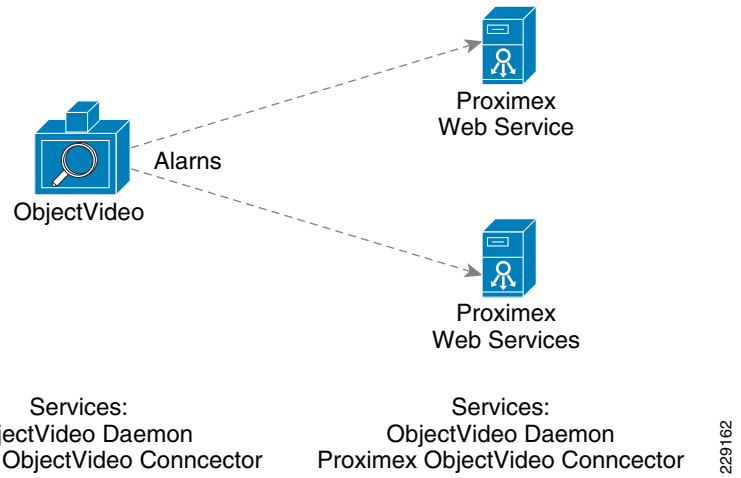
Note A detailed log for each sensor is saved under the *C:\Windows\Temp* directory. The filename is based on the Sensor ID; for example, *Sensor-0d9a2b06-07ea-4df6-a1c4-8ee2eb71a77b.log*.

Configuring Surveillint to Receive ObjectVideo Alerts

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

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

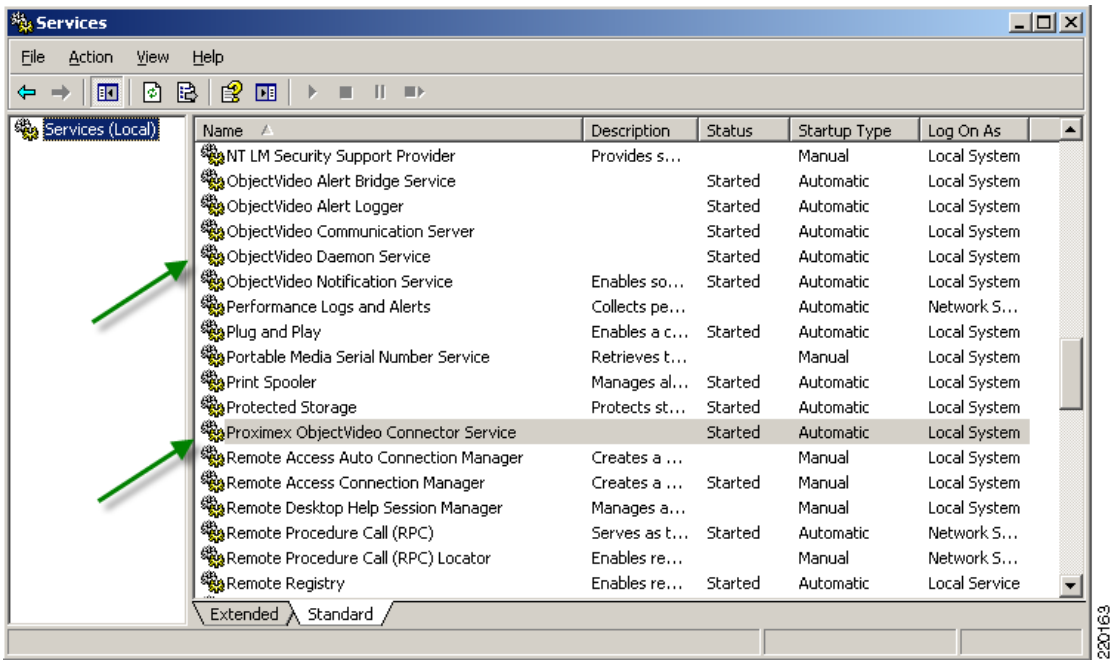
Figure 5-31 Services Required



Perform the following steps:

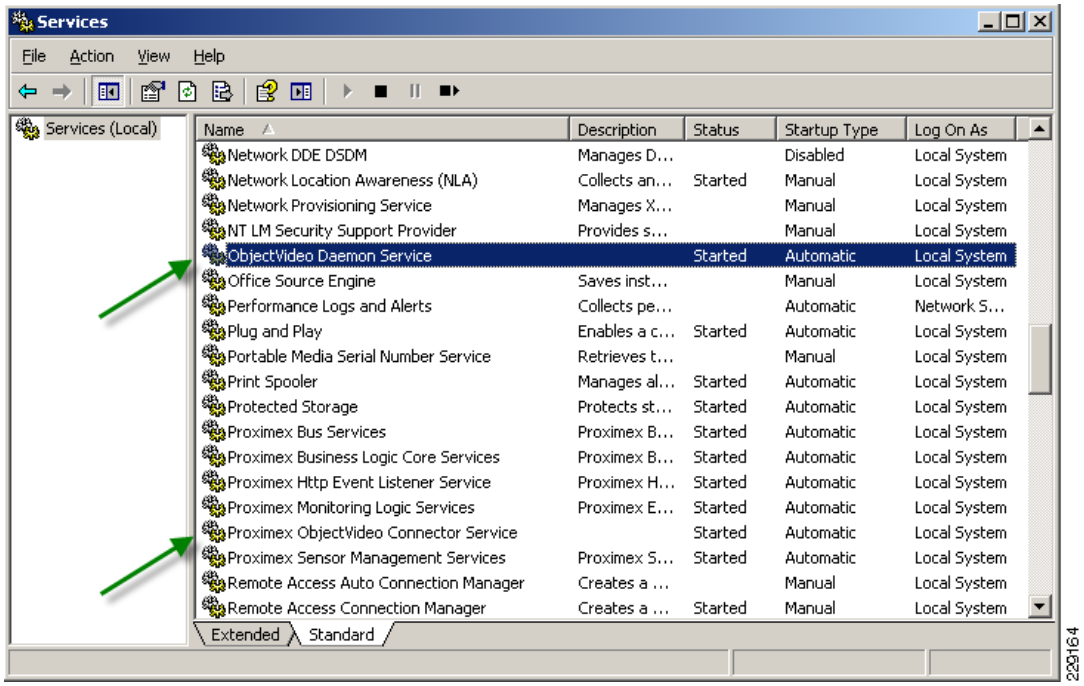
Step 1 On the ObjectVideo server, verify that the ObjectVideo Daemon Service is running and install the Proximex ObjectVideo Integration Module on the same server. The Integration Module is provided by Proximex as a **ProximexOVSetup.msi** installation file. Figure 5-32 shows the services running on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

Figure 5-32 ObjectVideo Services



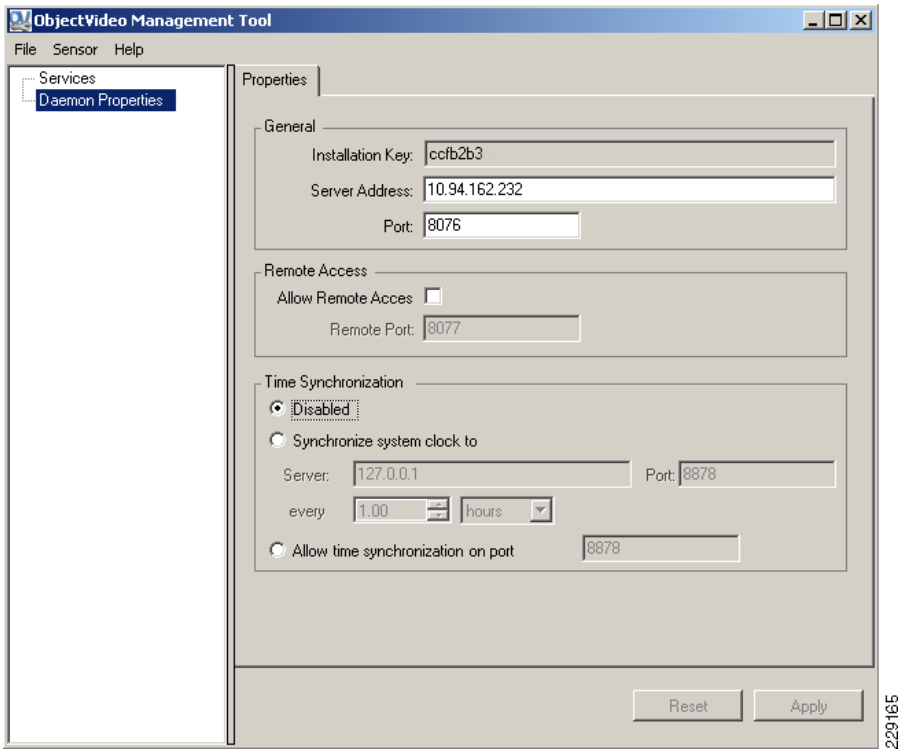
Step 2 On the Surveillint server, install the ObjectVideo Management Tool to receive alerts from ObjectVideo. A new service, *ObjectVideo Daemon Service* is installed in the Surveillint server, as shown in Figure 5-33.

Figure 5-33 Surveillint Services



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

Figure 5-34 Daemon Properties



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

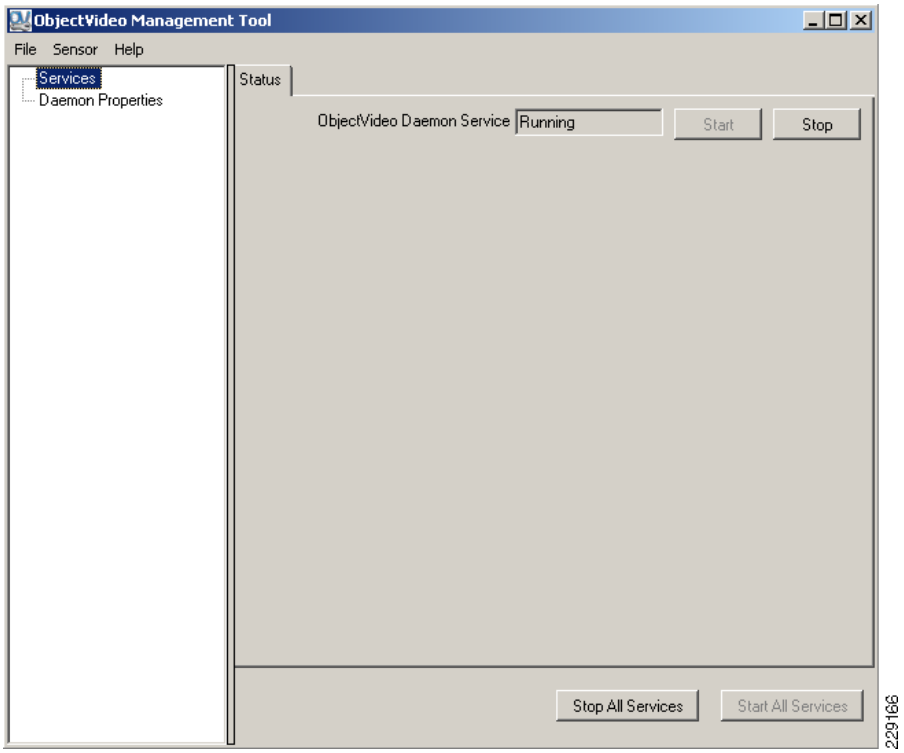
Step 5 Enter the IP address of the ObjectVideo server.

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

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

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

Figure 5-35 Restart the Daemon Service



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

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

Receiving Alerts from ObjectVideo

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

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

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

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

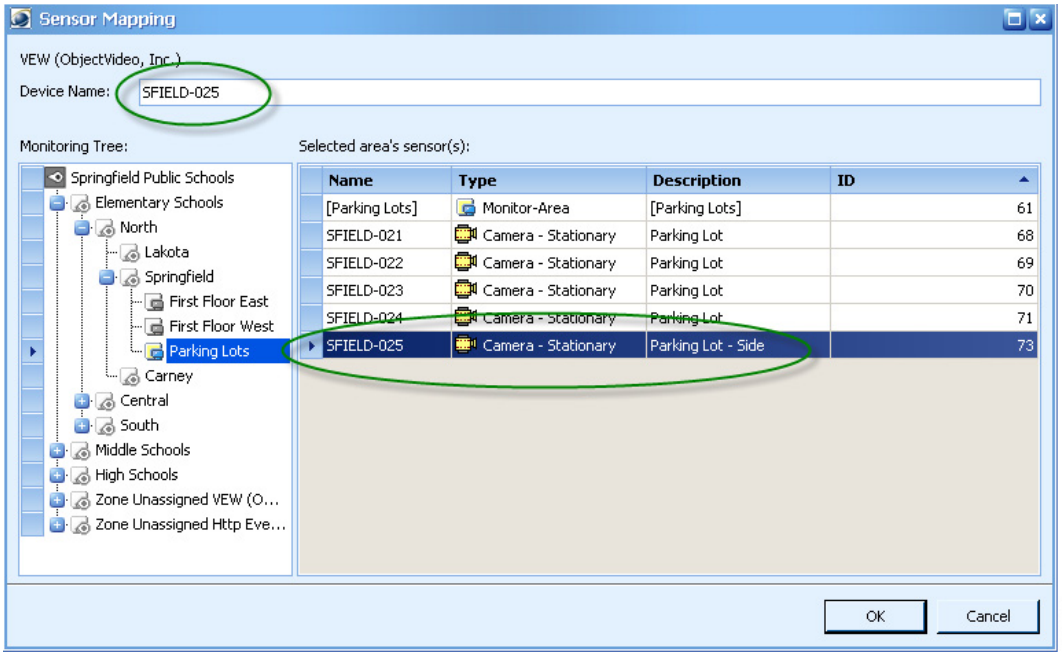
Step 2 Under Application Name, select **VEW (ObjectVideo, Inc.)**

Step 3 Click **Add…**

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

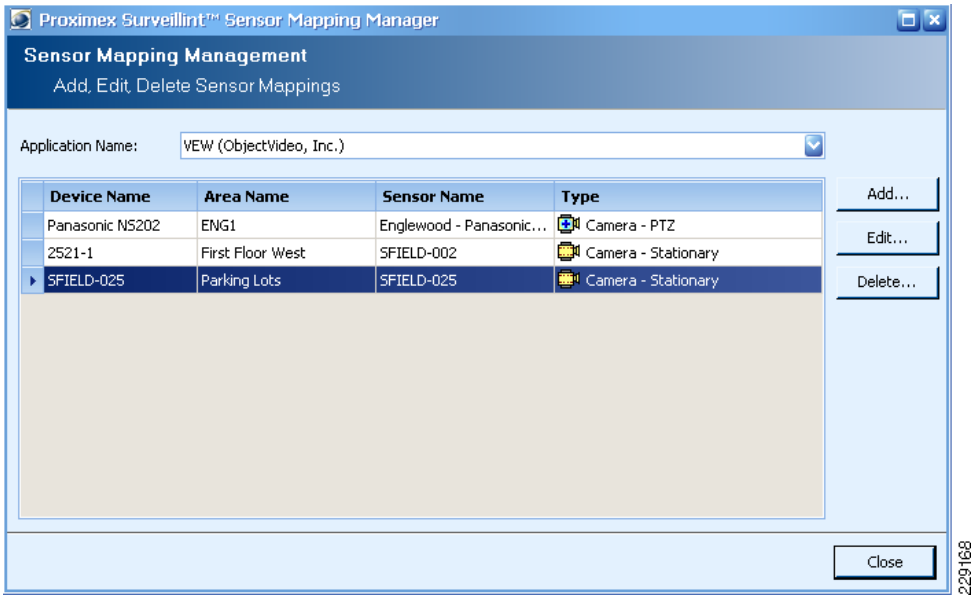
Step 5 Select the monitoring area and sensor to which SFIELD-025 will be mapped (see Figure 5-36).

Figure 5-36 Selecting the Monitoring Area and Sensor



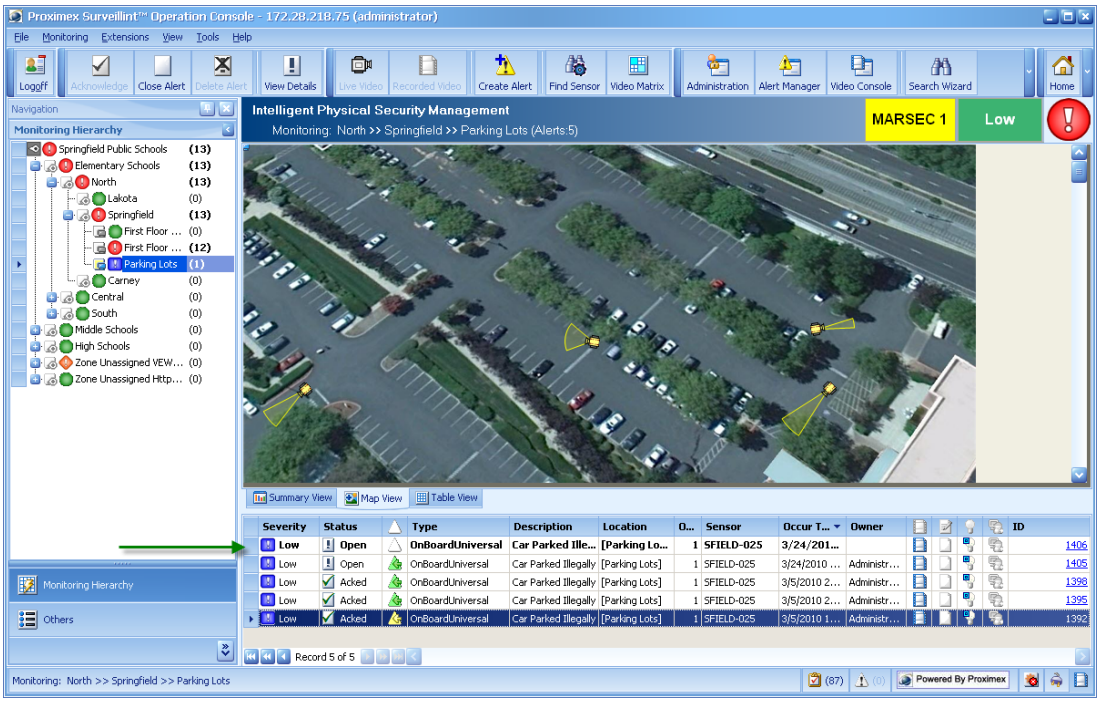
This defines a mapping between ObjectVideo's SFIELD-025 sensor and Surveillint's SFIELD-025 sensor in the Parking Lots area, as shown in Figure 5-37.

Figure 5-37 Sensor Mapping



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

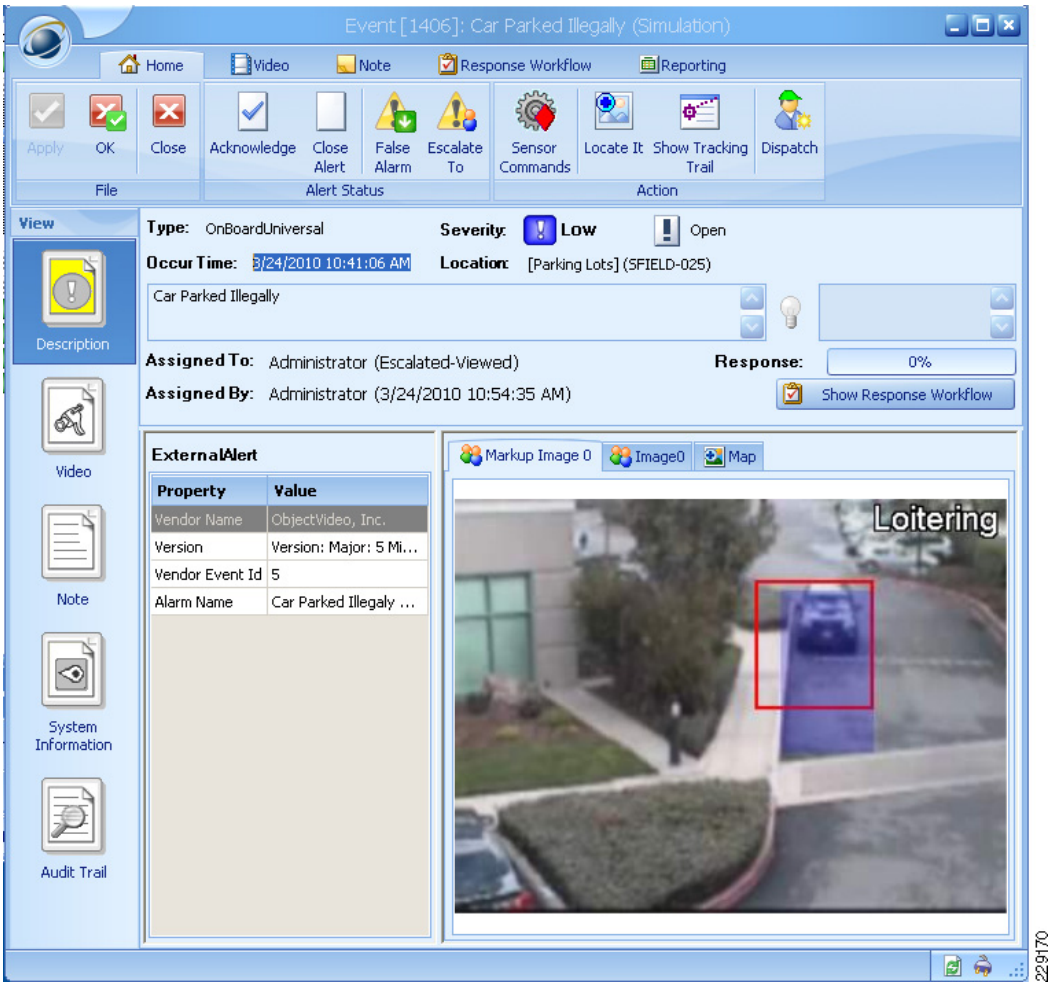
Figure 5-38 ObjectVideo Alert in Surveillint



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

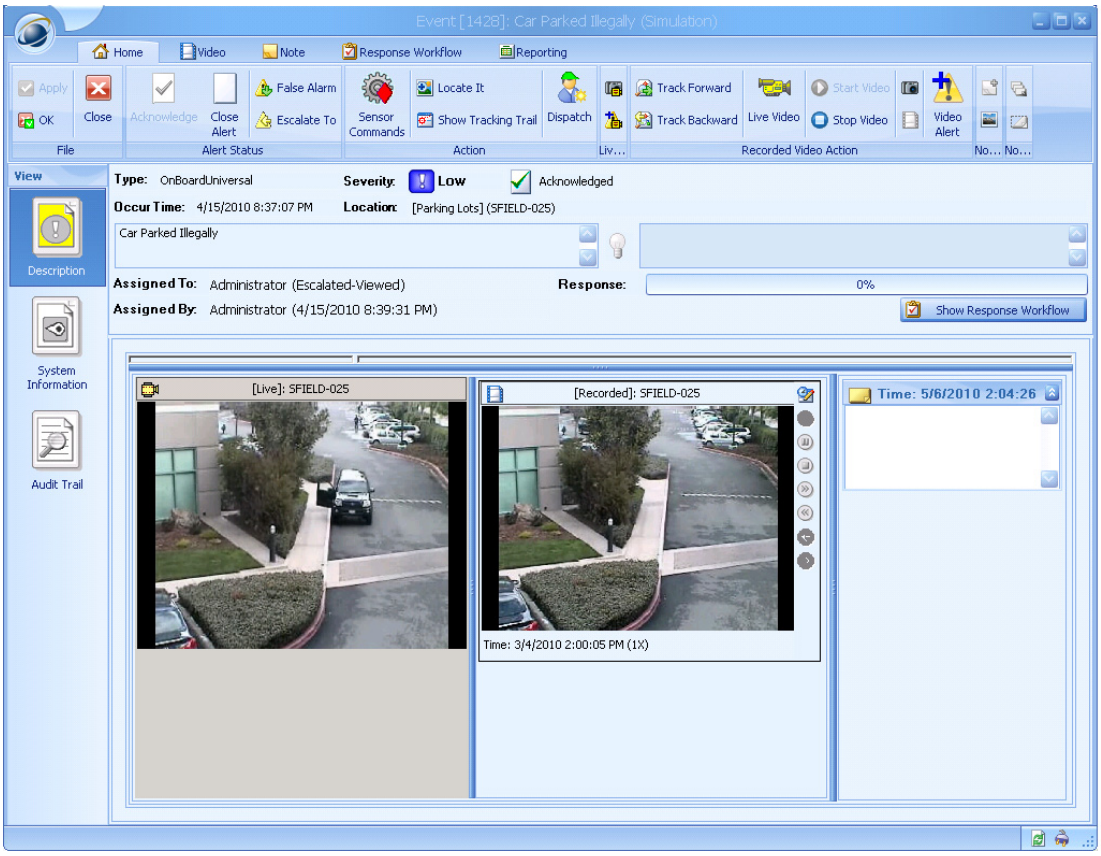
By double-clicking on the new alert, the operator can review the event details. Figure 5-39 shows an alert in Surveillint originated by ObjectVideo.

Figure 5-39 Video Analytics Alert



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

Figure 5-40 Live and Recorded Video



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

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

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

Integrating Surveillint with other Systems

Video Integration with Cisco Video Surveillance Operations Manager

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

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

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

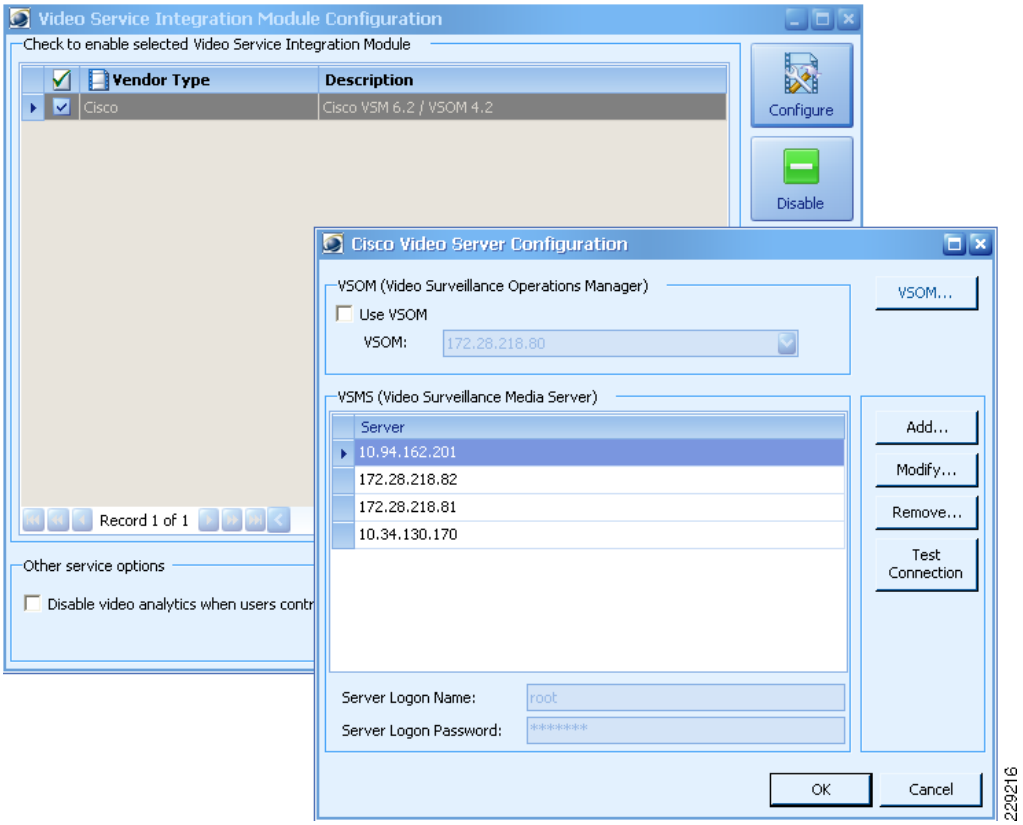
Note Contact Proximex for an updated list of video servers that have been integrated with Surveillint.

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

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

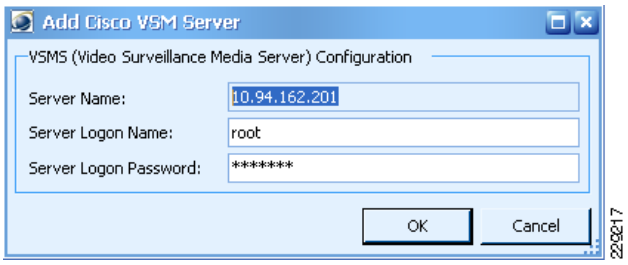
Step 2 Select Cisco VSM6.2 /VSOM 4.2 and click **Configure** (see Figure 5-41).

Figure 5-41 Configuring Video Server



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

Figure 5-42 Verifying the Settings



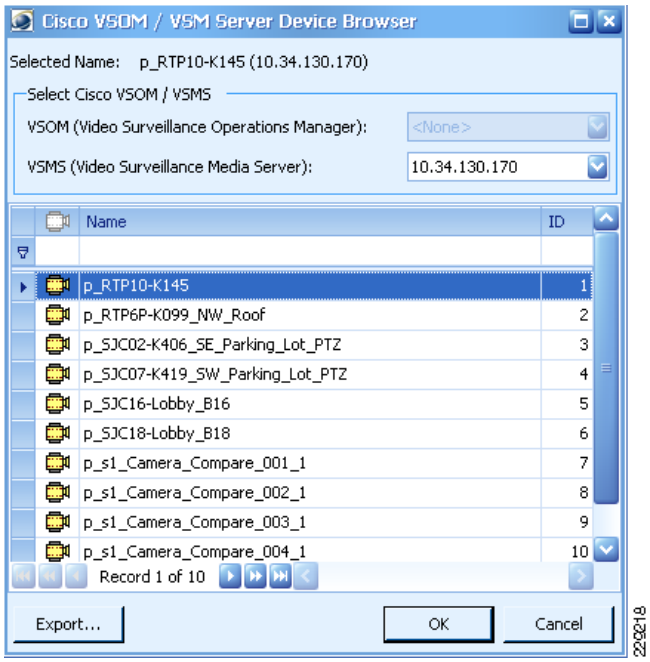
After the integration with VSOM has been defined, the IP Cameras may be added as sensors using the Administration Console.

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

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

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

Figure 5-43 Available Cameras



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

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

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

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

Figure 5-44 Video Management Console

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

Exporting and Importing Sensors

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

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

Sensor Integration and Grouping

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

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

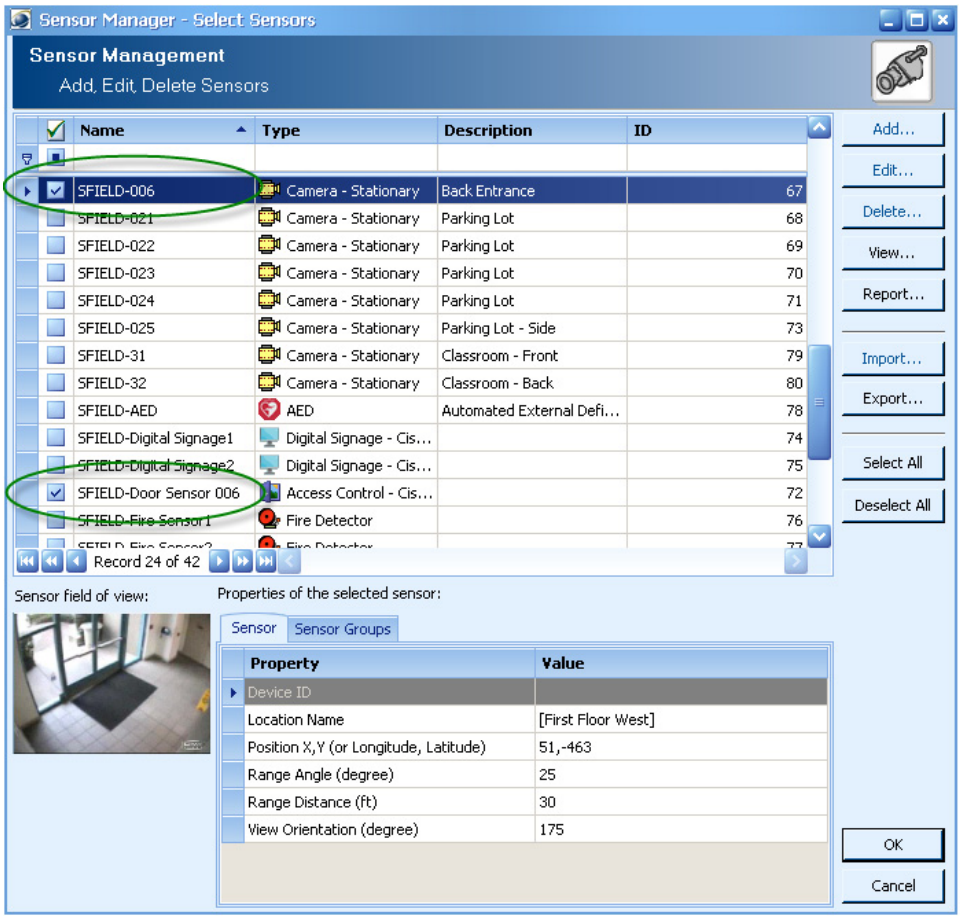
To associate an access control door with a video camera sensor, perform the following steps:

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

Figure 5-45 New Sensor Group

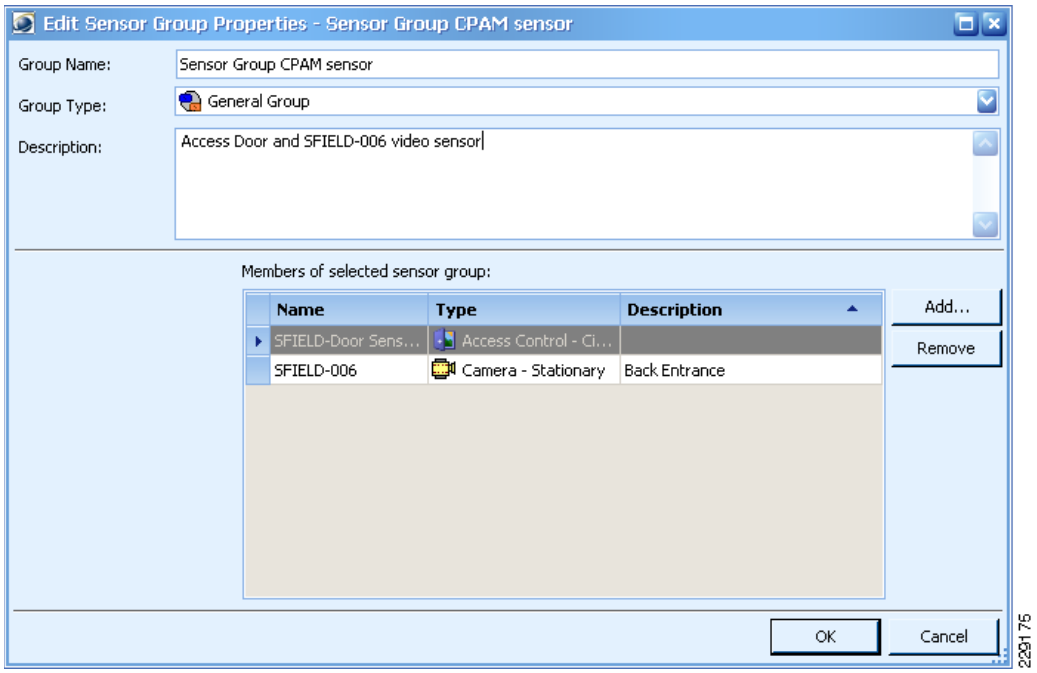
Step 2 To add members to the new group, click **Add** and select the new members by clicking the check box for each sensor, as shown in Figure 5-46.

Figure 5-46 Group Members



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

Figure 5-47 Sensor Group Properties



Simulating Alerts with Business Logic Policies

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

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

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

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

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

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

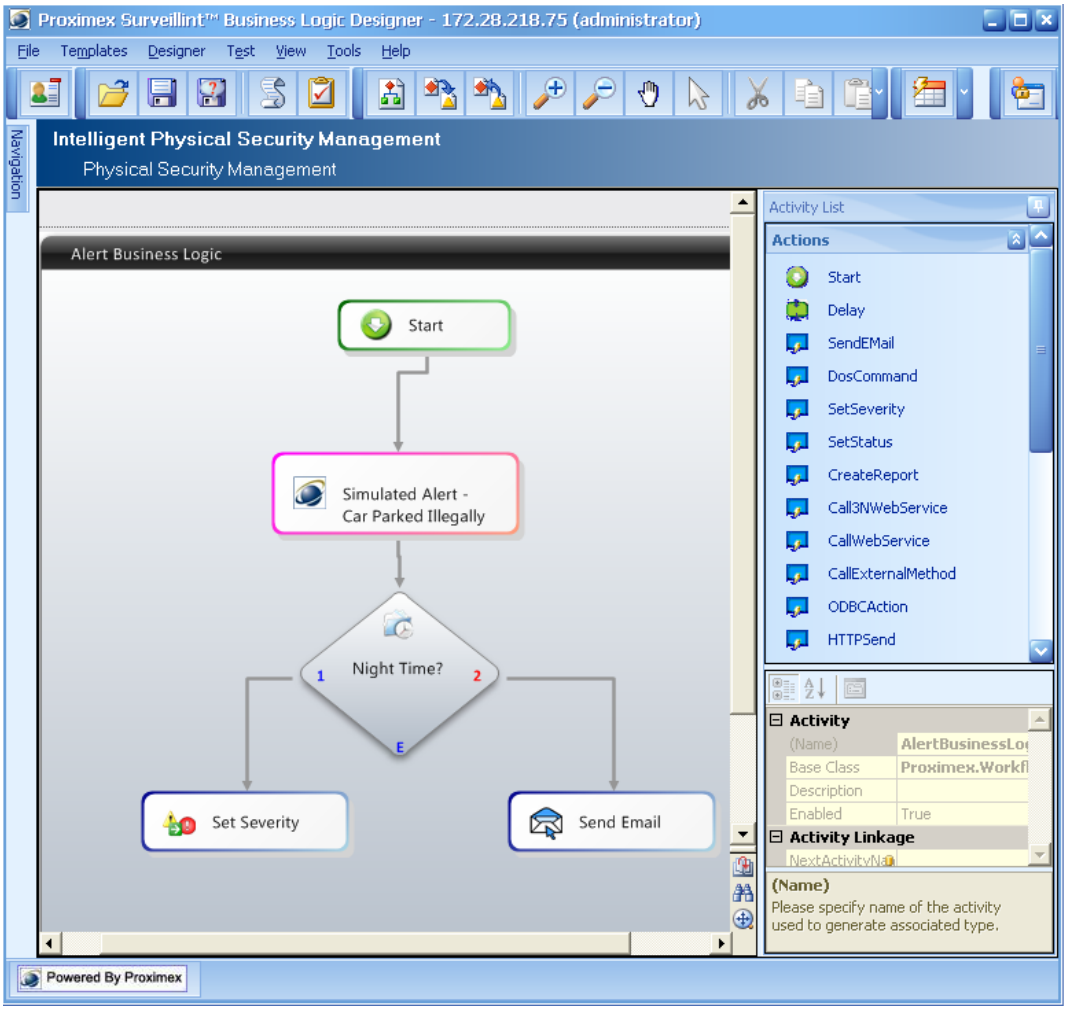
Step 3 To simulate an existing alert for testing purposes, edit the Simulate Alert component by double-clicking the **Simulate Alert** activity.

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

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

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

Figure 5-48 Business Logic



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

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

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

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

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

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

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

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

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

HTTP URL Notification with Surveillint

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

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

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

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

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

Figure 5-49 URL Event Notifications

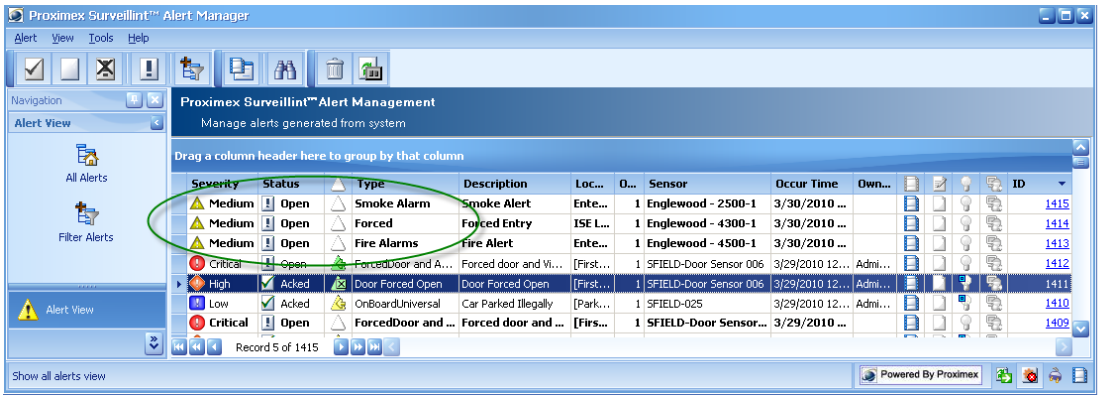
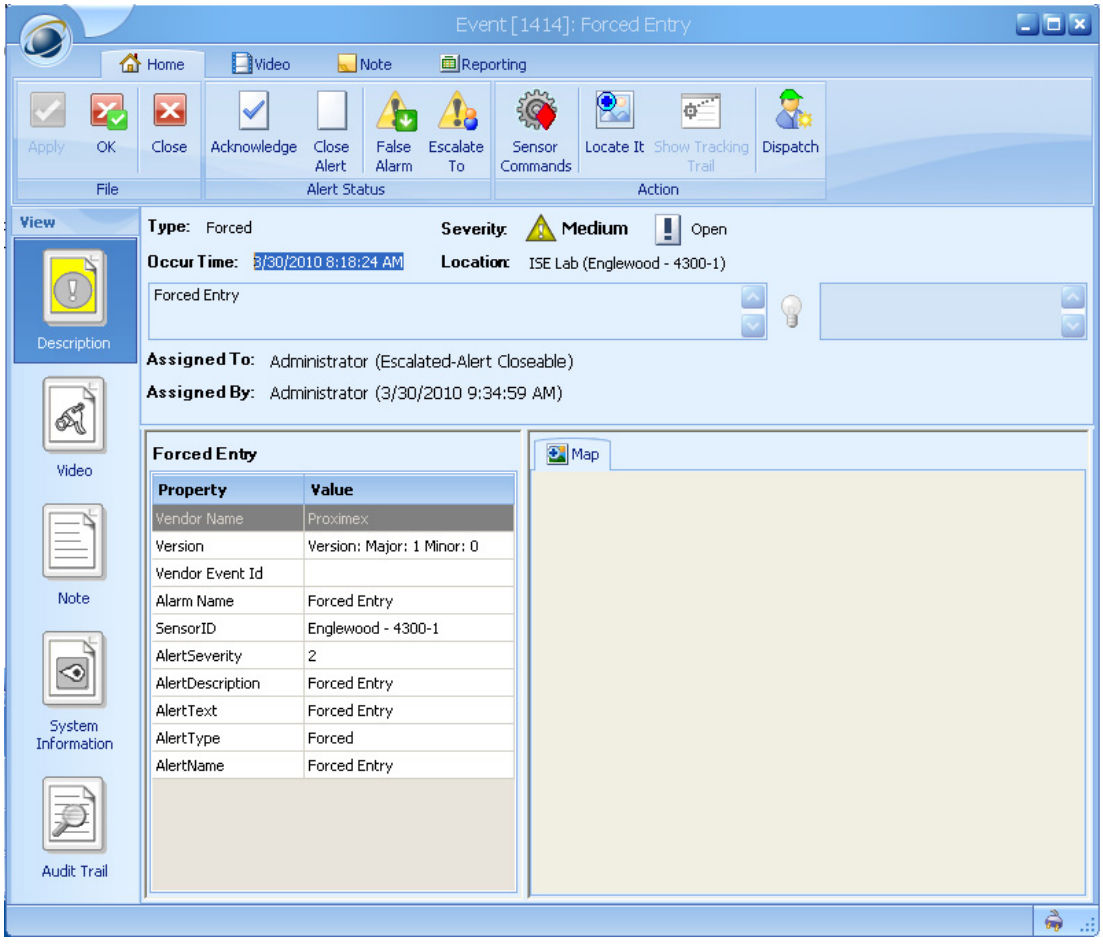


Figure 5-50 shows the new event and the parameters that were passed by the URL notification. The event is created and located in the monitoring area according to the sensor used in the URL.

Figure 5-50 New HTTP URL Notification



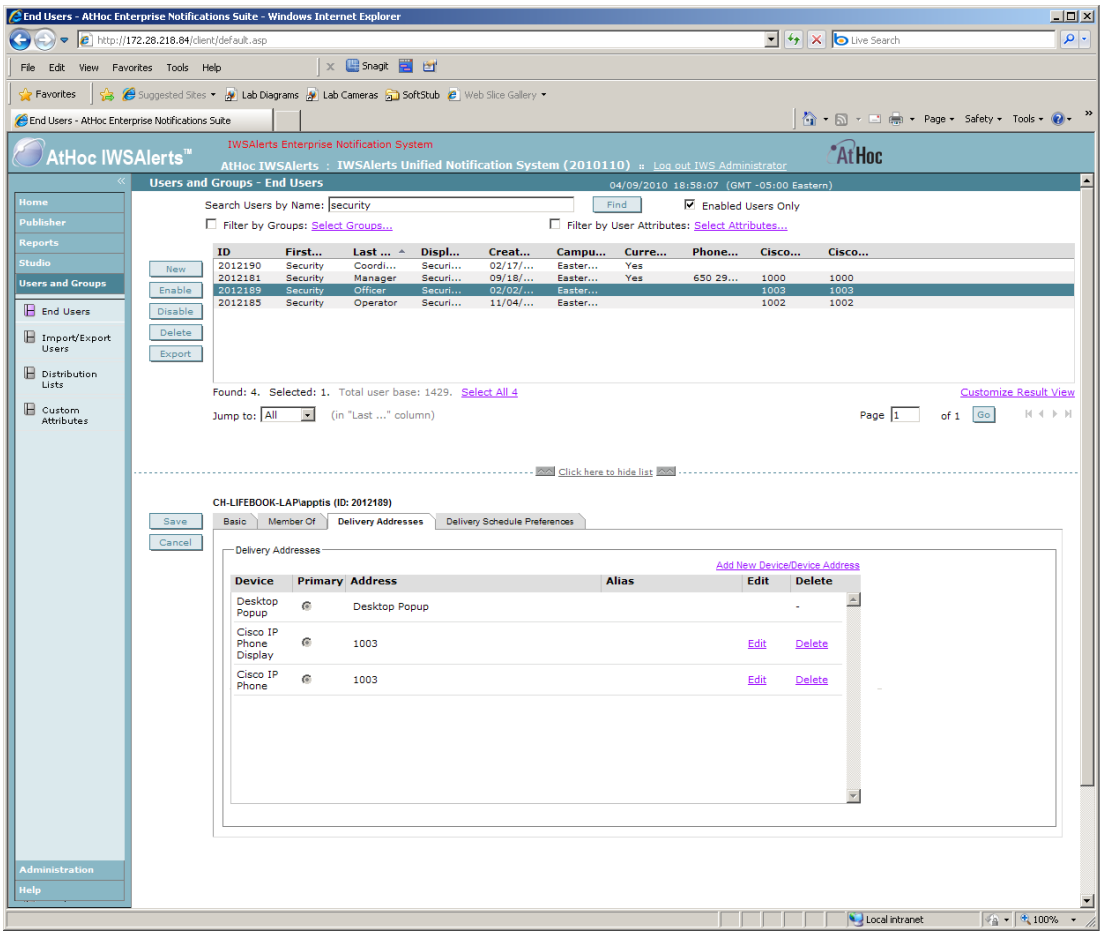
AtHoc Integration

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

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

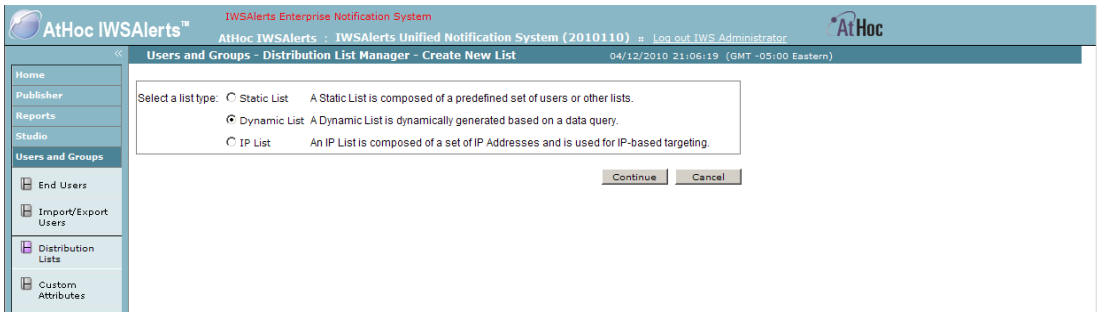
Step 1 Figure 5-51 shows how to create end users. In this example several end users are created. They have extension number 1000, 1002, 1003 respectively.

Figure 5-51 Create End Users



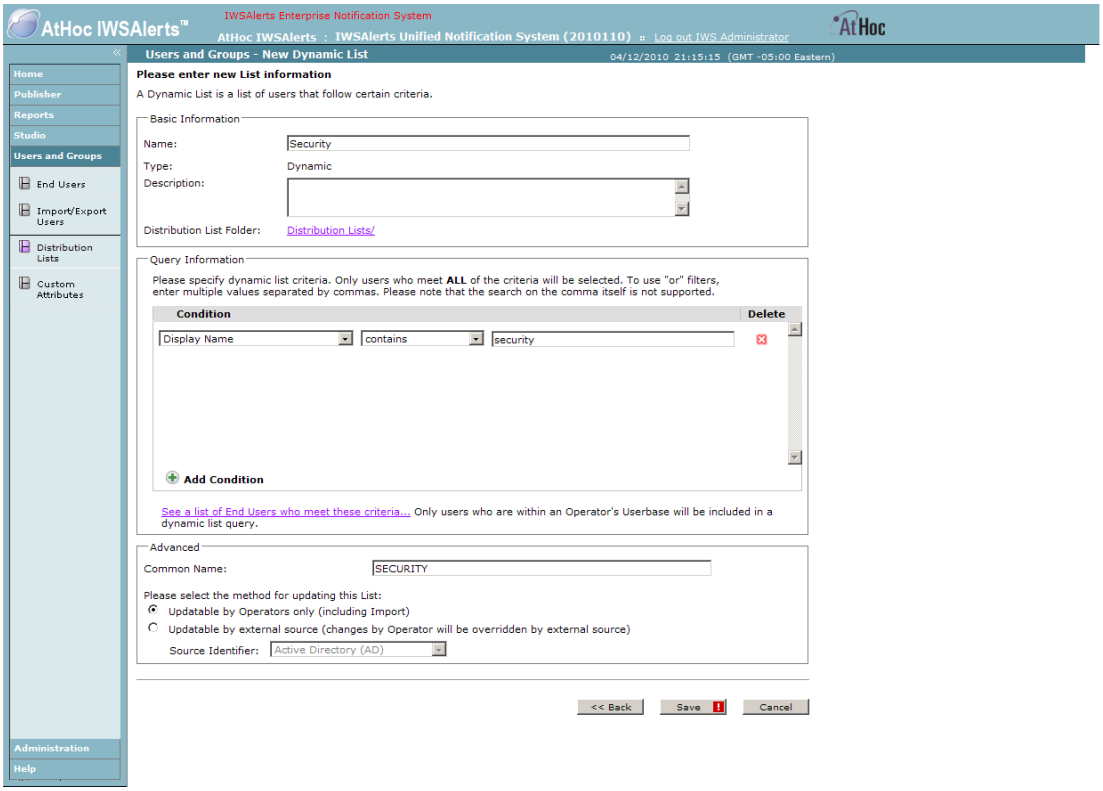
Step 2 Create a distribution list, as shown in Figure 5-52.

Figure 5-52 Specify a Dynamic List



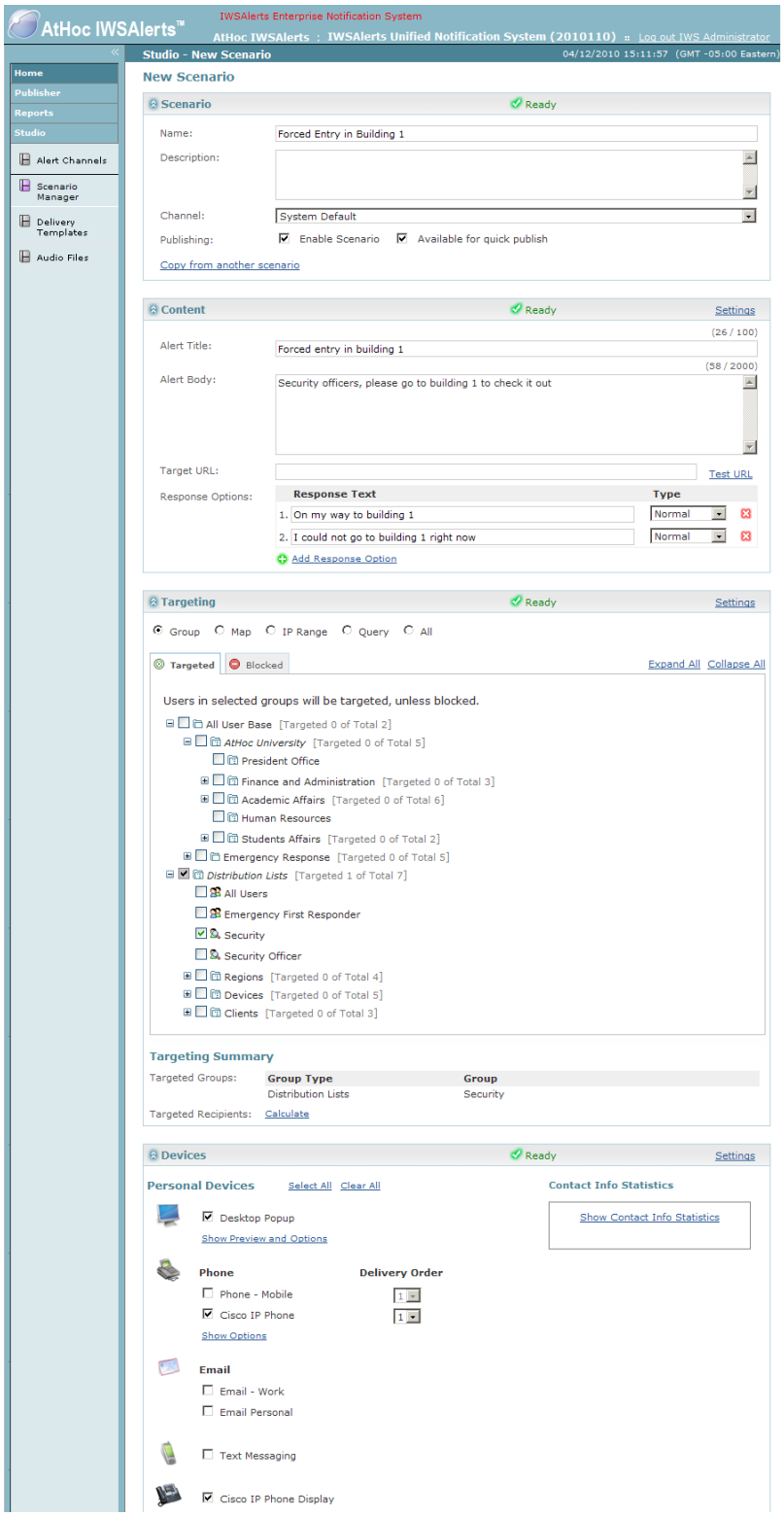
Step 3 Specify conditions for the list, as shown in Figure 5-53.

Figure 5-53 Specify Conditions for the List



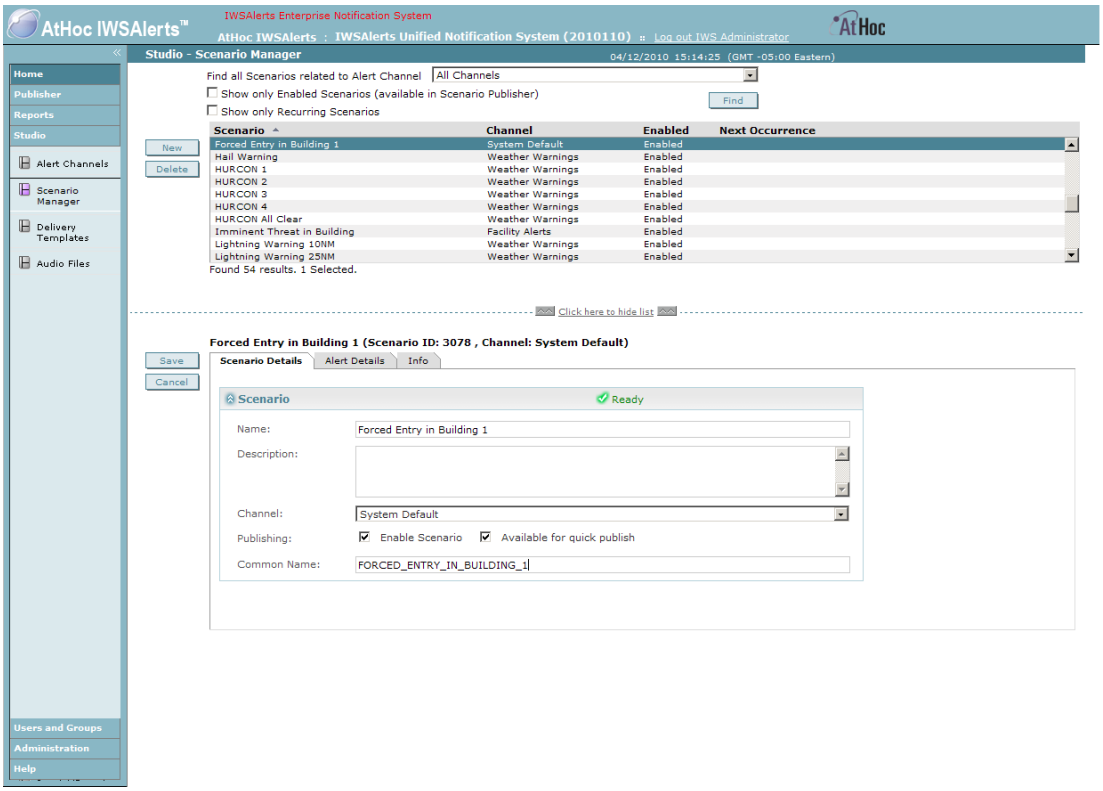
Step 4 Create a scenario, as shown in Figure 5-54. Here a scenario called “forced entry” is created.

Figure 5-54 Create a Scenario—Forced Entry



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

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



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

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

Phones will ring to notify about the forced entry incident.

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

Integrating AtHoc and Surveillint

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

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

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

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

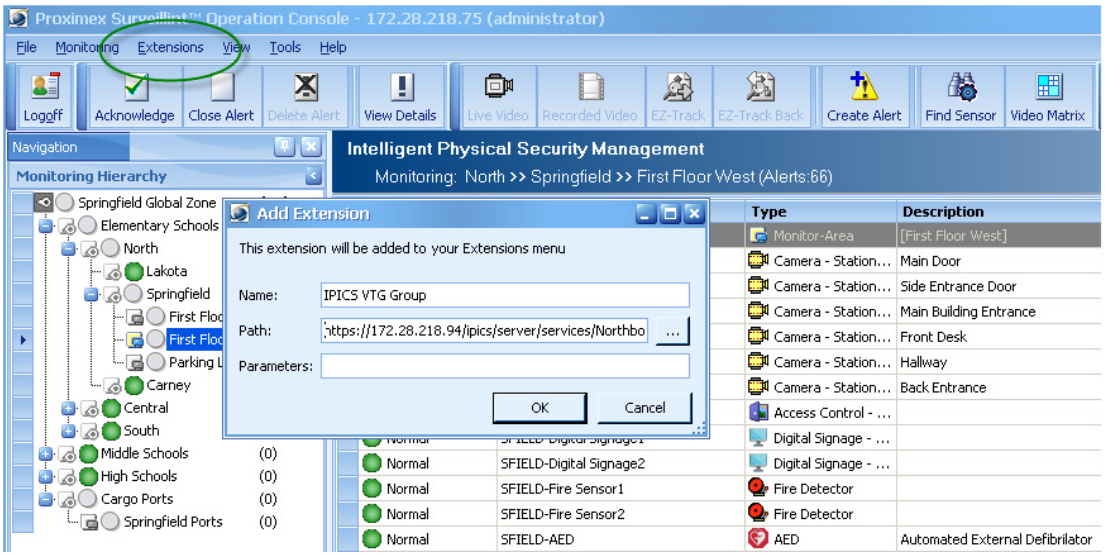
Configure Acting on Alerts through "Extensions"

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

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

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

Figure 5-56 Extensions



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

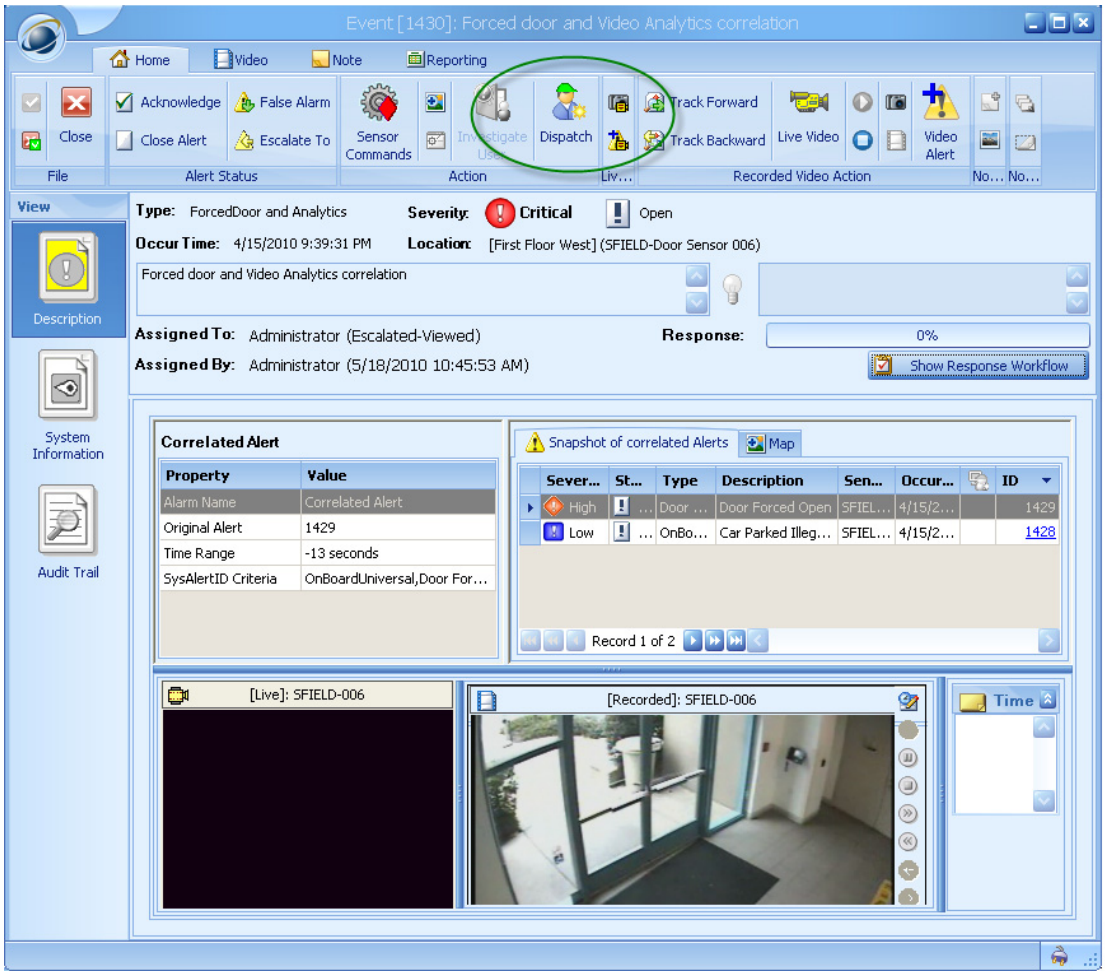
Configure Acting on Alerts through the "Dispatch" Button

To enable the Dispatch Button, perform the following steps:

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

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

Figure 5-57 Dispatch Button



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