



**Milestone
XProtect[®]**

Analytics 2.2
Agent Vi VCA
Administrator's Manual





Target Audience for this Document

This document is aimed at administrators of the Milestone XProtect Analytics – Agent Vi Video Contents Analysis solution.

This document provides detailed descriptions of how to install and configure XProtect Analytics – Agent Vi VCA. It furthermore provides a number of targeted “how-to” examples, guiding users through completing common configuration tasks.

For information about viewing video motion detection data together with video in the XProtect Smart Client, refer to the separate XProtect Analytics User's Manual, available on the software DVD as well as from www.milestonesys.com.

For information about using XProtect Analytics with other video content analysis providers than Agent Vi VCA, please refer to the relevant manuals:

- XProtect Analytics – BOSCH VMD Administrator's Manual
- XProtect Analytics – Dacolian LPR Administrator's Manual
- XProtect Analytics – Generic VA Administrator's Manual



Copyright, Trademarks and Important Information

Copyright

© 2011 Milestone Systems A/S.

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This document is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in this document's examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.



Contents

INTRODUCTION.....	6
Basic Data Flow	7
 SYSTEM REQUIREMENTS	 8
Surveillance Server Running XProtect Analytics	8
Smart Client Used for Viewing Analytics Data	8
 SERVER-SIDE INSTALLATION.....	 10
Important Prerequisites	10
Milestone Surveillance System.....	10
XProtect Transact	11
XProtect Smart Client.....	12
Agent Vi System	13
Installation Procedure	13
Installing the XProtect Analytics Software	13
Installing the XProtect Analytics Plugin for Agent Vi VCA.....	14
Installing the Alert Plugin Server-Side Installer.....	14
If You Later Change Transact Port.....	15
 AGENT VI VCA ADMINISTRATOR	 17
Agent Vi VCA Administrator Overview	17
Recommended Configuration Sequence.....	18
Specifying Agent Vi System	19
Specifying Surveillance System Servers	20
Specifying VCA Connections.....	22
Testing VCA Connections	24
Managing the Agent Vi VCA Server Service	25
Logging.....	25
Viewing the Agent Vi VCA Driver Log File	25
Viewing the Agent Vi VCA Server Log File	25



Changing Licenses (SLC/CLK).....	26
Specifying SLC and CLK to Upgrade	26
Specifying New CLK to Extend Number of Connections	27
Using the Built-in Help System	28
 EVENT MAPPING TOOL	 29
Event Mapping Tool’s Structure	29
Mapping-Compatible Surveillance System Events	30
Mapping Analytics Detections with Custom Events	30
Mapping Analytics Detections with Generic Events and/or Additional Hosts	31
Using the Event Mapping Tool’s Toolbar	32
Removing the Event Mapping Tool	32
 REMOVAL.....	 33
Removing the XProtect Analytics Software.....	33
Removing the Agent Vi VCA Plugin	33
Removing the Server-Side Alert Plugin Installer.....	33
Removing the Alert Plugin for Smart Clients.....	34
 GLOSSARY	 35



Introduction

Milestone XProtect Analytics provides an intelligent yet highly intuitive solution for video content analysis tasks such as license plate recognition (LPR), perimeter protection, left objects detection, etc.

Depending on which video content analysis plugins are used with XProtect Analytics, you can work with:

- License plate recognition (LPR)
- Perimeter protection
- Detection of persons, vehicles, etc. moving in unauthorized patterns or directions
- Unattended objects detection
- Loitering detection
- Tailgating detection
- Crowd formation detection
- People counting
- Detection of illegally parked vehicles
- Detection of removed items
- Advanced video motion detection (VMD)
- Countless other purposes (thanks to the XProtect Analytics Generic VA plugin, which allows third-party video content analysis applications to supply data for XProtect Analytics)

XProtect Analytics lets you easily combine video content analysis alerts with Milestone surveillance system features, such as recording, activation of outputs, etc.

A video content analysis alert on XProtect Analytics can thus, for example, trigger match against positive/negative lists, surveillance system recordings in a particular quality, opening of gates, switching on of lights, video of the incident popping up on the computer screens of particular members of security staff, mobile phone text messages being sent to other members of security staff, etc.—all in one go.

XProtect Analytics is therefore highly interesting in areas such as retail, transportation, education, industry, government, etc.

XProtect Analytics works in tight integration with a range of different Milestone products, notably:

XProtect Professional, **XProtect Enterprise** or **XProtect Corporate**, the surveillance systems providing your analytics solution with live video and recordings from cameras on your network.

- XProtect Professional is an advanced single-server video management system running up to 64 cameras per server including full-featured client access
- XProtect Enterprise is a comprehensive multi-server video management system running unlimited cameras and including full-featured client access



- XProtect Corporate is a premium multi-server video management system with central management of unlimited cameras, including full-fledged client access

XProtect Transact is a transaction management system normally used for integrating data streams from cash registers, ATMs, etc. with time-linked video. It is, however, extremely good at handling data streams from other sources as well, and is thus ideal for integrating analytics data into your surveillance system.

XProtect Smart Client is the client application used for viewing video combined with analytics data wherever you require.

XProtect Analytics also works in tight integration with solutions delivered by independent partners based on the Milestone Open Platform. Note that such solutions may impact the performance of your Milestone system.

Basic Data Flow

In an XProtect Analytics solution, video and analytics data basically flows between the products in the following way:

Cameras send raw video streams to the XProtect Professional, XProtect Enterprise or Corporate surveillance system server(s).



The video streams are passed on to XProtect Analytics, which processes the video streams in one or more steps: 1) Image analysis, for example for license plate recognition or left object detection, and 2) Match against associated positive and/or negative lists, if required.



Whenever a license plate, left object, etc. is detected, data is sent (as XML metadata, including exact timestamp information) to XProtect Transact.

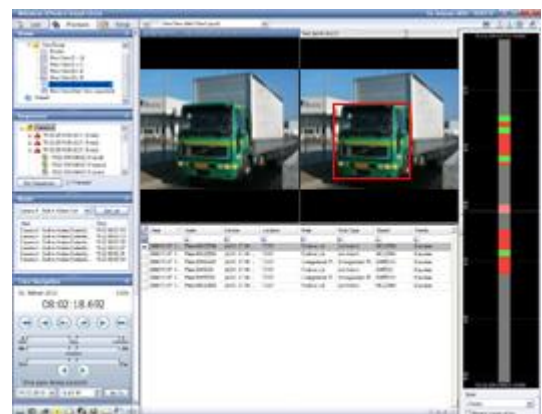


XProtect Transact stores the data together with the timestamp information, and then passes it on to the Smart Client.



In the Smart Client, users are able to view the analytics data together with video from the surveillance system.

The time-linking of the analytics data and video makes sure that Smart Client users are able to view and browse the analytics data and video simultaneously.



Example: Simultaneous viewing of analytics data and recorded video in the Smart Client



System Requirements

The following are *minimum* system requirements:

Surveillance Server Running XProtect Analytics

Operating System	Microsoft® Windows® 2008 Server R1/R2 (32 bit or 64 bit*), Windows Server 2003 (32 bit or 64 bit*), Windows 7 Professional (32 bit or 64 bit*), Windows 7 Enterprise (32 bit or 64 bit*), Windows 7 Ultimate (32 bit or 64 bit*), Windows Vista® Business (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*), Windows Vista Ultimate (32 bit or 64 bit*), Windows XP Professional** (32 bit or 64 bit*). * Running as a 32 bit application—and only on XProtect Professional and XProtect Enterprise systems ** On XProtect Corporate systems limited by Windows operating system to 10 concurrent, incomplete outbound TCP connection attempts
CPU	Intel® Pentium® 4, 2.4 GHz or higher (Core™ 2 recommended).
RAM	Minimum 1 GB (2 GB or more recommended).
Network	Ethernet (1 Gbit recommended).
Graphics Adapter	AGP or PCI-Express, minimum 1024×768, 16 bit colors.
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster).
Hard Disk Space	Minimum 80 GB free (depends on number of cameras and recording settings).
Software	Microsoft .Net 3.5 Framework with service Pack 1. DirectX 9.0 or newer.

Smart Client Used for Viewing Analytics Data

Operating System	Microsoft Windows XP Professional (32 bit or 64 bit*), Windows Server 2003 (32 bit or 64 bit*), Windows Server 2008 R1/R2 (32 bit or 64 bit*), Windows Vista Business (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*), Windows Vista Ultimate (32 bit or 64 bit*), Windows 7 Professional (32 bit or 64 bit*), Windows 7 Enterprise (32 bit or 64 bit*) or Windows 7 Ultimate (32 bit or 64 bit*). * Running as a 32 bit application
CPU	Intel Core2™ Duo, minimum 2.4 GHz or higher (more powerful CPU recommended for Smart Clients running high number of cameras and multiple views and displays).
RAM	Minimum 1 GB (higher RAM recommended for Smart Clients running high number of cameras and multiple views and displays).
Network	Ethernet (100 Mbit or higher recommended).
Graphics Adapter	AGP or PCI-Express, minimum 1024×768 (1280×1024 recommended), 16 bit colors.



Hard Disk Space 100 MB free.

Software Microsoft .Net 3.5 Framework with service Pack 1.
DirectX 9.0 or newer.
Analytics Alert Plugin, for more information about the Analytics Alert Plugin, see the document XProtect Analytics User's Manual on the surveillance system software DVDs and also available from www.milestonesys.com.

Tip: To check which DirectX version is installed on a computer, click *Start*, select *Run...*, and type `dxdiag`. When you click *OK*, the *DirectX Diagnostic Tool* window will open; version information is displayed near the bottom of its *System* tab. Should you require a DirectX update, the latest versions of DirectX are available from <http://www.microsoft.com/downloads/>.

XProtect Analytics works in tight integration with a range of different Milestone products—some of which require a particular version in order to work with XProtect Analytics—as well as video content analysis software supplying the analytics data. See *Important Prerequisites* below.



Server-Side Installation

Important Prerequisites

XProtect Analytics works in tight integration with Microsoft Windows components as well as a range of different Milestone products.

For your analytics solution to be able to work properly, you should therefore verify that the following important components are in place on your system **before** you install XProtect Analytics:

Milestone Surveillance System

XProtect Analytics works with XProtect Professional, XProtect Enterprise and XProtect Corporate surveillance systems. The surveillance systems provide your analytics solution with live video and recordings from cameras on your network.

If Using XProtect Professional or XProtect Enterprise

If using XProtect Enterprise, version 6.5c or later is required for integration with XProtect Analytics. If using XProtect Professional, version 6.5a or later is required for integration with XProtect Analytics.

If you require information about how to install XProtect Professional or XProtect Enterprise, refer to the Administrator's Manuals available on the surveillance system software DVDs as well as from www.milestonesys.com.

When XProtect Professional or XProtect Enterprise is installed, do the following:

- **Add the cameras you require for your analytics solution:** If you have not already added the cameras you are going to use with your analytics solution to your surveillance system, do so on the XProtect Enterprise or XProtect Professional system before you begin configuring XProtect Analytics.
- **User with full access:** Technically, the analytics solution will log in to your XProtect Enterprise or XProtect Professional system with a user account set up through the system's Management application (in version 7.0 or later) or Image Server Administrator (in versions earlier than 7.0). For this purpose, the user must have full access rights to all cameras used in connection with the analytics solution.

If Using XProtect Corporate

If using XProtect Corporate, version 2.0b or later is required for integration with XProtect Analytics.

If you require information about how to install XProtect Corporate, refer to the Administrator's Manual available on the XProtect Corporate software DVD as well as from www.milestonesys.com. When XProtect Corporate is installed, do the following:

- **Add the cameras you require for your analytics solution:** If you have not already added the cameras you are going to use with your analytics solution to your XProtect Corporate system, open the XProtect Corporate Management Client (in some versions called the Manager), and use the *Hardware Detection Wizard* to add the cameras you require for use with video contents analysis.
- **User with full access:** Technically, the analytics solution will log in to your XProtect Corporate system with a user account set up through the Management Client/Manager. For



this purpose, the user account in question must have a role with full access rights to all cameras used in connection with the analytics solution.

XProtect Transact

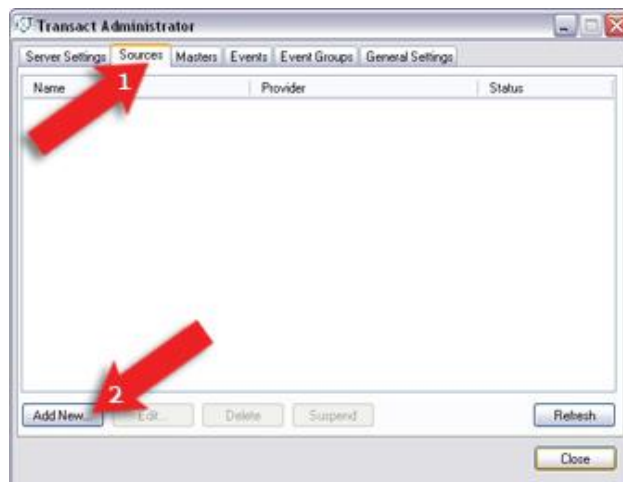
An add-on component used with the main surveillance system, XProtect Transact is normally used for integrating data streams from cash registers, ATMs, etc. with time-linked video. XProtect Transact is, however, extremely good at handling data streams from other sources as well, and is thus ideal for integrating analytics data into your surveillance system. XProtect Transact should be installed on the same computer as XProtect Enterprise or XProtect Professional Server.

XProtect Transact version 2.5c or later is required for integration with XProtect Analytics.

If you require information about how to install XProtect Transact, refer to the XProtect Transact Administrator's Manual available on the XProtect Transact software DVD as well as from www.milestonesys.com. When XProtect Transact is installed, do the following:

Configure XProtect Transact for use with your analytics solution: You basically need to make XProtect Transact aware that a new type of data—analytics data—is going to be used. You do this by adding a so-called *source*:

1. Open the *Transact Administrator* application, select the *Sources* tab, and click its *Add New...* button.



2. The *New Source* window opens.



- In the *Source name* field, type a descriptive name for your type of analytics data.
- In the *Source providers* list, select *Analytics Transact Provider*.

Then click *OK*.

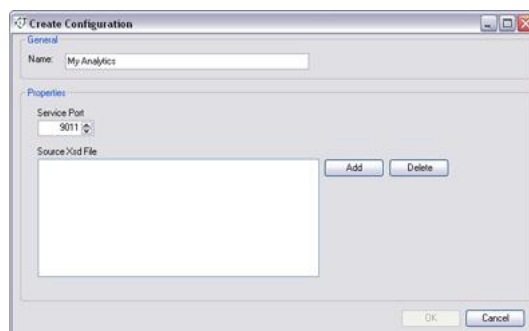


- The *Create Source* window will open. Click the *Add New...* button.



- You now get to specify a name for your source's configuration. If in doubt, give the configuration the same name as you specified for your source in step 2.

At this stage, do not change the port number or add any source XSD files.



- When ready, click *OK* twice, then the *Close* button to close the *Transact Administrator* application.

If you change the XProtect Transact Server service port number after you have installed XProtect Analytics, an XProtect Analytics configuration element must be updated manually. See *If You Later Change Transact Port* on page 15 for more information.

XProtect Smart Client

The XProtect Smart Client is the access client application used for viewing video from wherever you require. The Smart Client must be installed on every computer from which you want to be able to view video combined with analytics data.

If you require information about how to install the Smart Client, refer to the Smart Client User's Manual on the surveillance system software DVDs and also available from www.milestonesys.com.

For Smart Clients to be able to work with the analytics solution, each Smart Client must have a plugin installed:

- Alert Plugin for Smart Client:** This plugin enables the Smart Client to display analytics data received through the surveillance system's XProtect Transact add-on component.

Smart Client users download and install these plugins from the surveillance system server. The Smart Client should be installed first, then the plugin.



For more information about the Analytics Alert Plugin, see the document XProtect Analytics User's Manual on the surveillance system software DVDs and also available from www.milestonesys.com.

Agent Vi System

To run XProtect Analytics Agent Vi, a Vi-system installation configured with rules for motion detection or tripwires, etc. is required. See your Vi-system documentation for further information about how to configure the Vi-system.

Third-party video content analysis tools, such as the one mentioned above, are developed by independent partners delivering solutions based on the Milestone open platform. These solutions can impact performance on the Milestone surveillance system.

Installation Procedure

Before installing the XProtect Analytics software, make sure you understand the system requirements and prerequisites (see the previous sections).

Installing XProtect Analytics involves three tasks:

- First you install the XProtect Analytics software itself.
- Then you install the required XProtect Analytics plugin. This plugin gives your analytics solution the required functionality, in your case Agent Vi analytics for detection of persons, vehicles, etc. moving in unauthorized patterns or directions, unattended objects, loitering, tailgating, or whatever else your Agent Vi system has been set up to cover. Technically, the plugin installs as a service, but it also gives you access to the XProtect Analytics Administrator application through which you manage your analytics solution.
- Finally, you install the alert plugin server-side installer. Once installed, this will allow Smart Client users to connect to the surveillance system server and download the plugin required to view analytics data in the Smart Client.

Installing the XProtect Analytics Software

To install the Milestone XProtect Analytics Software, do the following:

1. Insert the XProtect Analytics software DVD, and click *Install XProtect Analytics Server*. Alternatively, if you downloaded XProtect Analytics from the internet, locate and double-click the file *Analytics.Installer.en-US.msi*.

After a short while the XProtect Analytics setup wizard opens. Click *Next* to begin the installation process.

2. On the wizard's second page, read and accept the license agreement. Then click *Next*.
3. On the next wizard page, select *Install licensed version* and specify your user name, organization and Software License Code (SLC). The SLC (example: AB1-2345-CD67) gives you the right to install and use a full version of the software. You will have received the SLC from your Milestone vendor, typically in an e-mail. Should you not have received the SLC, contact your Milestone vendor. If you are a Milestone vendor, and want information about how to retrieve SLCs for your customers, see the XProtect Analytics Getting Started Guide, available on the XProtect Analytics software DVD or from www.milestonesys.com.



Trial version? If installing a trial version, select *Install 30 days trial* and specify your user name and organization.

When ready, click *Next*.

4. On the next wizard page, select the folder in which you want to install XProtect Analytics. Then click *Next*.
5. Click the *Install* button to begin the actual installation.
6. When installation is complete, click the *Finish* button.

Installing the XProtect Analytics Plugin for Agent Vi VCA

1. Insert the XProtect Analytics software DVD, and click *Install AgentVi Plugin*. Alternatively, if you downloaded XProtect Analytics from the internet, locate and double-click the file *AgentVIPlugin.Installer.en-US.msi*. After a short while the XProtect Analytics Agent Vi VCA setup wizard opens. Click *Next* to begin the installation process.
2. On the wizard's second page, read and accept the license agreement. Then click *Next*.
3. On the next wizard page, select *Install licensed version* and specify your user name, organization and Software License Code (SLC). The SLC (example: AB1-2345-CD67) gives you the right to install and use a full version of the plugin. You will have received the SLC from your Milestone vendor, typically in an e-mail. Should you not have received the SLC, contact your Milestone vendor. If you are a Milestone vendor, and want information about how to retrieve SLCs for your customers, see the XProtect Analytics Getting Started Guide, available on the XProtect Analytics software DVD or from www.milestonesys.com.

Trial version? If installing a trial version, select *Install 30 days trial* and specify your user name and organization.

When ready, click *Next*.

4. Specify your Connection License Key (CLK). The CLK (example: 12abc34d56e78f90) determines how many cameras you are allowed to use with the plugin. You will have received the CLK from your Milestone vendor, typically in an e-mail. Should you not have received the CLK, contact your Milestone vendor. If you are a Milestone vendor, and want information about how to retrieve CLKs for your customers, see the XProtect Analytics Getting Started Guide, available on the XProtect Analytics software DVD or from www.milestonesys.com.

When ready, click *Next*.

Trial version? This step is not required if you install a trial version.

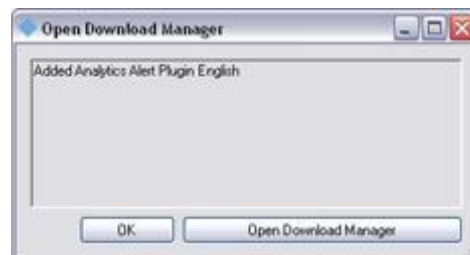
5. Click the *Install* button to begin the actual installation.
6. When installation is complete, click the *Finish* button

Installing the Alert Plugin Server-Side Installer

1. Insert the XProtect Analytics software DVD, and click *Install XProtect Analytics Alert Plugin ...* Alternatively, if you downloaded XProtect Analytics from the internet, locate and double-click the file *AlertPluginServerInstaller_en-US.exe*.



2. The compressed alert plugin server-side installer automatically extracts itself and installs. Once it is installed, your surveillance server's Download Manager will confirm the installation.
3. The Download Manager's default configuration ensures that the alert plugin immediately will be visible for download from the surveillance server's download page. In most cases you can therefore simply click *OK* to close the confirmation window. You only need to open the Download Manager if you actively want to hide the plugin from your users until a later point in time.



After installation, you can open the XProtect Analytics Administrator application—either from Windows' *Start* menu or by double-clicking the *Agent Vi VCA Administrator* desktop shortcut—and start configuring your analytics solution.

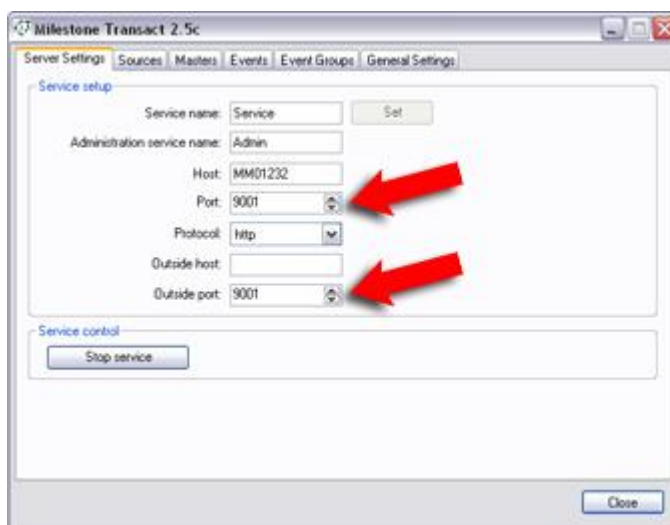
If You Later Change Transact Port

The following information is important only if you change XProtect Transact's main server settings after you have installed the XProtect Analytics software.

Background

The XProtect Transact Server service uses a specific port number for general communication with other entities. By default this port number is 9001, but it is possible to change the port number on the *Transact Administrator* application's *Server Settings* tab.

If you change the port number, information in the XML file containing the configuration of the alert plugin installer is not automatically updated. If you change the port number, the XML file must therefore be updated manually in order not to contain outdated port number information.



What to Do

To update the XML file, do the following:

1. If using XProtect Professional or XProtect Enterprise, open *C:\Program Files\Milestone\Milestone Surveillance\Plugin\Analytics\pluginconfiguration.xml* in Microsoft Notepad or another editing tool of your choice.

If using XProtect Corporate, open *C:\Program Files\Milestone\XProtect Corporate Management Server\ExternalPlugins\Analytics.xml* in Microsoft® Notepad or another editing tool of your choice.
2. In the XML file, edit the port number information so it matches the port number(s) specified on the *Transact Administrator* application's *Server Settings* tab.



```
<smartclient>
- <pluginconfigurations>
  <pluginconfiguration id="330393A5-FEF3-44da-B48D-24E9E79FF629"
    plugin="VideoOS.RemoteClient.Plugin.Alert\AlertImageContentType" />
  <pluginconfiguration id="05422533-B5FB-4f53-91BB-36B596E0BE9D"
    plugin="VideoOS.RemoteClient.Plugin.Alert\AlertContentType" />
  <pluginconfiguration id="EEC6C2B2-5C37-4ace-9136-1BBED9AEA00D"
    plugin="VideoOS.RemoteClient.Plugin.Alert\ViewLayout1x2" />
  <pluginconfiguration id="B18CDE7B-7644-765c-AAE7-BE0197EBB096"
    plugin="VideoOS.RemoteClient.Plugin.Alert\AlertPlugin">
    <transactplugin>
      <connections>
        <connection id="ab618f1f-cfc9-4228-a04d-77a44dfe5183" name="service"
          host="DKLT-RCL-01" port="9001" outsidehost="" outsideport="9001" />
      </connections>
    </transactplugin>
  </pluginconfiguration>
</pluginconfigurations>
</smartclient>
```

3. Save the changes you have made to the XML file.



Agent Vi VCA Administrator

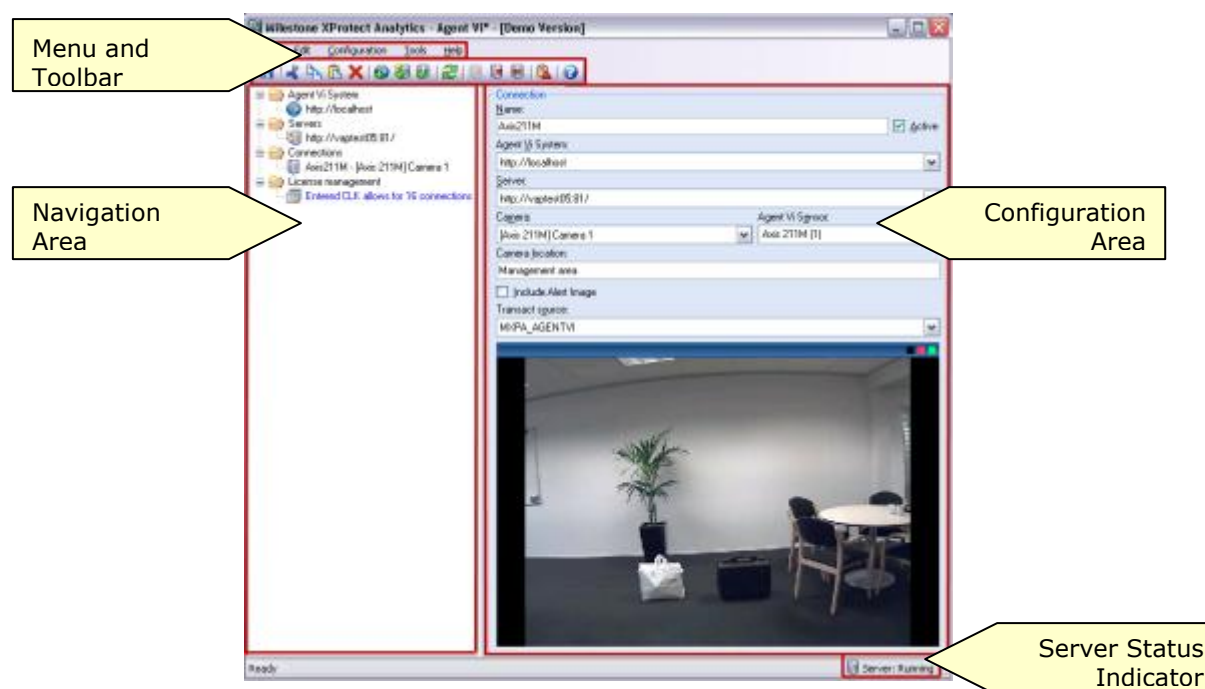
When all prerequisites (see page 10) are in place and you have installed the Milestone XProtect Analytics Agent Vi VCA service, you have access to XProtect Analytics' *Administrator* application, which lets you manage your Agent Vi video content analysis settings.

You access the Administrator application either by selecting it from Windows' *Start* menu (*Start > All programs > Milestone XProtect Analytics > Agent Vi VCA > Agent Vi VCA Administrator*), or by double-clicking the *Agent Vi VCA Administrator* desktop icon.



Agent Vi VCA Administrator Overview

The *Agent Vi VCA Administrator* consists of a number of sections:



The **menu** gives you access to commands for adding, deleting, saving, etc. of configuration details.

The **toolbar** provides you with shortcuts to often-used commands; a convenient alternative to using the menu. Read more about the toolbar in the following.

The **navigation area** lets you navigate between the *Administrator's* main areas of configuration. The navigation area has a classic expandable/collapsible tree structure.

The **configuration area** is where you specify the various elements of your configuration.

The **Server Status Indicator** provides you with at-a-glance information about the status of the Agent Vi VCA Server service (running, stopped, etc.).



Toolbar

The *Administrator's* toolbar provides you with shortcuts to often-used commands:



Save: Lets you save changes to your settings.



Cut: Lets you cut an item for pasting somewhere else.



Copy: Lets you copy an item for pasting somewhere else.



Paste: Lets you paste an item copied or cut from somewhere else.



Delete: Lets you delete an item.



Add Agent Vi System: Lets you specify an Agent Vi System (see page 19).



Add Server: Lets you specify a new surveillance system server (see page 19).



Add Connection: Lets you specify a new connection (see page 22).



Refresh: Lets you refresh the connection to the surveillance server(s).



Start Server: Lets you start the Milestone Agent Vi VCA server service.



Stop Server: Lets you stop the Milestone Agent Vi VCA server service.



Restart Server: Lets you restart the Milestone Agent Vi VCA server service.



Event Mapping Tool: Lets you access the Event Mapping Tool (see page 29).



Help: Lets you access the built-in help system (see page 28).

Recommended Configuration Sequence

If you are using the *XProtect Analytics Administrator* application for the first time, we recommend that you do things in a certain order:

You can check the list ☒ as you go along.



Open the *Administrator*, either from Windows' *Start* menu or by double-clicking the *Agent Vi VCA Administrator* desktop shortcut.



Specify Agent Vi System. By specifying which Agent Vi System XProtect Analytics should connect to, you automatically give XProtect Analytics information about the motion detection rules you are going to use for video contents analysis. See Specifying Agent Vi System on page 19 for more information.



- ☐ Specify surveillance system servers. By specifying which surveillance system server(s) XProtect Analytics should connect to, you automatically give XProtect Analytics information about the cameras connected to the surveillance system server(s). See *Specifying Surveillance System Servers* on page 19 for more information.
- ☐ Specify VCA connections. VCA (Video Content Analysis) connections define the exact analytics configuration for each camera you are going to use for video content analysis. See *Specifying Agent Vi VCA Connections* on page 22 for more information.
- ☐ Save your configuration in the *Administrator* application.
- ☐ Make sure the Milestone Agent Vi VCA Server service is running (restart it if required). See *Managing the Agent Vi VCA Server Service* on page 25 for more information.
- ☐ You can now use a Smart Client to connect to your analytics solution, and view video motion detection data combined with time-linked video. For more information, refer to the document *XProtect Analytics User's Manual* on the surveillance system software DVDs and also available from www.milestonesys.com.

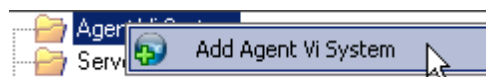
Specifying Agent Vi System

By specifying which Agent Vi System XProtect Analytics should connect to, you automatically give XProtect Analytics information about the motion detection rules you are going to use for video contents analysis.

Once XProtect Analytics has this information, you are subsequently able to specify the surveillance system server(s) to be used for your analytics solution.

To specify an Agent Vi System, do the following:

1. In the XProtect Analytics Administrator application right-click the *Agent Vi System* folder, and select *Add Agent Vi System*.



Tip: Alternatively, press ALT+F1 on your keyboard

2. Now you are able to specify information about the required Agent Vi System.

- **Host:** The *Host* field is automatically filled in with the default *http://localhost*. Specify the address of the required Agent Vi System. You can specify the address as an IP address (example: *http://123.123.123.123*) or as a host name (example: *http://ourserver*).



Tip: If XProtect Analytics is installed on the same physical computer as the required surveillance system server, you can simply type the host name <http://localhost>.

- **Port:** The *Port* field is automatically filled in with the default port number *15036*. Specify the host port number that your Agent Vi System uses.
 - **User:** XProtect Analytics automatically fills in the field *User* with the default *VISystemUser* and the field is unavailable for editing.
 - **Password:** XProtect Analytics automatically fills in the field *Password* with the default *VISystemUser* and the field is unavailable for editing.
3. Click the *Check* button in the lower right corner of the window. This way you are able to verify that you have a working connection to the Agent Vi System.

The result will appear in the *Agent Vi configuration* field. In the following example we have successfully connected to an Agent Vi System on a server called *MyAgentViServer* which in turn has a number of recording servers with a number of cameras attached:



If a camera, in the Agent Vi application also called *sensor*, appears gray it is because the association between Agent Vi and XProtect Analytics has not been made for the camera in question. Please see your Agent Vi documentation for information about how to assign the "external ID" needed for XProtect Analytics.

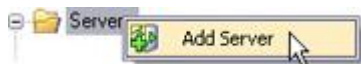
Specifying Surveillance System Servers

By specifying which surveillance system server(s) XProtect Analytics should connect to, you automatically give XProtect Analytics information about the cameras connected to the surveillance system server(s).

Once XProtect Analytics has this information, you are subsequently able to specify the VMD connections (see page 22) which define the exact analytics configuration for each camera you are going to use for video motion detection.

To specify a surveillance system server, do the following.

1. In the *Administrator* application, right-click the *Servers* folder, and select *Add Server*.



Tip: Alternatively, press ALT+F1 on your keyboard.

2. Now you are able to specify information about the required surveillance system server.
 - **Server:** Specify the address of the required surveillance system server. You can specify the address as an IP address



(example: `http://123.123.123.123`) or as a hostname (example: `http://ourserver`).

Tip: If XProtect Analytics is installed on the same physical computer as the required surveillance system server, you can simply type the hostname `http://localhost`.

If connecting to an XProtect Enterprise or XProtect Professional surveillance system server, XProtect Analytics assumes that the server should be contacted using the default port number (80) of the Image Server service (the service providing video streams to other applications). If the Image Server service does not use port 80, it is important that you specify the required port number immediately after the server address, separated by a colon. Examples (where port number 10000 is used): `http://localhost:10000`, `http://123.123.123.123:10000`.

- **Authentication:** Specify the authentication method to be used when connecting to the surveillance system server. Background:
 - *If connecting to an XProtect Enterprise or XProtect Professional server:* Technically, XProtect Analytics will log in to your surveillance system with a user account set up through XProtect Enterprise's or XProtect Professional's Management application (in version 7.0 or later) or Image Server Administrator (in versions older than 7.0). Select the authentication method specified for the required user account. Note that the user account in question must have full access rights to all cameras used in connection with the analytics solution.
 - *If connecting to an XProtect Corporate Management Server:* Technically, the analytics solution will log in to your surveillance system with a user account set up through the XProtect Corporate Management Client (in some versions called the Manager). XProtect Corporate user accounts always use either *Windows authentication* or *Windows authentication (current user)*. The user account in question must have a role with full access rights to all cameras used in connection with the analytics solution.
 - **User:** Specify the user name of the required user account on the surveillance system server.
 - **Password:** Specify the password required for the user account.
3. Click the *Check* button in the lower right part of the window. This way you are able to verify that you have a working connection to the surveillance system server. The result will appear in the *Cameras* and *Transact sources* fields. In the following example, the *Camera* field shows that we have successfully connected to a server which has a number of cameras attached:



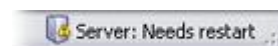
The *Transact sources* field simply lists Transact sources defined through XProtect Transact on the server in question.

4. Repeat if your analytics solution should be able to connect to other surveillance system servers.
5. Save your new settings by clicking the *Save* button in the *Administrator* application's toolbar.





Note that when certain settings have changed, the Agent Vi VCA Server service must be restarted. To verify whether this is required, look at the Agent Vi VCA Server service status indicator in the bottom right corner of the *Administrator* window.



In case restart is required, click the *Restart Server* button in the *Administrator* application's toolbar.

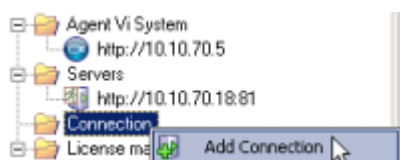


Specifying VCA Connections

Once XProtect Analytics has information about which surveillance system server(s) it should connect to, and hence which cameras are available, you can specify Agent Vi VCA connections. Agent Vi VCA connections define the exact analytics configuration for each camera you are going to use for video motion detection.

To specify a Agent Vi VCA connection, do the following:

1. In the *Agent Vi VCA Administrator*, right-click the *Connection* folder, and select *Add Connection*.



Tip: Alternatively, press ALT+F2 on your keyboard.

2. Now you are able to specify information about the required surveillance system server.

- **Name:** Type a descriptive name for the connection. If in doubt, choose a name which refers to the location of the camera you are going to use for the connection. Do not use spaces or the following special characters: ! \ ? " * : < > []
- **Active:** Lets you select whether the connection should be active or not. A connection must be active in order to be used for video motion detection.

Tip: You can only *use* as many connections as allowed by your Connection License Key (CLK; see page 26), but by making some of your connections inactive, you can *add* more connections. In cases where you do not need to use all of your connections at the same time, this can give you the freedom to switch between using different active connections.

- **Agent Vi System:** Select the required Agent Vi System from the list. The list will reflect the Agent Vi System you have previously specified (see Specifying Agent Vi System on page 19). By selecting an Agent Vi System you are subsequently able to select a server connected to the Agent Vi System.



- **Server:** Select the required surveillance system server from the list. The list will reflect the surveillance system servers you have previously specified (see Specifying Surveillance System Servers on page 19). By selecting a surveillance system server you are subsequently able to select a camera connected to the server.
- **Camera:** Select the required camera.
- **Agent Vi Sensor:** The Agent Vi sensor matching the camera defined in *Camera* is automatically selected from the list. The number in parentheses is the "sensor ID" from Agent Vi (a camera can be associated with more than one sensor).

If no Agent Vi sensor is automatically selected from the list, or if you want to use another sensor than the automatically selected, you can select a sensor manually. Click the drop-down arrow to see the Agent Vi Sensor list of available sensors. Sensors appearing in gray text are sensors not directly matching the camera selected in *Camera*. Possible reasons for sensors not directly matching selected camera:

- the sensor is not associated with any camera at all
- the sensor is running as an embedded agent (Agent Vi 3.2, please see your Agent Vi documentation for further information about embedded agents)
- the sensor is running as an embedded agent and has not been assigned an *external ID* (Agent Vi 3.3, please see your Agent Vi documentation for further information about assigning external IDs to embedded agents)

Tip: Right-click the field *Camera* and select *Copy* to use the XProtect Enterprise camera name in Agent Vi when assigning external ID to the sensor associated with the XProtect Enterprise camera.

When you select a sensor appearing in gray text, a dialog will ask you whether or not you want to keep the selected sensor that appears not to match the selected camera. Click Yes to keep the new sensor.

If you select a sensor appearing in gray text you might receive incorrect alerts in the Smart Client: because the sensor appearing in gray text might be associated with another camera than the one selected in *Camera*, alerts originating from [camera a] may be shown as occurring on [camera b].

Tip: Provided you have a working connection to the surveillance system server and the selected camera, live video from the selected camera will be displayed in the lower part of the screen.

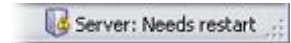
- **Camera location:** Optionally specify physical location of the selected camera. *Camera location* is displayed in the Smart Client which is helpful in large installations.
- **Include Alert Image:** Lets you select whether you want the Agent Vi VCA image to be sent to Transact or not. Selecting this option will ensure that the image, including its Agent Vi annotations, stays in the Transact database even if the surveillance system's recording database itself is deleted. However, selecting this option also means Transact will run slightly slower than usual, and that you cannot correct the Agent Vi annotations to the image. If in doubt, do not select this option.
- **Transact source:** Select required Transact source as configured in XProtect Transact's Administrator application. For more information, see Important Prerequisites on page 10.



3. Save your new settings by clicking the *Save* button in the *Administrator* application's toolbar.



Note that when certain settings have changed, the Server service must be restarted. To verify whether this is required, look at the Server service status indicator in the bottom right corner of the *Administrator* application.



In case restart is required, click the *Restart Server* button in the *Administrator* application's toolbar.



4. If you want to add further connections, repeat steps 1-3 for each new connection.

Tip: The *Administrator* application has an easy-to-use tool for testing your Agent Vi VCA connections. Read more in the following.

Testing VCA Connections

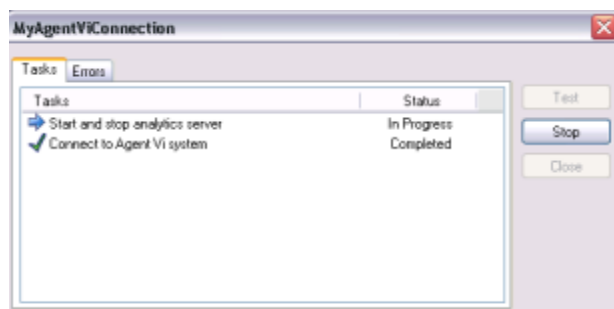
Once you have added VCA connections, you are able to quickly test each of your VCA connections in order to verify that they will work properly.

To test a VCA connection, do the following:

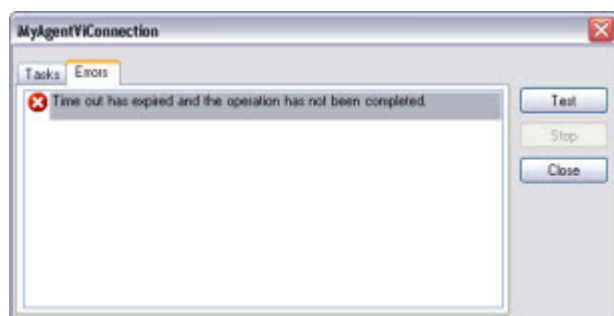
1. In the *Administrator* application, expand the *Connections* folder, right-click the required connection, and select *Test Connection Settings...*



2. The test will begin. A small window lets you monitor the progress of the test.



If any errors are detected during the test, details about the error will be displayed on the test window's *Errors* tab.



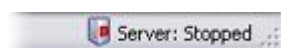


Managing the Agent Vi VCA Server Service

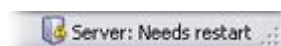
To verify the status of the Milestone Agent Vi VCA Server service, look at the Agent Vi VCA Server service status indicator in the bottom right corner of the *Administrator* application.



Service is running: To stop the service, click the toolbar's *Stop Server* button.



Service is stopped: To start the service, click the toolbar's *Start Server* button.



Service needs restart: To restart the service, click the toolbar's *Restart Server* button.



What does "restart" mean? When you have changed certain settings through the *Administrator* application, the Server service must be stopped and then started again in order for the new settings to take effect. The restart feature lets you complete the two actions in one go.

Logging

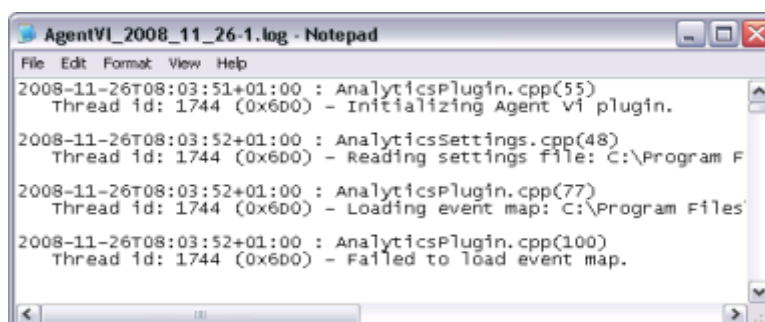
Viewing the Agent Vi VCA Driver Log File

The Milestone Agent Vi VCA Server driver logs its activity in a log file. The log file can be a very useful tool for monitoring and troubleshooting the status of the driver.

To view the Milestone Agent Vi VCA Server driver log file, select the *Agent Vi VCA Administrator's Tools* menu, then select *View Log File* and then *Driver Log*.

Tip: Alternatively, press ALT+F9 on your keyboard.

All entries in the log are time-stamped, with the most recent entries displayed at the bottom of the log file.



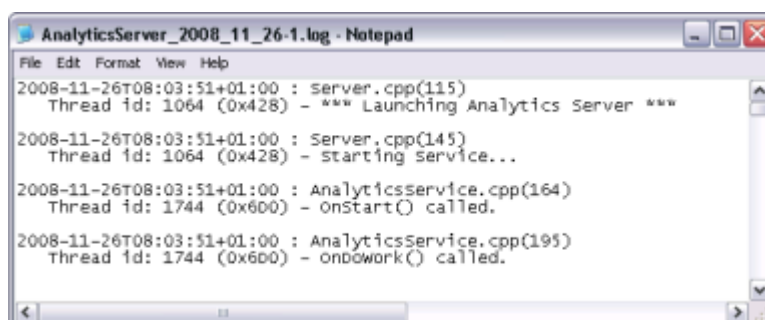
Viewing the Agent Vi VCA Server Log File

The Milestone Agent Vi VCA Server service logs its activity in a log file. The log file can be a very useful tool for monitoring and troubleshooting the status of the service.

To view the Milestone Agent Vi VCA Server service log file, select the *Agent Vi VCA Administrator's Tools* menu, then select *View Log File* and then *Server Log*.

Tip: Alternatively, press ALT+F10 on your keyboard.

All entries in the log are time-stamped, with the most recent





entries displayed at the bottom of the log file.

Changing Licenses (SLC/CLK)

Your licences determine how you are able to use XProtect Analytics:

- Your Software License Code (SLC) determines your right to use a full version of the software. The SLC is a 13-character long combination of digits, letters and dashes (example: AB1-2345-CD67).
- Your Connection License Key (CLK) determines how many cameras you are allowed to use with XProtect Analytics, and thus how many so-called connections you are able to establish. The CLK is a 16-character long combination of digits and letters (example: 12abc34d56e78f90).

You specify the SLC and CLK during installation of XProtect Analytics, unless you install a trial version (for which licenses are not required). Sometimes it is necessary to change the licenses, for example if:

- You want to **upgrade a trial version to a full version**. In that case you acquire a Software License Key (SLC) and a Connection License Key (CLK) from your Milestone vendor, and specify them in the *XProtect Analytics Administrator* application. See the following for more information.
- You want to **extend the number of cameras** you are allowed to use with XProtect Analytics. In that case you acquire a new Connection License Key (CLK) from your Milestone vendor, and overwrite the old one. See page 26 for more information.

Specifying SLC and CLK to Upgrade

1. In the *Administrator* application, expand the *License management* folder.
2. Click the blue *Trial Version - # day(s) left* text to access the *License management* features:



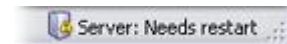
Tip: Note the *MAC address for this machine* field. The field lists the MAC (Media Access Control) address of the computer on which XProtect Analytics is installed. The MAC address uniquely identifies the computer. If you later need to get a new license—for example if you need to use more cameras than covered by your original license—your Milestone vendor is likely to ask you for the MAC address.

3. In the *Software License Code (SLC)* field, specify your SLC. Then click the *Set* button.
4. In the *Connection License Key (CLK)* field, specify your CLK. Then click the *Set* button.
5. Save your new settings by clicking the *Save* button in the *Administrator* application's toolbar.





Note that when certain settings have changed, the Server service must be restarted. To verify whether this is required, look at the server service status indicator in the bottom right corner of the *Administrator* application.



In case restart is required, click the *Restart Server* button in the *Administrator* application's toolbar.



6. You now have a fully working version with which you can use as many connections as allowed by your CLK:

Specifying New CLK to Extend Number of Connections

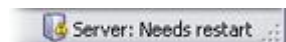
1. In the *Administrator* application, expand the *License management* folder.
2. Click the blue *Entered CLK allows for # connections* text to access the *License management* features:

Tip: Note the *MAC address for this machine* field. The field lists the MAC (Media Access Control) address of the computer on which XProtect Analytics is installed. The MAC address uniquely identifies the computer. If you later need to get a new license—for example if you need to use more cameras than covered by your original license—your Milestone vendor is likely to ask you for the MAC address.

3. In the *Connection License Key (CLK)* field, overwrite the old CLK with the new one. Then click the *Set* button.
4. Save your new settings by clicking the *Save* button in the *Administrator* application's toolbar.



Note that when certain settings have changed, the server service must be restarted. To verify whether this is required, look at the server service status indicator in the bottom right corner of the *Administrator* application. In case restart is required, click the *Restart Server* button in the *Administrator* application's toolbar.



5. You can now use as many connections as allowed by your new CLK.



Using the Built-in Help System

To use the *Administrator* application's built-in help system, simply press the F1 key on your keyboard. Alternatively, click the *Help* icon in the *Administrator* application's toolbar.



The built-in help system will open in a separate window, allowing you to easily switch between help and XProtect Analytics itself. The built-in help system is context-sensitive. This means that when you press F1 for help while working in a particular area of the *Administrator* application, the help system automatically displays a help topic relevant to that area.

Navigating the Built-in Help System

You are always able to freely navigate between the help system's contents. To do this, simply use the help window's four tabs: *Contents*, *Search*, *Favorites* and *Glossary*, or use the links inside the help topics.



- **Contents Tab:** Lets you navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer.
- **Search Tab:** Lets you search for help topics containing particular terms of interest. For example, you can search for the term *camera* and every help topic containing the term *camera* will be listed in the search results. Clicking a help topic title in the search results list will open the required topic.
- **Favorites Tab:** Lets you build a list of your favorite help topics. Whenever you find a help topic of particular interest to you, simply add the topic to your favorites list. Then you can access the topic with a single click—also if you close the help window and return to it later.
- **Glossary Tab:** What is a Connection License Key? What does VCA mean? The *Glossary* tab provides a glossary of common surveillance and network-related terms. Simply select a term to view a corresponding definition in the small window below the list of terms.

Links in Help Topics

The actual content of each help topic is displayed in the right pane of the help window. Help topic texts may contain various types of links, notably so-called expanding drop-down links. Clicking an expanding drop-down link will display detailed information. The detailed information will be displayed immediately below the link itself; the content on the page simply expands. Expanding drop-down links thus help save space.

Tip: If you wish to quickly collapse all texts from expanding drop-down links in a help topic, simply click the title of the topic in the help system's *Contents* menu.

Printing Help Topics

To print a help topic, navigate to the required topic and click the help window's *Print* button. When you click the *Print* button, a dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading. If in doubt, select *Print the selected topic* and click *OK*.




When printing a selected help topic, the topic will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links (see above), click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you require.



Event Mapping Tool

The Event Mapping Tool is used for making analytics detections trigger surveillance system events.

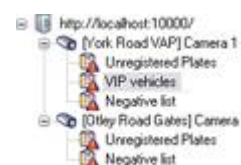
What happens when the surveillance system is triggered is highly individual as it depends entirely upon the configuration of your surveillance system. Example: In connection with license plate recognition, triggered events are often used to subsequently trigger output signals for raising of parking barriers, etc. However, triggered events can also be used for making cameras record in high quality or similar. You can even use a triggered event to subsequently trigger combinations of such actions. For more information about coupling events with actions, see the Administrator's Manual for your surveillance system.

You access the Event Mapping Tool by clicking the  icon in the Administrator application's toolbar. Alternatively, use Windows' *Start* menu, selecting *All Programs > Milestone XProtect Analytics > Agent Vi VCA > Agent Vi VCA Event Mapping Tool*.

Event Mapping Tool's Structure

The Event Mapping Tool consists of three sections:

- An expandable list of servers, connections to cameras, and analytics rules/lists. In this area you select the type of analytics detection you want to map with a surveillance system event.
- A *Custom Events* section, in which you select the surveillance system events you want to trigger based on the selected analytics detection.



- A *Generic Events* section, in which you have the option of making the selected analytics detection send data that will trigger a generic event on the surveillance system. Generic events are surveillance system events based on the analysis of received data in the TCP and/or UDP format.





Mapping-Compatible Surveillance System Events

You can only map analytics detections with certain types of surveillance system events:

- Events set up as *event buttons* on the surveillance system server
- Events set up as *generic events* on the surveillance system server

Note that these events can easily be used for subsequently triggering output, etc.—this is defined on the surveillance system server itself.

Mapping Analytics Detections with Custom Events

- Use this method to trigger *event buttons*.
 1. In the expandable list in the left side of the Event Mapping Tool, select the required analytics detection.

Depending on your type of analytics, the required analytics detection may be a rule (such as the detection of a person crossing a line, an illegally parked vehicle, a left object, etc.) or a list (used in, for example, license plate recognition where particular license plates may be on positive or negative lists).




In the example, from license plate recognition, we have selected a list of VIP vehicle license plates.

2. In the *Custom Events* section’s *Available events* list, select the surveillance system event you want the analytics detection to trigger, then click the > button to move the selected event to the *Mapped events* list.


In the following example, we have selected an event which will trigger that a barrier is raised. Thanks to output signals associated with the event (configured on the surveillance server), this will allow vehicles whose license plates are on the VIP vehicles list (which we selected in step 1) to enter a VIP parking area.



You can make an analytics detection trigger more than one event, simply use the > or >> buttons to move each required event to the *Mapped events* list.

3. Save your event mapping by clicking the  button in the Event Mapping Tool’s toolbar.

Repeat if you want other analytics detections to trigger other surveillance system events.

4. Open the XProtect Analytics Administrator application and restart the server service by clicking the *Restart Server* button in the Administrator application’s toolbar. 



Tip: If mapping events to XProtect Corporate user-defined events, metadata containing the ID of the camera behind the analytics event will be included in the mapping. This means, that it will be possible to make XProtect Corporate start recording on the camera.

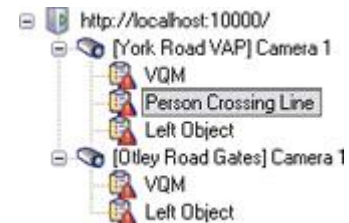
Mapping Analytics Detections with Generic Events and/or Additional Hosts

Use this method to trigger *generic events*. This method can also be used for sending data about analytics detections to additional hosts, such as the Event Proxy Tool which lets you combine analytics detections in order to present them as one combined detection to users in the Smart Client. Read more in step 5 in the following.

1. In the expandable list in the left side of the Event Mapping Tool, select the required analytics detection.

Depending on your type of analytics, the required analytics detection may be a rule (such as the detection of a person crossing a line, an illegally parked vehicle, a left object, etc.) or a list (used in, for example, license plate recognition where particular license plates may be on positive or negative lists).

In the following example, from we have selected the analytics detection rule *Person Crossing Line*:



2. In the *Generic Events* section's *Available events* list, either ...
 - Select *Send alert text as event*. This will send the entire analytics detection alert text in the data packet which the surveillance server will analyze in order to trigger the generic event. If using this option, you must be sure that the alert text contains the data matching the requirements of the generic event configuration on the surveillance server.
 - or -
 - Use the *Event text* field to type the phrases or numbers required to trigger the generic event. If more than phrase or number can be used for triggering the generic event, type them on separate lines (press your keyboard's ENTER key for a new line). Example:



3. In the *Server generic event port* field, specify the port number on which the surveillance server listens for generic event data. By default the port number is 1234. However, if the port number has been changed on the surveillance server, make sure you match the change in the Event Mapping Tool.

To verify which port is used for generic events on the surveillance server, open the surveillance server's Administrator application, click the *I/O Setup* button, then the *Advanced...* button, and look for the port number in the *Alert Port* field.


4. Select the protocol on which the surveillance server listens for generic event data, either TCP or UDP. Again, your selection must match what has been specified for the required generic event on the surveillance server.
5. Optionally, you are able to send the data defined in step 2 to an additional host.


Sending data about analytics detections to an additional host can be interesting in several scenarios, depending on your organization's needs. For example if you want to combine



two or more analytics detections in order to present them as one combined detection to users in the Smart Client. To combine analytics detections you use the Event Proxy Tool, accessed by double-clicking the file *VideoOS.EventProxy.ProxySetup.exe* in the XProtect Analytics installation folder, which also contains documentation for the Event Proxy Tool. If using the Event Proxy Tool to combine analytics detections, you would use the Event Mapping Tool’s *Additional host* fields to specify the address, port and protocol on which the Event Proxy Tool listens for input.

Specify the address of the additional host in the *Additional output host* field, the required port number in the *Additional output port* field, and the required protocol in the *Additional output event protocol* field.

6. Save your event mapping by clicking the  button in the Event Mapping Tool’s toolbar.

Repeat if you want other analytics detections to trigger other generic events or sending of data to additional hosts.
7. Open the XProtect Analytics Administrator application and restart the server service by clicking the *Restart Server* button in the Administrator application’s toolbar .

Using the Event Mapping Tool’s Toolbar



Save: Lets you save changes to your settings.



Cut: Lets you cut an item for pasting somewhere else.



Copy: Lets you copy an item for pasting somewhere else.



Paste: Lets you paste an item copied or cut from somewhere else.



Delete: Lets you delete an item.



Refresh: Lets you refresh the connection to the relevant XProtect Analytics plugin and its associated surveillance ser(s).

Use this command the first time you access the Event Mapping Tool as well as every time you have made changes to settings in the XProtect Analytics Administrator application or to the surveillance server’s event configuration.



Help: Lets you access the Event Mapping Tool’s built-in help system, which works in the same way as the Agent Vi VCA Administrator’s built-in help system. See Using the Built-in Help System on page 28 for more information.

Removing the Event Mapping Tool

The Event Mapping Tool is automatically removed when you remove the XProtect Analytics plugin with which you have used the Event Mapping Tool.



Removal

When removing XProtect Analytics, bear in mind that the analytics solution consists of several components:

On the server side, there is the XProtect Analytics software itself, a plugin for each type of video content analysis your organization uses as well as a server-side installer for the analytics alert plugin used by Smart Clients. On the client side, there is the analytics alert plugin itself.

Removing the XProtect Analytics Software

Removing the XProtect Analytics software will also remove the ability to use the Administrator application for any type of video content analysis.

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*. This will open the *Add or Remove Programs* window.
2. In the *Add or Remove Programs* window's list of currently installed programs, select the *Milestone XProtect Analytics [version #]* entry, and click the *Remove* button.
3. You will be asked to confirm that you want to remove the software. Click *Yes*, and follow the removal instructions.

Removing the Agent Vi VCA Plugin

Removing the *Agent Vi VCA* plugin will also remove the ability to use the XProtect Analytics Administrator application for setting up *Agent Vi* video content analysis.

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*. This will open the *Add or Remove Programs* window.
2. In the *Add or Remove Programs* window's list of currently installed programs, select the no longer required *Milestone XProtect Analytics [version #] Agent Vi VCA* plugin.

Then click the *Remove* button.

3. *You will be asked to confirm that you want to remove the software. Click Yes, and follow the removal instructions.*

Removing the Server-Side Alert Plugin Installer

The server-side installer for the analytics alert plugin used by Smart Clients is removed through your surveillance server's Download Manager. For more information about the Download Manager, see the documentation for your XProtect Enterprise or XProtect Professional surveillance solution.



Removing the Alert Plugin for Smart Clients

To remove the alert plugin from a computer running a Smart Client, do the following on the computer running the Smart Client

After you remove the alert plugin, it will no longer be possible to view analytics data in the Smart Client.

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*. This will open the *Add or Remove Programs* window.
2. In the *Add or Remove Programs* window's list of currently installed programs, select the *Milestone XProtect Smart Client Plug-in for Analytics [version #]* entry, and click the *Remove* button.
3. You will be asked to confirm that you want to remove the software. Click *Yes*, and follow the removal instructions.

For information about how to remove other Milestone products used in connection with your analytics solution, such as XProtect Transact, refer to the documentation for these products (available on product software DVDs or from www.milestonesys.com).



Glossary

A

Analytics: Common term for the functionality you can achieve by analyzing a video stream in order to recognize and find specific types of information. Analytics functionality can relate to license plate recognition, face recognition, object recognition, etc.

Aperture: On a camera, aperture refers to the adjustable opening (a.k.a. iris) used for controlling the amount of light coming through a lens. The aperture thus has a significant effect on the exposure of images.

ATM: Abbreviation for Automatic Teller Machine, i.e. a cash dispenser.

C

CLK: Abbreviation for Connection License Key, a key required to use your analytics solution. The key determines the number of cameras you are allowed to use with your solution, and thus how many so-called connections you are able to establish.

Codec: A technology for compressing and decompressing audio and video data, for example in an exported AVI file.

D

DirectX: A Windows extension providing advanced multimedia capabilities.

Dynamic Range: A camera's dynamic range determines, among other things, its sensitivity in low- and high-light conditions, how it reacts to changing light conditions, and how sensitive it is to infrared lighting.

E

Event: A predefined incident occurring on the surveillance system; used by the surveillance system for triggering actions. Depending on surveillance system configuration, events may be caused by input from external sensors, by detected motion, by data received from other applications, or manually through user input. The occurrence of an event could, for example, be used for making a camera record with a particular frame rate, for activating outputs, for sending e-mail alerts, or for a combination thereof.

F

FPS: Frames Per Second, a measure indicating the amount of information contained in video. Each frame represents a still image, but when frames are displayed in succession the illusion of motion is created. The higher the FPS, the smoother the motion will appear. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame Rate: A measure indicating the amount of information contained in motion video. Typically measured in FPS (Frames Per second).

G

Gain: Gain is basically the way in which a camera takes a picture of a scene and distributes light into it.



H

Host: A computer connected to a TCP/IP network. A host has its own IP address, but may - depending on network configuration - furthermore have a name (host name) in order to make it easily identifiable.

Host Name: A name by which a particular computer on a network is identified. Host names are often easier to remember than IP addresses.

HTTP: Hyper Text Transfer Protocol, a standard for exchanging files across the internet. HTTP is the standard used for formatting and transmission of data on the world wide web.

I

I-Frame: Short name for intraframe. Used in the MPEG standard for digital video compression, an I-frame is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the following frames (P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files. An I-frame is similar to a keyframe.

I/O: Short for Input/Output.

Interlacing: Interlacing is a method determining how an image is refreshed when shown on a screen. With interlacing, the image is refreshed by first scanning every other line in the image, then scanning every opposite line, and so forth. This allows for a faster refresh rate because less information must be processed during each scan. However, in some situations, interlacing may cause flickering, or the changes in only half of the image's lines for each scan may be noticeable.

IP: Internet Protocol; a protocol (i.e. standard) specifying the format and addressing scheme used for sending data packets across networks. IP is often combined with another protocol, TCP (Transmission Control Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

IP Address: Internet Protocol address; the identifier for a computer or device on a network. Used by the TCP/IP protocol for routing data traffic to the intended destination. An IP address consists of four numbers, each between 0 and 256, separated by full stops (example: 192.168.212.2).

IPIX: A technology that allows creation and viewing of 360-degree panoramic images.

Iris: On a camera, iris refers to the adjustable opening (a.k.a. aperture) used for controlling the amount of light coming through a lens. Iris thus has a significant effect on the exposure of images.

J

JPEG: An image compression method, also known as JPG or Joint Photographic Experts Group. The method is a so-called lossy compression, meaning that some image detail will be lost during compression. Images compressed this way have become generically known as JPGs or JPEGs.

JPG: An image compression method, also known as JPEG or Joint Photographic Experts Group. The method is a so-called lossy compression, meaning that some image detail will be lost during compression. Images compressed this way have become generically known as JPGs or JPEGs.

K

Keyframe: Used in the MPEG standard for digital video compression, a keyframe is a single frame stored at specified intervals. The keyframe records the entire view of the camera, whereas the following frames record only the pixels that change. This helps greatly reduce the size of MPEG files. A keyframe is similar to an I-frame.

Km/h: Kilometers per hour.



M

MAC Address: Media Access Control address, a 12-character hexadecimal number uniquely identifying each device on a network.

MPEG: A group of compression standards and file formats for digital video, developed by the Moving Pictures Experts Group (MPEG). MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information: Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reduce the size of MPEG files.

Mph: Miles per hour.

N

ND Filter: Neutral Density filter. An ND filter (a.k.a. gray filter) basically reduces the amount of light coming into a camera; effectively working as "sunglasses" for the camera. An ND filter thus affects the exposure of images.

O

Output: Data going out of a computer. On IP surveillance systems, output is frequently used for activating devices such as gates, sirens, strobe lights, etc.

Overexposure: Overexposure is when images are exposed to too much light, resulting in a burnt-out and overly white appearance.

P

P-Frame: Short name for predictive frame. The MPEG standard for digital video compression uses P-frames together with I-frames. An I-frame, also known as a keyframe, is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the following frames (the P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files

Port: A logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic which is used when viewing web pages.

PoS: Also POS. Abbreviation for Point of Sale.

PTZ: Pan/Zoom/Tilt; a highly movable and flexible type of camera.

R

Recording: In IP video surveillance systems, the term "recording" means "saving video and, if applicable, audio from a camera in a database on the surveillance system." In many IP surveillance systems, all of the video/audio received from cameras is not necessarily saved. Saving of video and audio in is in many cases started only when there is a reason to do so, for example when motion is detected, when a particular event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, when motion is no longer detected, when another event occurs or similar. The term "recording" originates from the analog world, where video/audio was not taped until the record button was pressed.



S

SLC: Abbreviation for Software License Code; a code required to use a full version of the analytics solution.

Smear: Smear is an effect leading to unwanted light vertical lines in images; it is frequently linked to slight imperfections in cameras' CCD imagers (the sensors used to digitally create the images).

SMS: Systems Management Server, a Microsoft tool which lets system administrators build up databases of hardware and software on local networks. The databases can then—among other things—be used for distributing and installing software applications over local networks.

T

TCP: Transmission Control Protocol; a protocol (i.e. standard) used for sending data packets across networks. IP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

TCP/IP: Transmission Control Protocol/Internet Protocol; a combination of protocols (i.e. standards) used when connecting computers and other devices on networks, including the internet.

Transact: Product available as an add-on to surveillance systems. With Transact, it is possible to combine video with time-linked PoS or ATM transaction data.

U

Underexposure: Underexposure is when images are exposed to too little light, resulting in a dark image with hardly any contrast.

URL: Uniform Resource Locator; an address of a resource on the world wide web. The first part of a URL specifies which protocol (i.e. data communication standard) to use when accessing the resource, whereas the second part of the URL specifies the domain or IP address at which the resource is located. Example: <http://www.myorganization.org>.

V

VMD: Video Motion Detection. In IP video surveillance systems, recording of video is often started by detected motion. This can be a great way of avoiding unnecessary recordings. Recording of video can of course also be started by other events, and/or by time schedules.

X

X-Axis: The horizontal axis in a coordinate system.

Y

Y-Axis: The vertical axis in a coordinate system.

Z

Z-Axis: The spatial axis in a coordinate system. When using joysticks, the Z-axis typically refers to the depth (zoom) level.

Milestone Systems offices are located across the world. For details about office addresses, phone and fax numbers, visit www.milestonesys.com.



The Open Platform Company