

# 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.



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.



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.

СРАМ	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)

Table 5-1 List of Integration Examples

# **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.



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.

🧕 General Integration Module C	onfiguration	
-Installed general integration modules (a	dd or remove instances)	
🗾 🤿 Module Name 🔷	Description 🕺 🎑	+
Agent¥I (3.3)	AgentVI plugin for Surveillint 🕺	Add Instance
AMAG (6.0)	AMAG connector plugin for Surveillint 🛛 💸 📄	
AxisEncoder (1.0)	Axis Encoder connector for Surveillint 🕺	đ
Bosch (7.0)	Bosch Security plugin for Surveillint 🛛 🔌 💻	Refresh
Commend (1.0)	Intercom-Commend connector plugin for Surveillint 🛛 💸	
▶ 🔽 CPAM (1.1)	Cisco Physical Access Manager plugin for Surveillint 🛛 🔀	
DMP (1.0)	Digital Monitoring Products plugin for Surveillint 🕺	
GEPP (4.0)	GE Picture Perfect plugin for Surveillint	
HirschVelocity (3.1)	HirschVelocity plugin for Surveillint	
Record 6 of 21	<u>&lt;</u>	
Module Instances for CPAM (1.1)		
🚔 🚔 Instance Name 🛛 Desc	ription Deployed 📈 🤾	
•	1×10 1×17	X
		Configure
		<u>R</u> emove
Record 1 of 1		
		Class
		Liose

#### 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.

🗿 Eisco PAM	Server A	dministration -	Microsoft Internet Evolu	rer				
File Edit	View F	avorites Tools	Help					
Back 👻	<u>ب</u>	💌 🖻 🏠	) 🔎 Search   👷 Fav	orites 🧭 👔	2- چ 📧	• 📃 🏭		
Address 🦉 H	http://172.	28.218.77/status					-	- 🔁 Go
Links 💽 Lab	Diagrams	📦 Lab Cameras	;					
cisco	Cisc	D PAM Se	erver Adminis	tration	Welcome	🔓 Log Out	④About	🕜 Help
Monitoring	Setup	Commands	Launch CPAM Client	Downloads				
Monitoring :	> Status							
Server Admin Sta Server Mo Version: Serial Num High Avail	ate: ode: nber: ability Au	dit:	Up Active 1.2.0 0015179 disabled	0A1CB		S	top	
Services TFTP Serv Web Servi	ice ice API		Up Enabled			S	top ;able	

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.

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

Proximex our veilint. Environmen	t Management	
ile <u>M</u> onitoring Ma <u>p</u> <u>T</u> ools <u>H</u> elp	_ <b>K</b>	
lonitoring Hierarchy	i 🔟 🖻 🔜 i 🕹 🖬 🔞 🖬 🏟 🥥 🔎 🔸 🗙 i	
<ul> <li>Springfield Global Zone</li> <li>G Elementary Schools</li> <li>G M North</li> </ul>	Proximex Surveillint <sup>™</sup> Environment Management - (First Floor East) [Design Mode]: Modify North >> Springfield >> First Floor East	
Cargo Ports		
🛞 🕺		

### **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.

🕙 Policies - Mozilla Firefox							<u>_ 🗆 ×</u>
<u>Eile E</u> dit <u>Vi</u> ew Hi <u>s</u> tory <u>B</u> ookmar	'ks	<u>T</u> ools <u>H</u> elp					
🔇 🔊 - C 🗙 🏠 🛛	alala <mark>Cisco</mark>	172.28.218.94 https://172.28.2	18.94/ipics_server/ippe/Ma	nagePolicies.do	1	🗧 🕶 Google	P
📄 Lab Cameras 📄 Event Generator							
Seco Policies		÷.					-
cisco Cisco IPICS Ac	dm	ninistration Consol	e - 4.0(0.031)				Logout   About
Server Policy Engine	Р	Policy Management: <b>Policie</b>	s				<u> </u>
✓ □ Policy Management		Policies			Items 2	-1 of 1   Rowsper	page: 10 🔹 Go
Policies		Name Name	Туре	Action Names	Trigger Names	Ops View	Prompt
Execution Status		First Response	Multi-Purpose	CommandCenter		SYSTEM No	t Recorded
		Add Delete Acti	vate Associations		Pa	ge 🚺 of 1 🚺	
			Source of: htt	:ps://172.28.218.94/ipics_se	erver/ippe/ManagePoli	cies.do - Mozilla Firefo	× ×
			<u>File Edit View</u>	/ <u>H</u> elp			
			<pre>%" border="0</pre>	" cellspacing="0" cl	Lass="cuesTableTi	tleBg"> <td< td=""><td>class="cuesTab</td></td<>	class="cuesTab
	•		tById('pagin =r1" style="	g_policyTable').inne width:100%;overflow:	erHTML=' <nobr><sp :hidden;"&gt;<table< td=""><td>an class="cues] id="policyTable</td><td>'ablePagingItem: HeaderRow" <b>bas</b>ı</td></table<></sp </nobr>	an class="cues] id="policyTable	'ablePagingItem: HeaderRow" <b>bas</b> ı
			ass="cuesTab	leSelectionColumn" w	ridth="20" class=	"cuesTableSelec	tionColumn"> <i< td=""></i<>
			th>				
			names				
			=w				
			div> <div id="&lt;/td"><td>"policyTableScroller</td><td>c2" class="cuesTa</td><td>bleScrollableBg</td><td>" style="width</td></div>	"policyTableScroller	c2" class="cuesTa	bleScrollableBg	" style="width
			d> <a <="" href="#&lt;/td&gt;&lt;td&gt;" onclick="doShowPo" td=""><td>licyDetails('29')</td><td>:"/&gt;First Respo</td><td>nsek/a&gt; ▼</td></a>	licyDetails('29')	:"/>First Respo	nsek/a> ▼	
🕨 🗞 Dial Engine					,		
~	•	( <u> </u>	× Find: First	Response 😽 Next	👚 Previous 🖌 Highlight	all 🗖 Match case	Reached end of page, •
Done			Line 903, Col 74				//

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?policy Id=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.

🖉 Devices - AtHoc Enterprise Notifications Suite - Windows Internet Explorer 💌 😽 🗙 🗔 Live Search 😋 😔 🔻 🙋 http://172.28.218.84/client/default.asp 2 🗴 🛄 Snagit 🧮 😁 File Edit View Favorites Tools Help 🖕 Favorites 🛛 🖕 🏉 Suggested Sites 🔹 🔊 Lab Diagrams 🔊 Lab Cameras 🔂 SoftStub 🧧 🏠 • 🔝 - 🖃 🌧 • Page • Safety • Tools • 🔞 • 🔗 Devices - AtHoc Enterprise Notifications Suite \*At Hoc AtHoc IWSAlerts<sup>™</sup> Administration - Devices • Device Name Device ID Default Template Def. Template ID Statu 998 1004 1006 1005 26 27 28 31 1001 21 Enabled Enabled Disabled Disabled Disabled Disabled Disabled IPICS Policy OCS Instant Messag... OCS Phone Pager (Numeric) Pager (Numeric) Pager (Two Way) Phone - Emergency Phone - Home Dhone - Home IPICS Policy OCS IM OCS Phone 2007 2009 2008 OCS Phone Pager (Numeric) Pager (One Way) Pager (Two Way) Phone - Emergency Phone - Home Phone - Home 2018 2019 2020 2023 📙 Setup 2004 2013 Disabled Disabled • My Details Phone - Home Jound 33 results. 1 Selected. 21 🔒 Operators 📙 Virtual Systems Click here to hide list 🔒 Devices IPICS LMR TTS (ID: 998) Agents Save Basic Disable 🝓 System Tasks Device Name: IPICS LMR TTS Status: Enabled Archive Common Name: httpIPICSLMRTTS Delivery Type: Bulk Immediate (Push Based) Users Can Edit Address: Yes Quiet Mode Supported: Yes Device Template Supported: No Default Template: Simplest Template (998) 💌 Delivery Order Supported: No User Order Supported: No Preset for New Users: No Preview available: No Device Protocol ID: HTTPLMRTTS Users Can Remove All Device Addresses Delivery Agent: N/A Max Retries: Retry Interval: 0 0 Device MetaStore: • CmetaStore>curl><![CDATA [https://172.88.218.94/ipics\_services/NorthboundService/executePolicy? policy12429message=ATTENTION,+ATTENTION,+[TITLE]+[BOD7]]] Device Protocol MetaStore: \* -229141 Local intranet 🖓 🔹 🔍 100%

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.

1

Publisher - Alert Publisher	04/30/2010 17 <u>:00:52 (GMT -05:00 Easter</u>
Publish a Scenario : 1 - Trip Wire Activated	
Scenario	
Name: 1 - Trip Wire Activated	
Description:	Review & Publish
Channel: Facility Alerts	Or, <u>Select Another Scenario</u>
	✓ Ready For Publishing
Contant	Ø Deady
V Content	Keauy
Targeting	🗸 Ready
Group ○ Map ○ IP Range ○ Query ○ All	
S Targeted Slocked	Expand All Collapse All
Users in selected groups will be targeted, unless blocked.	
🖬 🔲 🛅 All User Base [Targeted 0 of Total 2]	
AtHoc University [Targeted 0 of Total 5]      Resident Office	
E      Finance and Administration [Targeted 0 of Total 3]	
Academic Affairs [Targeted 0 of Total 6]	
Human Resources      G Students Affairs [Targeted 0 of Total 2]	
Emergency Response [Targeted 0 of Total 5]	
Distribution Lists [Targeted 1 of Total 9] All Users	
🔲 🕰 Building security	
Campus Security	
Emergency First Responder	
Security Officer	
Constant Regions [Targeted 0 of Total 4]      Provides [Targeted 1 of Total 5]	
Second Se	
I B Device LMR TTS ■ B Device Strobe	
🗌 🕿 Twitter	
🖷 🗖 🛱 Clients [Targeted 0 of Total 3]	
Targeting Summary	
Targeted Groups: Group Type Group	
Distribution Lists Device	LMR TTS
Devices	🌌 Ready
Personal Devices Select All Clear All	Contact Info Statistics
Desktop Popup	Show Contact Info Statistics
Show Preview and Options	
None Delivery Order	
Phone - Mobile	
Cisco IP Phone 1 V Show Options	
Email	
Email Personal	
📓 🔄 Text Messaging	
Cisco IP Phone Display     Show Options	
Mass Communication Devices Select All Clear All	
Giant Voice	
Show Options	
<b>V</b>	
LMR	
LMR	

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).





# **Creating HTML Content for the DMP**

Proximex Surveillint

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.



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">
 
   
<b><font color="#fffffff" size="7">!ALERT!</font></b> 
<b><font color="#ffffff" size="7">Chemical Leak Reported</font></b><br>
<b><font color="#ffffff" size="7">Avoid South Building
Exits</font></b><br>
<blockquote>
      <blockguote>
       <blockquote>
         <blockquote> <br>
          <img
src="http://10.94.162.201/video.jpg?framerate=0&source=p_s1_Englewood_-_4500-1_1">
          <b><font color="#fffffff" size="5">Still
Snapshot</font></b><br>
```

```
</blockquote>
</blockquote>
</blockquote>
</blockquote>
</blockquote>

</cr>

</tobedy>

</body>

</body>
```

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



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=h ttp://<web\_server\_ip\_address>/<web\_page\_name>&init.TVZILLA\_URL=http://<web\_server\_ip\_add ress>/<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.

AtHoc IWS	SAlerts™	IWSAlerts Enterprise N AtHoc IWSAlerts	lotification System WSAlerts Unified Noti	fication Syst	tem (2010110)	" Change System	m Log out Ar	lmin User
«	Users and	Groups - End Users			04/30	D/2010 12:40:59	(GMT -05:00 E;	astern)
Home	s	Search Users by Name: DI	MP		Find	🛛 🗹 Enab	led Users Only	
Publisher	Г	Filter by Groups: Select	Groups		🗌 Filter by User	Attributes: Select	Attributes	
		ID 🔺 First	Last Disnl	Creat	Campu Curi	re Phone	Cisco	Cisco
Studio	New	2012174 DMP	One DMP1	06/13/				
Users and Groups	Enable	2012191 DMP	User DMP Lo	02/19/	Easter			
📙 End Users	Disable							
H Import/Export Users	Delete							
Distribution		Found: 2. Selected: 1.	Total user base: 1429. Si	elect All 2			Customiz	e Result View
Custom Attributes		Jump to: All				Page 1	of 1 Go	н < > н
	Cancel	Basic Member Of User Attributes Expand all Collapse all	Pelivery Addresses Deliver	r Schedule Prefe	rences	E	dit attributes	
		- Basic Attribu	tes	Cha				
		First Name:	DMP	Sta	tus:	Enabled		
		Last Name:	One	Car E	npus Regions:			
		Display Name:	DMP 1	Emi	ergency Response:			
		AtHoc University:		ROP	8: ///_=			
		Username:	dmp1	Med	icai iraining: —			
		Created On:	06/13/2009 03:57:59	Use	r Type:	Device		
		Personnel Ac	countability	Mv	Current Location			
				му	Carrent Location:			
		Medical Need	verity	Hou	ising Need:			
Administration		Transportation Nee	d:	HOU	ising Need:			•
Help								

#### 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.

Γ

♥AtHoc IW	SAlerts™	AtHoc IV	s Enterprise I /SAlerts :	Notification Syst IWSAlerts Un	nified Notific	ation Syst	em (201011	LO) = <u>Cha</u>	nge System	Log out Ad	<u>min User</u>	<b>Č</b> Ať Ho
*	Users and	Groups - E	nd Users				(	04/30/2010	12:40:59 (GM	Г -05:00 Ea	stern)	
	s	earch Users	by Name: D	MP			F	ind	🗹 Enabled I	Jsers Only		
		Filter by G	Groups: <u>Selec</u>	t Groups			🔲 Filter by I	User Attribut	es: <u>Select Attr</u>	ibutes		
		ID A	First	last	Displ	Creat	Campu	Curre	Phone	fisco	fisc	
	New	2012174	DMP	One	DMP 1	06/13/	campan	current	THOREM	cipeoin	UIDE	
sers and Groups	Enable	2012191	DMP	User	DMP Lo	02/19/	Easter					
End Users	Disable											
	Delete											
Import/Export Users	Evport											
Design and the second	Export											
Lists		Found: 2 9	Coloctod: 1	Total usar basa	v 1429 Sele	ot All 2					Curtor	nine Recult View
Custom			selected, I.	Total user base	5, 1425, <u>3616</u>	CC AIL 2					<u>Custor</u>	
Attributes		Jump to: [A	Y						Page	1	of 1	
		dmp1 (1D: 20'	12174)			Click here t	o hide list 🖂 -					
	Save Cancel	dmp1 (ID: 20' Basio M Delivery	12174) Member Of Addresses	Delivery Addresse	es Delivery	Schedule Pref	o hide list 🔊 -					]
	Save Cancel	dmp1 (ID: 20' Basio M Delivery	12174) Adember of Addresses	Delivery Addresse	es Delivery	Click here t	o hide list and -		Add Ne	w Device/De	vice Addres	2
	Save Cancel	dmp1 (ID: 20' Basio M Delivery Device	12174) Aember of Addresses	Delivery Addresse	es Delivery	Schedule Pref	o hide list and -	lias	Add Ne	w Device/Dev Edit D	vice Addres elete	2
	Save Cancel	dmp1 (ID: 20' Basio M Delivery Device DMP	Addresses	V Address 172.28.218.3	es Delivery	Schedule Pref	o hide list 🔊 -	lias	Add Ne	w Device/De Edit D Edit -	vice Addres elete	2
	Save Cancel	dmp1 (ID: 20/ Basio h Delivery Device DMP	Addresses Primary	y Address 172.28.218.	as Dolivery	Click here t	o hide list and -	lias	Add Ne	w Device.De Edit D Edit -	vice Addres elete	2
	Save Cancel	dmp1 (ID: 20/ Basio N Delivery Device DMP	Addresses	Pelivery Addresse y Address 172.28.218.	74	웹 <u>Click here</u> t	o hide list and -	lias	Add Ne	w Device/Der Edit D Edit -	vice Addres elete	

#### 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.

	SAIerts	AtHoc IWSAlerts : IWSAlerts Unified N	lotification System (2010	)110) : <u>Change S</u>	System Log out Admin User	<b>ČAť Hoc</b>
~	Studio - S	Scenario Manager		04/30/2010 12:48	8:21 (GMT -05:00 Eastern)	
		Find all Scenarios related to Alert Channel	Channels		•	
		Show only Enabled Scenarios (available in Sc	enario Publisher)			
		Show only Recurring Scenarios			Pillo	
		Scenario 🔺	Channel	Enabled	Next Occurrence	
lio	Nov	Emergency Action Message Transmission	Command Post	Enabled		
a :	new	Emergency Conference	System Default	Enabled		
Services	Delete	EMNS lest	Escility Alasta	Enabled		
D. state and		Fire in Banang Flash Flood	Weather Warpings	Enabled		
Buttons		Forced Entry in Building 1	System Default	Enabled		
Toolbar Builder		Hail Warning	Weather Warnings	Enabled		
rooibar builder		HURCON 1	Weather Warnings	Enabled		
Catalog Builder		HURCON 2	Weather Warnings	Enabled		
catalog builder		HURCON 3	Weather Warnings	Enabled		
Alert Channels		Found 54 results. 1 Selected.				
Scenario						
Manager			Click here to hide lis	<u>t 🗠</u>		
Deliveru						
Templates		Forced Entry in Building 1 (Scenario ID: 3	078 , Channel: System Def	fault)		
	Save	Scenario Details Alert Details Info				
Audio Files	Save	Scenario Details Alert Details Info				
Audio Files	Save Cancel	Scenario Details Alert Details Info				
Audio Files	Save Cancel	Scenario Details Alert Details no		🗸 Ready	Settings	
Audio Files	Save Cancel	Scenario Details Alert Details Info		🗸 Ready	<u>Settinas</u>	
Audio Files	Save Cancel	Scenario Details Alert Details Info		✔ Ready	Settings	
Audio Files	Save Cancel	Scenario Details Alert Details Info		🗸 Ready	<u>Settings</u> Settings	
Audio Files	Save Cancel	Scenario Details Alert Details Info Content		✔ Ready ✔ Ready	<u>Settings</u> Settings	
Audio Files	Cancel	Scenario Details Alert Details Info		✓ Ready ✓ Ready	<u>Settinas</u> Settinas	
Audio Files	Save Cancel	Scenario Details Alert Details Info		✔ Ready ✔ Ready ✔ Ready	<u>Settinas</u> <u>Settinas</u> <u>Settinas</u>	
Audio Files	Cancel	Scenario Details Alert Details Info		✔ Ready ✔ Ready ✔ Ready	<u>Settinas</u> <u>Settinas</u> <u>Settinas</u>	
audio Files	Cancel	Scenario Details Alert Details Info		✓ Ready ✓ Ready ✓ Ready ✓ Ready	Settinas Settinas Settinas Settinas	

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.

Γ

#### Figure 5-17 **Target Devices**

Forced Entry in Building 1 (Scenario ID: 3078 , Channel: System Detault) Scenario Details Alert Details Info

S Content	🗸 Ready	<u>Settings</u>
* Targeting	✓ Ready	<u>Settings</u>
⊙ Group C Map C IP Range C Query C All		
Sargeted Slocked	<u>Expar</u>	nd All Collapse All
Users in selected groups will be targeted, unless blocked.		
All User Base [Targeted 0 of Total 2]		
□ □ □ AtHoc University [Targeted 0 of Total 5]		
G President Office		
🗉 🗖 📴 Finance and Administration [Targeted 0 of Total 3]		
🗷 🗖 📴 Academic Affairs [Targeted 0 of Total 6]		
🔲 🛅 Human Resources		
🗷 🗖 📴 Students Affairs [Targeted 0 of Total 2]		
🗷 🗖 🛅 Emergency Response [Targeted 0 of Total 5]		
🖃 🗹 🛅 Distribution Lists [Targeted 2 of Total 9]		
🔲 🕿 All Users		
🔲 🕰 Building security		
🔲 💁 Campus Security		
🗌 📽 Emergency First Responder		
🗹 🔍 Security		
Security Officer		
H Regions [Targeted U of Total 4]		
🖃 🗹 🛅 Devices [Targeted 2 of Total 5]		
🗹 🕿 Device DMP		
🗌 🕿 Device EAS		
🗹 🕿 Device LMR TTS		
🔲 🕿 Device Strobe		
🗌 🕿 Twitter		
Clients [Targeted 0 of Total 3]		

* Devi	ces	🗸 Ready	Settings
Person	al Devices Select All Clear All	Contact Info St	atistics
4	✓ Desktop Popup Show Preview and Options	Show Cont	act Info Statistics
4	Phone Delivery	Order	
	Phone - Mobile		
	Cisco IP Phone		
	Show Options		
	Email		
	🗖 Email - Work		
	🗖 Email Personal		
	☐ Text Messaging		
	🔽 Cisco IP Phone Display		
	Show Options		
Mass C	Communication Devices Select All Cle	ar All	
Ð	🗖 Giant Voice		
	Show Options		
1	LMR		
	TIPICS LMR TTS		
	IPICS Policy		
	Show Options		
	🗖 Strobe Light		
-			
t	Twitter		
	T EAS		

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.

AtHoc IWS	SAlerts™	IWSAlerts Enterprise I	Notification System	ification Suctom ( 2	010110) - Los o	ut Th
"		1 - Trip Wire Activated		Eacility Alerts	Enable	
		2 - Event on Camera		Facility Alerts	Enable	-
Home		2a - Intruder Detected E	OC Collab	Facility Alerts	Enable	
		2b - Security Event on Ca	ampus	Facility Alerts	Enable	
Publisher		6 - EDU - School Evacuat	ion	Facility Alerts	Enable	
Reports		8.1 MED - Code BLUE		Facility Alerts	Enable	
Reports		8.2 MED - Code PINK		Facility Alerts	Enable	
Studio		8.3 MED - Code GREEN		Facility Alerts	Enable, 💙	
		Found 54 results, 1 Selec	ted.			
H Alert Channels			Click here to hide list	<u>.</u>		-
Manager		2 - Event on Camera (	Scenario ID: 3048 . Ch	annel: Facility Alert	·s)	
📔 Delivery Templates	Save	Scenario Details Ale	ert Details Info			=
📙 Audio Files	Cancel	Scenario			🝼 Ready	
		Name:	2 - Event on Cam	era		
		Description:				
Users and Groups		Channel:	Facility Alerts			
Administration		Publishing:	🗹 Enable Scenario	🗹 Available for qui	ck publish	
Help		Common Name:	VIDEO			~
<u>}</u>					🧿 Internet	

#### 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.

🛗 http://10.94.162.201/mfo.bwk?type=proxy8dsplay=html												
		P	roxy Se	erver Information								
name	status	type	exec	source	mediatype	f/b-rate	quality	width	height	model	res	format
p_EnglewoodPanasonic_NS202	Running	panasonic_ns_202	proxy	1@10.94.162.248:80	jpeg	20.00000	50	640	480	104	4cif	ntsc
p_EnglewoodPanasonic_NS202_OV	Running	panasonic_ns_202	proxy	1@10.94.162.248:80	jpeg	7.50000	50	320	240	104	cif	ntsc
p_EnglewoodAxis210A-1	Running	axis210	proxy	1@10.94.162.252:80	jpeg	20.00000	50	640	480	27	4cif	ntsc
p_EnglewoodAxis210A-1_OV	Suspended	axis210a	proxy	1@10.94.162.252:80	jpeg	7.50000	50	320	240	56	cif	ntsc
p_EnglewoodAxis210A-2	Running	axis210	proxy	1@10.94.162.217:80	jpeg	7.50000	50	320	240	27	cif	ntsc
p_EnglewoodAxis210A-2_OV	Suspended	axis210	proxy	1@10.94.162.217:80	jpeg	7.50000	50	320	240	27	cif	ntsc
p_EnglewoodAxis_213-1_0	Suspended	axis213	proxy	<u>1@10.94.162.226:80</u>	jpeg	15.00000	50	704	480	45	4cif	ntsc
p_EnglewoodAxis_213-1_OV	Suspended	axis213	proxy	1@10.94.162.226:80	jpeg	7.50000	50	352	240	45	cif	ntsc
p_EnglewoodAxis_232D_0	Running	axis232	proxy	1@10.94.162.215:80	jpeg	20.00000	50	704	480	44	4cif	ntsc
p_EnglewoodAxis_232D_OV	Running	axis232	proxy	1@10.94.162.215:80	jpeg	7.50000	50	352	240	44	cif	ntsc
p_EnglewoodIQeye_501_1	Running	iqeye501	proxy	1@10.94.162.228:80	jpeg	20.00000	50	640	512	86	4cif	ntsc
p_EnglewoodIQeye_501_OV	Running	iqeye501	proxy	<u>1@10.94.162.228:80</u>	jpeg	7.50000	50	320	256	86	cif	ntsc
p_s1_Englewood2500-1_1	Running	cisco-2500	proxy	1 1@10.94.162.220:80	jpeg	5.00000	50	720	480	110	d1	ntsc
p_s1_Englewood2521-1_OV_1	Running	cisco_252xV	proxy	1 1@10.94.162.223:80	jpeg	7.50000	50	352	240	173	cif	ntsc
p_s1_Englewood2521-2HW_1	Running	cisco_252xV	proxy	1 1@10.94.162.224:80	jpeg	7.50000	50	720	480	173	d1	ntsc
p_s1_Englewood2521-2_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_Englewood4500-1_1	Running	cisco_4500	proxy	1 1@10.94.162.222:80	jpeg	20.00000	50	704	480	168	4cif	ntsc
p_s1_Englewood4500-1_OV_1	Running	cisco_4500	proxy	1 1@10.94.162.222:80	jpeg	5.00000	50	352	240	168	cif	ntsc
p_sT_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												

#### Figure 5-21 List of Running 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.





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



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.

₩ Object¥ideo Managemen	t Tool	
ObjectVideo Managemen           File         License         Sensor         Help           Services         Server Properties         Daemon Properties           Daemon Properties         -         -           Services         -         2520-21           -         -         4500-1           -         -         2521-2           -         2521-1	E Tool Sensor Properties Sen Sensor Name: Sensor Type: Sensor ID: Video Source: Auto-Start: Store Forensics Data:	
	Start Status:	Started

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, 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.

Γ

Gile Configuration Hale			- <b>-</b> ×
		Connect Status: Connected Server Status: Online since 3/23/10 2::	34 PM
RULE MANAGER	Properties View Rules	Schedules Filters	
⊟–ŞI ObjectVideo Server	Name	Active	Event
— E Group 001 — E Group 002	+ ≪ Rules ↓ ↓ ♥ SFIELD-025		
⊞-1000 SFIELD-025			
			▲ ▼
	New	View Edit Delete	Refresh
OV ObjectVideo Ready.	I		

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.

Rule Wizard: E	dit Event			x
Create New	Event			
Copy From E	xisting Eve	ent		
Existing Eve	nt: Car Par	ked Illegaly Event		•
lame: Car Park	ed Illegaly Ev	/ent		
Scene Cha	nge			
 Tripwire	Ŭ			
🗌 Multi-line Ti	ripwire			
🗹 Partial Viev	v			
🗌 Full View				
Event Specificat	ion			
Detect when				
[Vehicle] [Loite	rs] <u>Car Pa</u>	rked Illegally(Gr	ound Plane)	
where loitering	time is at l	least <u>0 minutes</u>	45 seconds	
				Edit Filters
				ī — — — — — — — — — — — — — — — — — — —

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.

🙀 Area	Editor	
O Cre	eate New Area	
O Co	py From Existing Area	
Exi	sting Area: 💌 🔻	
Name:	Restricted area	
Desc:		
	🖲 (Ground Plane) 🛛 (Image Plane)	
	Cancel Clear Refresh Save	2001 E

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.

```
<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.

Rule Wizard: Create Response     Oreate New Response     Cropy Existing Response	X
Response: Car Parked Illegally Response	<b></b>
System Resp	Custom Response Fields
Display Alert in Real-time Alert Sound: NONE  Solution Require User Acknowledger C Log Alert in Database Alert Message Alert Message Alert Detect when [Vehicle] [Left behind in] where the object is left for at least 0 minutes	Key         Message           HTTP_Trigger         http://172.28.218.80/vsom/service/event_nd
	New Delete
	OK Cancel
Cancel	Custom Fields

#### 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



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.



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.

ſ

e <u>A</u> ction <u>V</u> iew						
→   🗉   🗳						
Services (Local)	Name 🛆	Description	Status	Startup Type	Log On As	
	NT LM Security Support Provider	Provides s		Manual	Local System	
	🆓 ObjectVideo Alert Bridge Service		Started	Automatic	Local System	
	🆓 ObjectVideo Alert Logger		Started	Automatic	Local System	
	🖓 ObjectVideo Communication Server		Started	Automatic	Local System	
_	🖉 🎇 ObjectVideo Daemon Service		Started	Automatic	Local System	
	📲 🎇 ObjectVideo Notification Service	Enables so	Started	Automatic	Local System	
	Reformance Logs and Alerts	Collects pe		Automatic	Network S	
	Rug and Play	Enables a c	Started	Automatic	Local System	
	Regional Serial Number Service	Retrieves t		Manual	Local System	
	Rint Spooler	Manages al	Started	Automatic	Local System	
	Rotected Storage	Protects st	Started	Automatic	Local System	-
	Proximex ObjectVideo Connector Service		Started	Automatic	Local System	
	Remote Access Auto Connection Manager	Creates a		Manual	Local System	
	Remote Access Connection Manager	Creates a	Started	Manual	Local System	
_	Remote Desktop Help Session Manager	Manages a		Manual	Local System	
	Remote Procedure Call (RPC)	Serves as t	Started	Automatic	Network S	
	Remote Procedure Call (RPC) Locator	Enables re		Manual	Network S	
	Remote Registry	Enables re	Started	Automatic	Local Service	

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.

services						×
<u>File A</u> ction <u>V</u> iew	Help					
≻ →   🖬   😭 [	ᄚ ฿   😫 🖬   ▸ ■ ॥ ■▸					
🗞 Services (Local)	Name 🛆	Description	Status	Startup Type	Log On As	
	Network DDE DSDM	Manages D		Disabled	Local System	
	Network Location Awareness (NLA)	Collects an	Started	Manual	Local System	
	Network Provisioning Service	Manages X		Manual	Local System	
	NT LM Security Support Provider	Provides s		Manual	Local System	
-	ObjectVideo Daemon Service		Started	Automatic	Local System	
	📲 🍓 Office Source Engine	Saves inst		Manual	Local System	
	Reformance Logs and Alerts	Collects pe		Automatic	Network S	
	Rug and Play	Enables a c	Started	Automatic	Local System	
	Rortable Media Serial Number Service	Retrieves t		Manual	Local System	
	Rint Spooler	Manages al	Started	Automatic	Local System	
	Rotected Storage	Protects st	Started	Automatic	Local System	
	Roximex Bus Services	Proximex B	Started	Automatic	Local System	
	Revealed the services and the services and the services and the services are services and the services are services and the services are services ar	Proximex B	Started	Automatic	Local System	
	Roximex Http Event Listener Service	Proximex H	Started	Automatic	Local System	
	Revealed the services with the services with the services and the services and the services are services and the services are services and the services are servi	Proximex E	Started	Automatic	Local System	
_	📕 🍓 Proximex ObjectVideo Connector Service		Started	Automatic	Local System	
	📲 🍓 Proximex Sensor Management Services	Proximex S	Started	Automatic	Local System	
	Remote Access Auto Connection Manager	Creates a		Manual	Local System	
	Remote Access Connection Manager	Creates a	Started	Manual	Local System	-
	Extended Standard					

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.

WobjectVideo Management Too	1		
File Sensor Help			
Services Pro	perties		
	General		
	Installation Key:	ccfb2b3	
	Server Address:	10.94.162.232	
	Port:	8076	
	Remote Access		
	Allow Remote Acces		
	Remote Port:	8077	
ſ	Time Synchronization -		
	C Synchronize system	clock to	
	Server: 127.0.0.1	Port:	8878
	every 1.00	Hours	
	C Allow time synchron	ization on port 8878	
		F	Apply
IU			000

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.

🜉 Object Video Managemen	t Tool	
File Sensor Help	Norma I	
Daemon Properties	Status	
	ObjectVideo Daemon Service Running	Stop
	Stop All Services Start All	Services
1		8

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.



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

Sensor Mapping					
VEW (ObjectVideo, Inc.)					
Device Name: SFIELD-025					
Monitoring Tree:	Selected area's sense	or(s):			
Springfield Public Schools	Name	Туре	Description	ID	<b>^</b>
Elementary Schools	[Parking Lots]	🧾 Monitor-Area	[Parking Lots]		61
North	SFIELD-021	📴 Camera - Stationary	Parking Lot		68
Lakota	SFIELD-022	📴 Camera - Stationary	Parking Lot		69
Birst Floor Fast	SFIELD-023	📮 Camera - Stationary	Parking Lot		70
- First Floor West	SFIELD-024	Camera - Stationary	Parking Lot		71
Parking Lots	SFIELD-025	📮 Camera - Stationary	Parking Lot - Side		73
📄 🐻 Central					
🔄 🛃 South					
Middle Schools					
High Schools					
Zone Unassigned VEW (O					
Cone Unassigned Http Eve					
				ОК	Cancel
				0.00	

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

0	Proximex Surveilli	int™ Sensor Mapping	Manager		
5	ensor Mapping	Management			
	Add, Edit, Delete	e Sensor Mappings			
	r				
Ap	oplication Name:	VEW (ObjectVideo, Inc.)			
	Device Name	Area Name	Sensor Name	Туре	Add
	Panasonic NS202	ENG1	Englewood - Panasonic	🛃 Camera - PTZ	Edit
	2521-1	First Floor West	SFIELD-002	📮 Camera - Stationary	
	SFIELD-025	Parking Lots	SFIELD-025	📮 Camera - Stationary	Delete
					Close

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.



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 5-39 Video Analytics Alert



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

I

- 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*.



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).

ſ

heck to enable selected Video Service	Integration Module	7
🖌 📔 Yendor Type	Description	
🗸 🔽 Cisco	Cisco VSM 6.2 / VSOM 4.2 Conf	igure
	Disa	able
	Cisco Video Server Configuration	
	VSOM (Video Surveillance Operations Manager)	VSOM
	Use VSOM	
	VSOM: 172.28.218.80	
	VSMS (Video Surveillance Media Server)	
		Add
	► 10.94.162.201	Mdd
	172.28.218.82	Modify
a a surd to fit a fit a fit	172.28.218.81	Remove
Record 1 of 1 P P P	10.34.130.170	
ther service options		Test Connection
Disable video analytics when users	contr	
	Server Logon Name:	
	Server Logon Password:	

#### 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

Add Cisco VSM Serve	er 🗖 🗵	
VSMS (Video Surveillance Ma	edia Server) Configuration	
Server Name:	10.94.162.201	
Server Logon Name:	root	
Server Logon Password:	*****	
	OK Cancel	Ę
	OK Canta	5000

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.

	Cisc	o VSOM / VSM Server Device Brov	vser		×					
Selected Name: p_RTP10-K145 (10.34.130.170)										
VSOM (Video Surveillance Operations Manager): <a></a> <a></a> <a></a>										
۷	VSMS (Video Surveillance Media Server): 10.34.130.170									
		Name		ID						
₽										
Þ	<b>0</b> 4	p_RTP10-K145		1						
		p_RTP6P-K099_NW_Roof		2						
		p_SJC02-K406_SE_Parking_Lot_PTZ		3						
	<b>_</b> 4	p_SJC07-K419_SW_Parking_Lot_PTZ		4	=					
		p_SJC16-Lobby_B16		5						
		p_SJC18-Lobby_B18		6						
		p_s1_Camera_Compare_001_1		7						
		p_s1_Camera_Compare_002_1		8						
		p_s1_Camera_Compare_003_1		9						
Re		p_s1_Camera_Compare_004_1 Record 1 of 10		10						
	Export OK Cancel									

#### 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
```



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.

Γ

🖌 Name	<u>.</u>	Туре	Description	ID		Add
	000	The Comment Chattanamy	Deall February			Edit
SETEL	-006	Camera - Stationary	Back Entrance		68	Delete
	)-022	Camera - Stationary	Parking Lot		69	
SETEL	)-023	Camera - Stationary	Parking Lot		70	View
SETELD	)-023	Camera - Stationary	Parking Lot		71	Report
SEIELD	)-025	Camera - Stationary	Parking Lot - Side		73	-
SFIELD	)-31	Camera - Stationary	Classroom - Front		79	Import
SFIELD	)-32	Camera - Stationary	Classroom - Back		80	Importerri
SFIELD	-AED	S AED	Automated External (	Defi	78	Export
SFIELD	)-Digital Signage1	Digital Signage - Cis			74	
SFIELD	-Digital Signage2	🖳 Digital Signage - Cis			75	Select All
SFIELD	-Door Sensor 006	Access Control - Cis			72	Desident A
SFIELD	-Fire Sensor1	💁 Fire Detector			76	Deselect A
CETEL	Eiro Concor?	Eiro Dotoctor			77 ど	
or field of v	iew: Prop	erties of the selected sensor	ri			
		Property	¥alue	•		
		Device ID				
		Location Name	[First F	=loor West]		
	1970	Position X,Y (or Longitude, L	atitude) 51,-46	3		
		Range Angle (degree)	25			
		Range Distance (ft)	30			

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.

🧕 Edit Sensor Gr	oup Pro	perties - Senso	r Group CPAM sensor									
Group Name:	Sensor G	roup CPAM sensor										
Group Type:	😪 General Group											
Description:	Access D	:ess Door and SFIELD-006 video sensor										
						$\sim$						
	ſ	Members of selected	d sensor group:									
		Name	Туре	Description		Add						
		SFIELD-Door Se	ens 💽 Access Control - Ci			Remove						
		SFIELD-006	🛄 Camera - Stationary	Back Entrance								
					ОК	Cancel						

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



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&AlertD escription=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&AlertD escription=Forced+Entry&AlertText=Forced+Entry&AlertType=Forced&AlertName=Forced+Entry y
- http://172.28.218.75:9100/motion?SensorID=Englewood%20-%204500-1&AlertSeverity=2&AlertD escription=Fire+Alert&AlertText=Fire+Detected&AlertType=Fire+Alarms&AlertName=Fire+Det ected

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

Figure 5-49 URL Event Notifica
--------------------------------

Proximex Surveillin	t™ Aler	t Manager															
<u>Alert View T</u> ools <u>H</u> el	lp 🛛																
	!   1	5 D	<i>8</i> 4	Û	<u>1</u>												
Navigation	E F	roximex Su	urveillint <sup>m</sup> /	lert	Management												
Alert View		Manage a	lerts genera	ed fr	om system												
<b>E</b> 2	Dr	ag a column	header her	e to g	proup by that colum	n											
All Alerts		Severity	Status		Туре	Description	Loc	0	Sensor	Occur Time	0wn		2	9	<b>9</b> 2 I	D	-
*-		🛕 Medium	! Open	$ \Delta $	Smoke Alarm	Smoke Alert	Ente	1	Englewood - 2500-1	3/30/2010				9	5	<u>141</u>	5
		🛕 Medium	👤 Open	$ \Delta $	Forced	Forced Entry	ISE L	1	Englewood - 4300-1	3/30/2010				9	5	<u>141</u>	4
Filter Alerts		🛕 Medium	👤 Open	$\triangle$	Fire Alarms	Fire Alert	Ente	1	Englewood - 4500-1	3/30/2010				9	9	141	3
		Critical	- Open		ForcedDoor and A	Forced door and Vi	[First	1	SFIELD-Door Sensor 006	3/29/2010 12	Admi			9	92	141	2
	•	📀 High	🖌 Acked	À	Door Forced Open	Door Forced Open	[First	1	SFIELD-Door Sensor 006	3/29/2010 12	Admi			<b>P</b>	5	141	1
A Alert View		🚺 Low	🖌 Acked	Ġ	OnBoardUniversal	Car Parked Illegally	[Park	1	SFIELD-025	3/29/2010 12	Admi			9	5	<u>141</u>	0
		🚺 Critical	👤 Open	$\triangle$	ForcedDoor and	Forced door and	[Firs	1	SFIELD-Door Sensor	3/29/2010				9	5	140	9 🗸
	<b>»</b>	🔍 🚺 Reci	ord 5 of 1415	È	<b>≫</b> ₩ <							-			-	1	
Show all alerts view											S Pow	wered	By Pro	ximex	3	۵	

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

		Event	[1414]: Forced Entry	
	Home Video	🐱 Note 🛛 📠 Report	ng	
Apply OK	Close Acknowledge	Close Alert Status	Sensor ommands Action	
View	Type: Forced	Severity:	🔥 Medium 🔳 Open	
	Occur Time: 3/30/2	2010 8:18:24 AM Location	ISE Lab (Englewood - 4300-1)	
	Forced Entry			
Description	Assigned To: Adr Assigned By: Adr	ninistrator (Escalated-Alert C ninistrator (3/30/2010 9:34:	oseable) 59 AM)	
Video	Forced Entry		Map Map	
VIGEO	Property	Value		
	Vendor Name	Proximex		
	Version	Version: Major: 1 Minor: 0		
	Vendor Event Id			
Note	Alarm Name	Forced Entry		
	SensorID	Englewood - 4300-1		
$\overline{\mathbf{A}}$	AlertSeverity	Z Envend Entry		
		Forced Entry	-	
System	AlertType	Forced		
Information	AlertName	Forced Entry		
Audit Trail				
				- 👼) 8

# **AtHoc Integration**

ſ

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.

🦉 End Users - AtHoc Ente	erprise Notification	ns Suite - Wi	indows Inter	net Explorer									_	
🕒 🗢 🖉 http://17	2.28.218.84/client/c	default.asp								• 47	X O Live Searc	1		<b>P</b> -
File Edit View Favor	rites Tools Help	,	x	🛄 Snagit 📃	<b>2</b>									
🖕 Favorites 🛛 🖕 🏉	Suggested Sites 🝷	🔊 Lab Diag	rams 🔊 Lab	Cameras 🔝 So	oftStub 🥫 W	eb Slice Gallery •								
AtHoc Enterg	orise Notifications Su	ite								17	• 🗟 - 🖬 é	• Page • Safety	🔹 Tools + 🕡	- »
		IWSAlerts	Enterprise I	Notification Sv:	tem					] -				
🥭 AtHoc IWS	Alerts™								out IWS Admini		<b>ČAtHoc</b>			
*	Users and G	roups - En	d Users					04/09/2010	18:58:07 (GMT	-05:00 Eas	stern)			-
Home	Sea	arch Users b	y Name: s	ecurity			F	ind	🗹 Enabled U	sers Only				
Publisher		Filter by Gr	oups: <u>Selec</u>	t Groups			Filter by	User Attribu	tes: <u>Select Attril</u>	outes				
Reports	1	ID	First	Last *	Displ	Creat	Campu	Curre	Phone	Cisco	Cisco			- 11
Users and Groups	New	2012190	Security	Manager	Securi	02/17/	Easter	Yes	650 29	1000	1000			- 11
	Enable	2012189 2012185	Security Security	Officer Operator	Securi Securi	02/02/ 11/04/	Easter Easter			1003	1003			
End Users	Disable													
H Import/Export Users	Export													
	expore													
Lists	Fo	ound: 4. Se	elected: 1.	Total user bas	e: 1429. <u>S</u> e	lect All 4						Custo	mize Result Vi	ew
Custom	Ju	ump to: All	<b>▼</b> (i	n "Last" coli	umn)						Page	l of 1 Go		н
							Click here t	hide list	g					
	C	H-LIFEBOOK-	LAP\apptis (	ID: 2012189)										
	Save	Basic Me	ember Of	Delivery Address	es Delive	ry Schedule Pref	erences							
	Cancel	Delivery A	ddresses											
		Davica	Daiman	Addross			,	liac	Add Nev	v Device/Dev	rice Address			
		Desktop	Fillinar	y Address				liids		an Di	A late			
		Popup	( <u>e</u> )	Desktop Po	pup					-				
		Cisco IP Phone Display	6	1003					E	<u>idit De</u>	<u>slete</u>			
		Cisco IP Phone	0	1003					E	idit De	elete			
											~			
Administration														
Help														
											🚺 j ocal in	tranet	a 🔹 🔍 100%.	
											) Jacocari	J.		- 11,

Figure 5-51 Create End Users

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

229181

1

AtHoc IWS	SAlerts" Atthoc TWSAlerts : TWSAlerts Unified Notification System (2010110) = Log out TWS Administrator
«	Users and Groups - Distribution List Manager - Create New List 04/12/2010 21:06:19 (GMT -05:00 Eastern)
Home	
Publisher	Select a list type: C Static List A Static List is composed of a predefined set of users or other lists.
Reports	Opynamic List A Dynamic List is dynamically generated based on a data query.
Studio	C IP List An IP List is composed of a set of IP Addresses and is used for IP-based targeting.
Users and Groups	
📙 End Users	Continue Cancel
Import/Export Users	
Distribution	
Custom Attributes	

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

AtHoc IWS	IWSAlerts Alerts <sup>™</sup> AtHoc IW	Enterprise Notification System SAlerts : IWSAlerts Unified	Notification System (201	D110) ::: Log out IWS Adr	ministrator	<b>At Hoc</b>
«	Users and Groups - N	ew Dynamic List		04/12/2010 21:15:15 (G	MT -05:00 Easte	m)
Home	Please enter new List in	formation				
Publisher	A Dynamic List is a list of u	sers that follow certain criteria.				
Reports	Basic Information					
Studio	Name:	Security				
Users and Groups	Type:	Dynamic				
📙 End Users	Description:	,		*		
Import/Export				<b>v</b>		
Davis	Distribution List Folder:	Distribution Lists/				
Lists	Query Information					
Custom Attributes	Please specify dynamic enter multiple values se	list criteria. Only users who mee parated by commas. Please note	ALL of the criteria will be sele that the search on the comm	ected. To use "or" filters, a itself is not supported.		
	Condition				Delete	
	Display Name	contains	security			
	Add Condition				Y	
	See a list of End User dynamic list query.	s who meet these criteria Only	users who are within an Opera	tor's Userbase will be includ	led in a	
	Advanced					
	Common Name:	SECURITY				
	Please select the method	for updating this List:				
	Opdatable by Operat	ors only (including Import)				
	C Updatable by extern	al source (changes by Operator v	vill be overridden by external a	source)		
	Source Identifier:	Active Directory (AD)	]			
			_	Save	Cancel	
Administration						
Help						

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

Γ

	Studio - New Scenar	VSAlerts : IWSAlerts l io	Inified Notification S	ystem (2010110) 04/12/2010	15:11:57 (GMT - <u>05:00 East</u>		
me	New Scenario						
	© Scenario			🗸 Ready			
ports Jdio	Name:	Forced Entry in Building	1				
Alert Channels	Description:				A		
Scenario							
Manager	Channelli				<b>*</b>		
Delivery Templates	Publishing:	Enable Scenario	Available for quick	nublish	•		
Audio Files	Copy from another s			paonon			
	Content			🗸 Ready	Settings		
	Alert Title:	Forced entry in building	1		(26 / 100)		
		Forced entry in ballang	1		(58 / 2000)		
	Alert Body:	Security officers, please	go to building 1 to che	ck it out	<u> </u>		
	Target URL:				Test URL		
	Response Options:	Response Text			Туре		
		1. On my way to building	1g 1		Normal 💌 🔀		
		2. I could not go to bui	ding 1 right now		Normal 💌 🔀		
		Add Response Option	1				
	© Targeting			🗸 Ready	Settings		
	C Group C Map	C IP Range C Query	C All				
	Group Chap	<ul> <li>Trikelige &lt; Query</li> </ul>	~ 60				
	S Targeted Slow	cked			Expand All Collapse Al		
	B ☐ TÂ Acat B ☐ TÂ Acat B ☐ Tâ Acat B ☐ Tê Stuc B ☐ Tê Emerge C Distribution S & Emerge S & Scatth S & Scathh S & Scatth S & Sc	demic Affairs [Targeted 0 han Resources Jents Affairs [Targeted 0 on Nors Response [Targeted 1 of LUSIS [Targeted 1 of Total s uncy First Responder y y Officer s [Targeted 0 of Total 4] s [Targeted 0 of Total 4]	f Total 6] f Total 2] of Total 5] 7]				
	w El ta clients	[Targeted 0 of Total 5]					
	Targeting Summa	ry					
	Targeted Groups:	Group Type	Group				
	Targeted Recipients:	Calculate	Security				
	Devices			🗸 Ready	Settings		
	Personal Devices	Select All Clear All		Contact Info	Statistics		
	Desktop	Рорир		Show C	ontact Info Statistics		
	Show Preview	w and Options					
	Phone	Delive	ry Order				
	Cisco IP	Phone	1 •				
	Show Option	-					
	Show Option						
	Show Option	At I-					
	Show Option	Work rsonal					
	Show Option Email Email - V Email - V Email Pe	Work Irsonal					
	Show Option	Work ersonal ssaging					

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.

I

							-						
	Alorto	IWSAlerts Enterprise No	otification System				AtHor						
	Aleris	AtHoc IWSAlerts : I	WSAlerts Unified Notif	ication System (2010)	110) :: Log out IV	VS Administrator	CALITOC						
	Studio - So	cenario Manager	n)										
Home		Find all Scenarios related t	o Alert Channel All Cha	nnels		*							
Publisher		Show only Enabled Scer	arios (available in Scenai	rio Publisher)									
		Show only Recurring Sc	enarios			Find							
		Scenario *		Channel	Enabled	Next Occurrence							
Studio	New	Forced Entry in Building 1		System Default	Enabled								
Changele	THE W	Hail Warning		Weather Warnings	Enabled								
Merc channels	Delete	HURCON 1		Weather Warnings	Enabled								
E Scenario		HURCON 2		Weather Warnings	Enabled								
Manager		HURCON 3		Weather Warnings	Enabled								
		HURCON 4		weather warnings	Enabled								
- Delivery		HORCON All Clear		Weather Warnings	Enabled								
Templates		Linktoine Wareige 10MM	ng	Facility Alerts	Enabled								
_		Lightning Warning 25MM		Weather Warnings	Enabled		<b>v</b>						
📙 Audio Files		Found 54 results 1 Selecte	ad	weather warnings	chabled		<u></u>						
				Click here	to hide list								
		Forced Entry in Building	a 1 (Scenario ID: 3078	Channel: System Defr									
				, endmen bystem ber	iuit)								
	Save	Scenario Details Aler											
	Cancel												
		© Scenario											
		Scenario V Ready											
		Name:	Forced Entry in Buildin	g 1									
		Description											
		Description.	-										
							Y						
		Channel:	System Default				•						
		Dublishing	Enable Scenario	Available for quick p	ublich								
		Publishing:	Ellable Scenario	<ul> <li>Available for quick p</li> </ul>	donan								
		Common Name:	FORCED_ENTRY_IN_B	JILDING_1									

#### 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"

Figure 5-56

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

Step 1 Click on Extensions > Add Extension.

Extensions

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

#### 🗿 Pro File Monit Extensions Tools Help \* 睂 Н X Ê **M** Ħ Close Alert View Details Create Alert Video Matrix Logoff Acknowledge Find Sensor Intelligent Physical Security Management Monitoring: North >> Springfield >> First Floor West (Alerts:66) **Monitoring Hierarchy** Springfield Global Zone Add Extension Туре Description 😹 🔵 Elementary Schools 📄 👩 🔵 North This extension will be added to your Extensions menu 🗇 Camera - Station... Main Door 🗟 🔵 Lakota 😅 Camera - Station... Side Entrance Door 🛛 🐻 🔘 Springfield Name: IPICS VTG Group 💭 Camera - Station... Main Building Entrance 🕞 🔘 First Flo Path: https://172.28.218.94/ipics/server/services/Northbo 📴 Camera - Station... Front Desk 🕞 🔵 First I 🗊 Camera - Station... Hallway 🗟 🔘 Parking Parameters: arney 🐻 📴 Camera - Station... Back Entrance 🗟 🔵 Central OK Cancel 🚺 Access Control - ... 🗟 🔵 South <u>i icco orgical orginago.</u> y norme 🖳 Digital Signage - ... a 🌑 Middle Schools 🔘 (0)Normal 💭 Digital Signage - ... SFIELD-Digital Signage2 🔄 🐻 🛑 High Schools (0) Normal SFIELD-Fire Sensor1 🌛 Fire Detector a 🖓 🔘 Cargo Ports (0)Normal SFIELD-Fire Sensor2 💁 Fire Detector G Sprinafield Ports (0)50-🜍 AED Normal SFIELD-AED Automated External Defibrilator

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.)

						Event [	1430]	: Force	d c	loor and	Video	o Analytic	s correla	ation					
	<b>6</b> I	Hom	e	Video	🔜 No	ote	Repo	orting	_	_	-								
Close		Ack Clos	nowledge se Alert	🏠 False . 👌 Escala	Alarm Ite To	Sensor Command	s	Investig	ate	200 Dispatch	17 18 18	Track	: Forward : Backward	Live Vide	0 0	Vide	o t		
File			Alert S	itatus			A	Action			Liv		Reco	rded Video	Action		No	. No	
View	1	Тур	e: Force	dDoor and A	Analytics	;	Severi	ty: 🚺	0	ritical		Open							
		Occ	ur Time:	4/15/2010	9:39:31	1 PM	Locati	on: [Fi	rst F	=loor West)	(SFIE	.D-Door Se	nsor 006)						
		Forced door and Video Analytics correlation																	
Description	_ /	Ass	igned T	o: Adminis	strator	(Escalate	d-View	red)				Resp	onse:			0%			
	1	Assigned By: Administrator (5/18/2010 10:45:53 AM)																	
System Information			Correlat	ted Alert					[	🔥 Snapsh	ot of c	orrelated A	lerts 💽	Мар					
			Property	Y	Value	alue				Sever.	. St.	Type	Descr	iption	Sen	Occur.	. 52	ID 🔻	
			Alarm Nan Original Al	ne Iort	Correla	ated Alert				High		Door	. Door Fo	orced Open	SFIEL	. 4/15/2		1429	
			Time Rang	je	-13 sec	conds				Low	2	OnBo	. Car Par	ked Illeg	SFIEL.	4/15/2	•	1420	
Audit Trail			SysAlertID	) Criteria	OnBoa	rdUnivers	al,Door I	For											
											Record	1 of 2 💽	<b>B M</b> <					>	
											- uuuu							-	
		[Live]: SFIELD-006								[Recorded]: SFIELD-006									
									-		-							~	
													-			<b></b>			
									1	P				1		0			
									1						4				
																		2	



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