Milestone

XProtect®

Analytics 2.2
Dacolian LPR
Administrator's Manual

milestone

Target Audience for this Document

This document is aimed at administrators of the Milestone XProtect Analytics – Dacolian LPR (License Plate Recognition) solution.

This document provides detailed descriptions of how to install and configure XProtect Analytics for use with the Dacolian LPR plugin. It furthermore provides a number of targeted "how-to" examples, guiding administrators through completing common configuration tasks.

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

For information about using XProtect Analytics with other plugins (Agent Vi VCA, BOSCH VMD or Generic VA), refer to the separate XProtect Analytics Administrator's Manuals for those plugins, available on the XProtect Analytics software DVD as well as from www.milestonesys.com.

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

Product Overview

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 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

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* in the following.

Upgrading from XProtect Analytics 1.5

If you are upgrading from XProtect Analytics 1.5 – LPR to XProtect Analytics 2.2 – Dacolian LPR, see the Release Notes on the XProtect Analytics 2.2 software DVD for important information about how to perform the upgrade **before** completing the installation procedure outlined in this manual.

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.

- **Adjust camera configuration for license plate recognition:** Once the cameras are added, adjust each required camera's settings on the on the XProtect Enterprise or XProtect Professional system so the settings will match the requirements for license plate recognition: Specify a frame rate of 6 frames per second, and specify a low compression and—if possible—a low sharpness value for the cameras you want to use for license plate recognition.

- **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.

- **Adjust camera configuration for license plate recognition:** Once the cameras are added, adjust each required camera's settings so they will match the requirements for license plate recognition: Specify a frame rate of 6 frames per second, a low compression, and—if possible—a low sharpness value for the camera.

- **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 most 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, XProtect Professional or XProtect Corporate's Management 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 (**1**), and click its *Add New...* button (**2**).

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*.

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

4. 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.

5. 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 16 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 the

Alert Plugin for Smart Client installed. 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 the plugin 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.

Dacolian Intrada ALPR

To run XProtect Analytics for Dacolian license plate recognition, a Dacolian Intrada® ALPR installation is required. Dacolian Intrada ALPR is included, and automatically installed, with the XProtect Analytics plugin for Dacolian LPR.

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 license plate recognition (LPR). 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 Dacolian LPR

1. Insert the XProtect Analytics software DVD, and click *Install Dacolian LPR Plugin*. Alternatively, if you downloaded XProtect Analytics from the internet, locate and double-click the file *DacolianLPRPlugin.Installer.en-US.msi*. After a short while the XProtect Analytics Dacolian LPR 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 *Dacolian LPR 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.
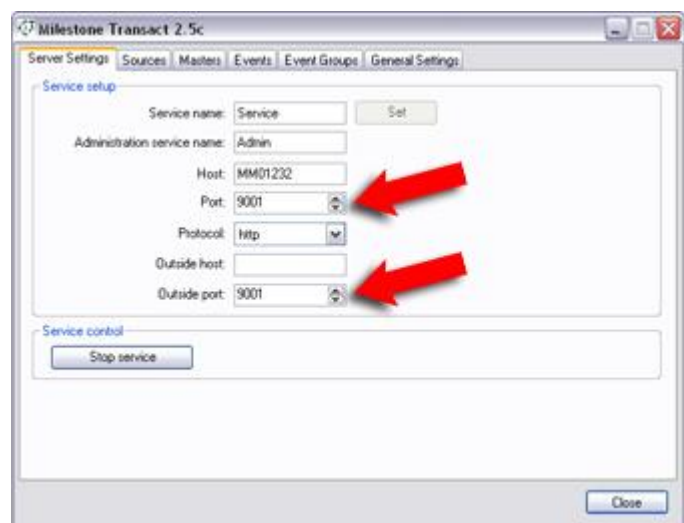
What to Do

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.

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

Dacolian LPR Administrator

When all prerequisites (see page 11) are in place and you have installed the Dacolian LPR plugin, you have access to XProtect Analytics' Administrator application, which lets you manage your license plate recognition settings.

You access the Administrator application either by selecting it from Windows' *Start* menu (*Start > All Programs > Milestone XProtect Analytics > Dacolian LPR > Dacolian LPR Administrator*), or by double-clicking the *Dacolian LPR Administrator* desktop shortcut.

Overview

The Administrator application consists of a number of sections:
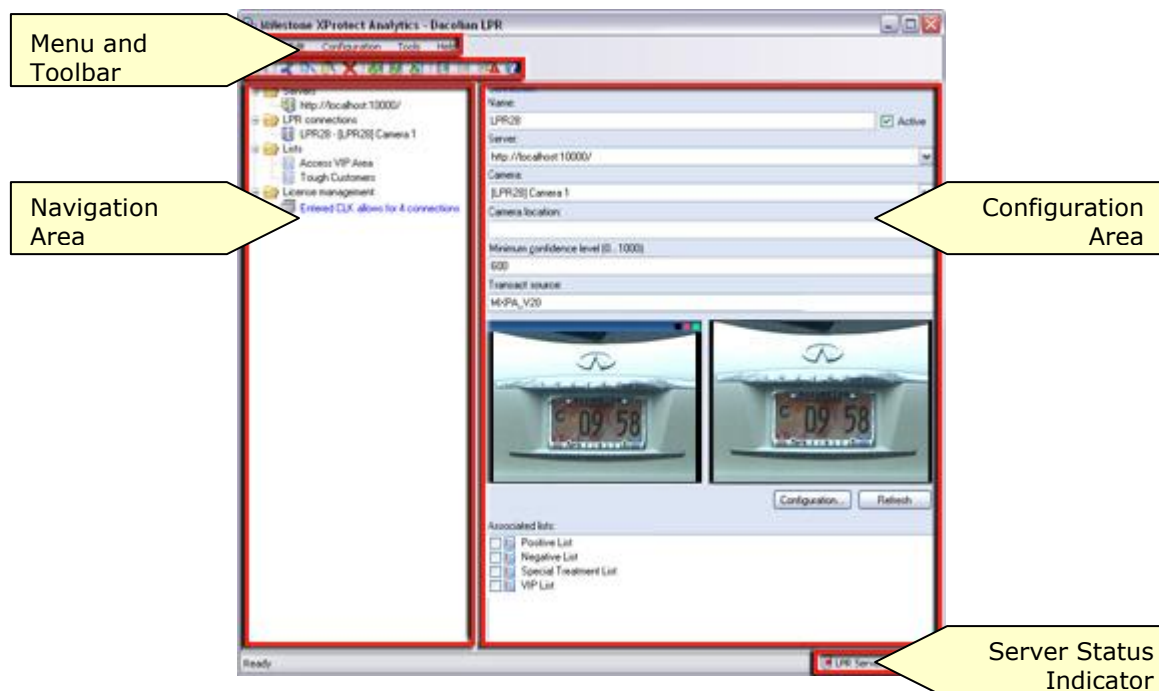
The **menu** gives you access to commands for adding, deleting, saving, etc. of configuration details.

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 Dacolian LPR 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 Server: Lets you specify a new surveillance system server (see page 20).

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

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

Start Server: Lets you start the Milestone Dacolian LPR server service.

Stop Server: Lets you stop the Milestone Dacolian LPR server service.

Restart Server: Lets you restart the Milestone Dacolian LPR server service.

Event Mapping Tool: Lets you access the Event Mapping Tool (see page 31).

Help: Lets you access the built-in help system (see page 36).

Recommended Configuration Sequence

If you are using the 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 application, either from Windows' *Start* menu or by double-clicking the *Dacolian LPR Administrator* desktop shortcut.

☐ 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 20 for more information.

☐ Specify LPR connections. LPR (License Plate Recognition) connections define the exact analytics configuration for each camera you are going to use for license plate recognition. See Specifying LPR Connections on page 22 for more information.

☐ If required, specify lists of license plates that you want your analytics solution to treat in a special way. Once you have specified lists, you can use them in combination with LPR connections to trigger surveillance system events. The surveillance system events can in turn trigger external units (for example gates, lights, etc.). See Specifying Positive/

Negative Lists on page 26 for more information.

☐ Save your configuration in the Administrator application.

☐ Make sure the Milestone Dacolian LPR Server service is running (restart it if required). See Managing the Dacolian LPR Server Service on page 28 for more information.

☐ If required, specify which surveillance system events should be triggered when license plates on—or not on—your lists are recognized. See Event Mapping Tool on page 31 for more information.

☐ You can now use a Smart Client to connect to your analytics solution, and view license plate recognition data combined with time-linked video. For more information, refer to the XProtect Analytics User's Manual, available on the XProtect Analytics software CD as well as from www.milestonesys.com.
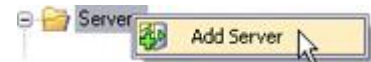
Specifying Surveillance System Servers

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 LPR connections (see page 22) which define the exact analytics configuration for each camera you are going to use for license plate recognition.

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 Professional or XProtect Enterprise 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 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 (if port 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 Professional or XProtect Enterprise server*: Technically, XProtect Analytics will log in to your surveillance system with a user account set up through XProtect Professional's or XProtect Enterprise's *Image Server Administrator*. Select the authentication method specified for the required user account in the *Image Server Administrator*. 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 XProtect Corporate 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 most 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. Depending on the selected authentication method, this information may not be required, in which case the field will appear gray.

- **Password:** Specify the password required for the user account. Depending on the selected authentication method, this information may not be required, in which case the field will appear gray.

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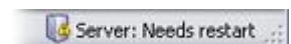
   In case restart is required, click the *Restart Server* button in the Administrator application's toolbar.

Specifying LPR 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 LPR connections. LPR connections define the exact analytics configuration for each camera you are going to use for license plate recognition.

Tip: In order to complete the following steps, the camera you are going to use for the LPR connection must be able to capture license plates. You will need this because you are going to capture a reference image, and base your further configuration on this image. If the camera is not physically positioned at a location with frequent traffic, you may consider having a colleague help you by driving a vehicle into the area covered by the camera's angle of view.

1. In the Administrator application, right-click the *LPR connections* 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 LPR 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 license plate recognition.

      Tip: You can only *use* as many LPR connections as allowed by your Connection License Key (CLK, see page 29), but by making some of your LPR connections inactive, you can *add* more LPR connections. If you do not need to use all of your LPR connections at the same time, this can give you the freedom to switch between using different active LPR connections.

    - *Server*: Select the required surveillance system server from the list. The list will reflect the surveillance system servers you have previously specified (see page 20). By selecting a surveillance system server you are subsequently able to select a camera connected to the server.

    - *Camera*: Select the required camera.

      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 left of the two reference image positions below the fields.

- **Camera location:** Optionally specify physical location of the selected camera; helpful in large installations.

- **Minimum Confidence Level:** Specify a value between 1 and 1000. The value determines the lowest acceptable confidence level for license plate recognition. If in doubt, use a value around 600. Using a minimum confidence level value of 600 will mean that XProtect Analytics should be at least 600/1000 certain that it has read a plate correctly before the data can be used for further processing; if less than 600/1000 certain about a plate, data will be discarded.

  Tip: Do not use a very high minimum confidence level (e.g. 950) to begin with, as this can lead to very little or no license plate recognition data to work with. Once you have worked with your LPR connection for a while you can adjust the minimum confidence level.

- **Transact source:** Select required Transact source. The source has been configured in XProtect Transact's Administrator application. For more information, see page 12.

- **Include alert image:** Lets you select whether you want images of detected license plates to be sent to Transact or not. Selecting this option will ensure that the image, including any 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 annotations to the image. If in doubt, do not select this option.

3. Wait until a vehicle is captured by the camera. When the vehicle is in a position allowing its license plate to be read, click the *Refresh* button below the two reference image positions. A still image from the selected camera will now appear in the right reference image position.

   You will use this still reference image for fine-tuning your analytics configuration in the following. It is therefore important that the image is realistic. If you are not happy with the image, you may have to repeat this step a number of times until you get a realistic image.

4. When ready, click the *Configuration...* button. This will open the *Intrada ALPR Settings Editor*.

5. Select the *General* tab. On the *General* tab, select the *User defined* option, click the [...] button, and select your reference image. When you captured the reference image in step 3, it was automatically saved as .jpg file which has a name matching the name of your LPR connection (you specified this name in step 2).

   Example: If the LPR connection is called *MyConnection*, select the file *C:\Program Files\Milestone\Milestone XProtect Analytics\plugin\DacolianLPR\MyConnection.jpg*.

6. Select the *Camera settings* tab. In the lower right part of the tab, select *Fixed* image size, and click the *Copy from current* button.

   Then go to the top left part of the tab, and clear any camera positions not relevant for the camera you are working with.
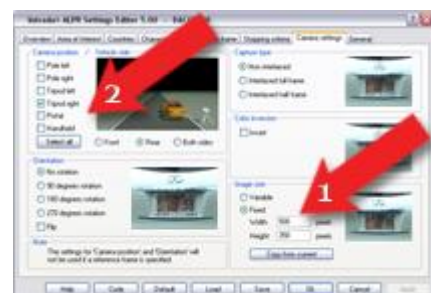
7. Select the *Stopping criteria* tab. In the tab's *Maximum complexity* section, select the *Maximum complexity level* option, and specify *10* in the accompanying field.

8. Select the *Character size* tab. The tab will display two images; each image will display the text *DACOLIAN* in a pixel size matching the pixel sizes specified below each image.

    Tip: The text *DACOLIAN* in the left image may initially be displayed in such a small pixel size that it is difficult to see. If you place your mouse pointer in the middle of the image, it will switch to a set of crosshairs, and you will be able to move the text to a part of the image in which you will be able to see it better.

    In the *Minimum character height* field below the left image, specify a pixel size so that the left image text *DACOLIAN* appears slightly smaller than the characters on the license plate in the image.

    In the *Maximum character height* field below the right image, specify a pixel size so that the right image text *DACOLIAN* appears slightly larger than the characters on the license plate in the image.

9. Select the *Countries* tab. The tab will list the countries/states for which your analytics solution is able to recognize license plates; exactly which countries/states appear on the list is determined by your software license.

    Select the countries/states required for your specific LPR connection.

10. Select the *Area of Interest* tab, and select its *Simple area of interest* option. Place your mouse pointer inside the image in the right part of the tab, and drag to select the area in which you expect license plates to appear.

    Only the selected area will be analyzed; anything in the red area will be ignored. The smaller the selected area, the quicker the license plate recognition process will be.

    Tip: If you are not happy with the selected area, simply drag and select again.
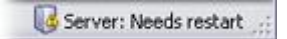
11. Save the settings by clicking the *Save* button in the settings editor's lower part. You will be asked to specify a name for the settings file. Give the file the same name as your LPR connection (you specified this name in step 2), and save the file in the folder containing your Milestone XProtect Analytics license plate recognition software.

    Example: If you specified settings for a configuration named *MyConnection*, save the file as *C:\Program Files\Milestone\Milestone XProtect Analytics\plugin\DacolianLPR\MyConnection.txt*.

12. Close the settings editor by clicking *OK* in the settings editor's lower part. You are now returned to the XProtect Analytics Administrator application.

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

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

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

If you want to add further LPR connections, repeat steps 1-13 for each new LPR connection.

Testing LPR Connections

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

1. In the Administrator application, expand the *LPR connections* folder, right-click the required LPR connection, and select *Test Connection Settings...*
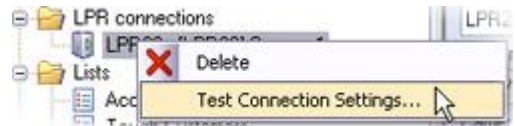
2. The test will begin. A small window lets you monitor the progress of the test.
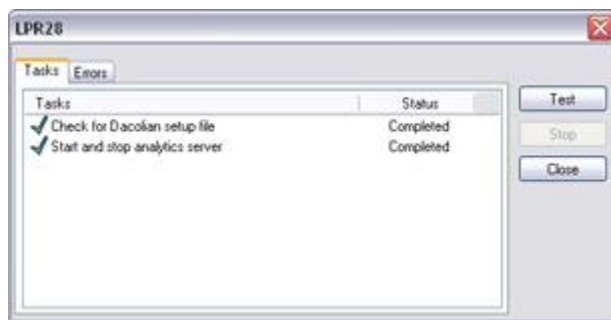
   If any errors are detected during the test, details about the error are available on the test window's *Errors* tab.
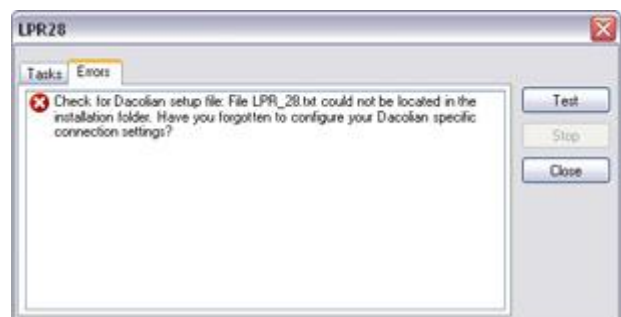
Specifying Positive/Negative Lists

Lists are lists of license plates that you want your analytics solution to treat in a special way. Once you have specified lists, you can use the Event Mapping Tool (see page 31) to make detections of license plates on lists trigger surveillance system events. Examples:

- A company HQ uses a list of executive management's company car license plates to grant executives access to a VIP parking area. When executives' license plates are recognized, the analytics solution triggers an output signal opening the gate to the VIP parking area.

- A chain of gas stations creates a list of license plates from vehicles which have previously left gas stations without paying for their gas. When such license plates are recognized, the analytics solution triggers output signals activating an alarm and temporarily blocking the gas supply to certain gas pumps.

FAQ: What happens when a surveillance system event is triggered? This is highly individual, as it depends entirely upon the configuration of your surveillance system. 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.

To specify a list, do the following:

1. In the Administrator application, right-click the *Lists* folder, and select *Add List*.
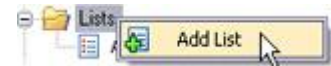
   Tip: Alternatively, press ALT+F3 on your keyboard.

2. Now you are able to specify basic information for your list.

   - **Name:** Type a descriptive name for your list. The name should be unique; do not use the same name for different lists.

   - **Priority:** Select a priority for your list. Giving your list a special priority number will not in itself mean that license plates on your list will be treated with a higher or lower priority than plates from other lists. The priority number is merely used to enable you to subsequently group or categorize your various lists.

   - **Description:** (Optional) Type a description of your list, typically information about the purpose of the list.

3. You have two ways of adding license plates to your list: Either by manually entering details of each license plate, or by importing an external list of license plates.

   - *Manual entering*: Type the required license plate registration number in the *New item* field. Do not include any spaces in the registration number, and always use capital letters. Examples: ABC123 (correct), ABC 123 (incorrect), abc123

(incorrect). Then click the *Insert* button to add the license plate to the list. Repeat for each required license plate.

- *Import*: Click the *Import...* button to browse for the required external list.

  For you to be able to import an external list, the following prerequisites must be in place:

  - The external list must have been saved in a .txt file format.

  - Each license plate must appear on a separate line in the .txt file.

  - There must not be any spaces in registration numbers. Examples: ABC123 (correct), ABC 123 (incorrect).

  - Only capital letters must be used in registration numbers. Examples: ABC123 (correct), abc123 (incorrect).

  Windows' simple text editor *Notepad* is an excellent tool for creating such .txt files. Example:
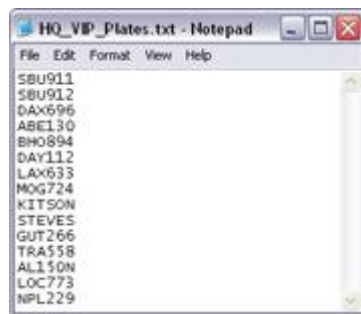
4. Save your new settings by clicking the *Save* button in the Administrator application's toolbar.

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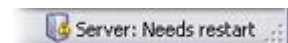
   In case restart is required, click the *Restart LPR Server* button in the Administrator application's toolbar.

If you want to add further lists, repeat steps 1-4 for each new list.

Unregistered License Plates

You would normally trigger a surveillance system event based on recognition of license plates which are included on your lists. However, you can also trigger a surveillance system event when a license plate which is *not* on a list is detected.

Example: A private car park uses a list of license plates to grant residents' vehicles access to the car park. If a vehicle with a license plate which is not on the list approaches the car park, the analytics solution triggers an output signal which lights a sign telling the driver to obtain a temporary guest pass from the Security office.

To trigger a surveillance system event if a license plate which is *not* on a list is detected, use the Unregistered Plates feature in the Event Mapping Tool (see page 31).

Managing the Dacolian LPR Server Service

To verify the status of the Milestone Dacolian LPR Server service, look at the 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.
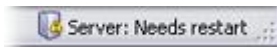
Service needs restart: To restart the service, click the toolbar's *Restart Server* button.

FAQ: 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

XProtect Analytics logs activity in log files. The log files can be a very useful tool for monitoring and troubleshooting the status of XProtect Analytics.

Viewing the Driver Log File

To view the driver log file, select the Administrator application's *Tools* menu, then select *View Log File > Driver Log*.

Tip: Alternatively, simply 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 Server Log File

To view the LPR Server service log file, select the Administrator application's *Tools* menu, then select *View Log File > Server Log*.

Tip: Alternatively, simply 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.

Licensing

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 DLK during installation of XProtect Analytics, unless you install a trial version (for which licenses are not required). Sometimes it is necessary to change the licences, 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.

- 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.

Use the following procedures:
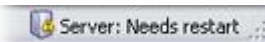
Specifying SLC and CLK to Upgrade

1. In the XProtect Analytics 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.
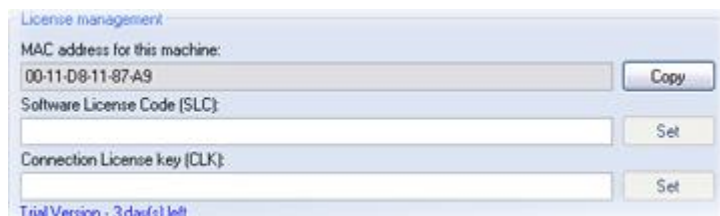
3. In the *Software License Code (SLC)* field, specify your SLC. Then click the *Set* button.

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:
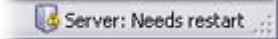
Specifying New CLK to Extend Number of LPR Connections

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.

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 *Event Mapping Tool* icon in the Administrator application's toolbar. Alternatively, use Windows' *Start* menu, selecting *All Programs > Milestone XProtect Analytics > Dacolian LPR > Dacolian LPR 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.

  When used with Dacolian LPR, you will see the positive/negative lists of license plates you have defined and selected for each connection in the XProtect Analytics Administrator application. You will also see an item called *Unregistered Plates*; use this for mapping surveillance system events which should be triggered if XProtect Analytics detects a vehicle with a license plate which is *not* on any of your positive/negative lists (see also page 32).

- 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 XProtect Professional or XProtect Enterprise surveillance systems. Generic events are surveillance system events based on the analysis of received data in the TCP and/or UDP format.
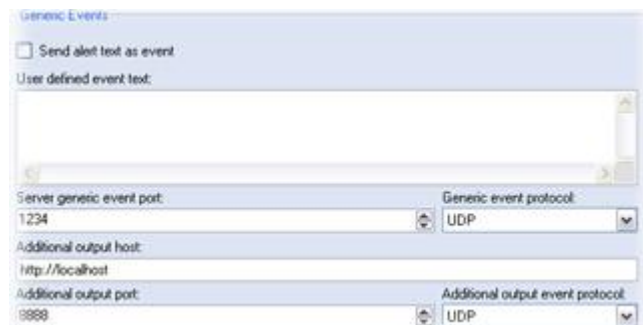
  Note that Generic events work with XProtect Enterprise and XProtect Professional surveillance systems only, not with XProtect Corporate.

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 built-in help system (see page 36).

Unregistered Plates

In the expandable list of servers, connections to cameras, and lists in the left side of the Event Mapping Tool you will see an item called *Unregistered Plates*.

Use this for mapping surveillance system events which should be triggered if XProtect Analytics detects a vehicle with a license plate which is *not* on any of your positive/negative lists.

Example: A private car park uses a positive list for granting residents' vehicles access to the car park. If a vehicle with a license plate which is not on the list approaches the car park, the analytics solution triggers an event which subsequently lights a sign telling the driver to go to the Security office.

Which Surveillance System Events Can I Use?

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

- If connected to **XProtect Professional** or **XProtect Enterprise** surveillance systems, you can map:

  o Events set up as *event buttons* on the surveillance system server

  o 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.

- If connected to **XProtect Corporate** surveillance systems you can map events set up as *user-defined events* on the surveillance system server. Note that these events can easily be used for subsequently triggering output, etc.—this is defined as part of the surveillance system's rules configuration.

Mapping Detections with Custom Events

Use this method to trigger *event buttons* if connected to XProtect Professional or XProtect Enterprise systems, or to trigger *user-defined events* if connected to XProtect Corporate systems.

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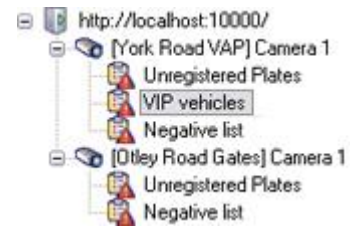
   In the example, from license plate recognition, we have selected a list of VIP vehicle license plates.

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 *Save* 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 Detections with Generic Events and/or Additional Hosts

Use this method to trigger *generic events* if connected to XProtect Professional or XProtect Enterprise systems. You cannot trigger generic events if connected to XProtect Corporate systems.

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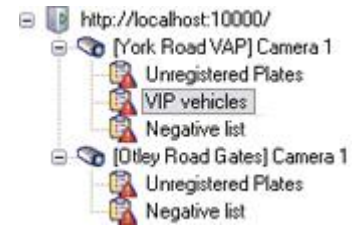
   In the example, from we have selected a list of VIP vehicle license plates.

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.

   FAQ: Why would I want to use 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 *Save* 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.

Built-in Help System

The Administrator application and the Event Mapping Tool each feature a built-in help system. To use a help system, simply press the F1 key on your keyboard. Alternatively, click the *Help* icon in the Administrator application's or Event Mapping Tool's toolbar. The help system will open in a separate window.

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 LPR 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.

Camera Tips & Tricks

Choosing the Right Cameras

License plate recognition differs from other kinds of video surveillance.

Normally, you choose cameras based on their ability to provide the best possible images for viewing by the human eye.

However, when choosing cameras for use with license plate recognition, only the small part of the images which contains the actual license plates is important.

Therefore, keep some basic features in mind when choosing cameras for use with license plate recognition:

- **Resolution:** Choose cameras which have a sufficient resolution.

- **Dynamic range:** Choose cameras which have a sufficient 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.

- **Shutter speed:** Choose cameras which give you the ability to set a shutter speed fit for your requirements. See also Lens & Shutter Speed on page 38.

- **Undesired features:** Choose cameras which give you the ability to disable image enhancement techniques, such as auto-gain and contrast/contour enhancement. For license plate recognition, you generally want your images as raw as possible. See also Undesired Camera Features on page 42.

- **Lenses:** Choose cameras which have—or lets you choose—lenses which are suitable for your required camera resolution and your external lighting conditions. For example, when infrared lighting is used it is preferable to also use a lens with an infrared pass filter or at least a lens which is compensated for infrared light. Otherwise you get a focus shift when the environment gets dark. To achieve a better dynamic range for your camera it is sometimes recommended to use a lens with auto-iris.

  - *Iris* is 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.
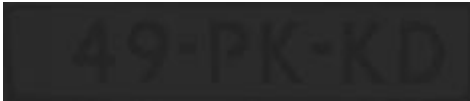
Contrast

When determining the right contrast for license plate recognition, consider the difference in gray value (when images are converted to 8-bit grayscale) between the license plate's characters and the license plate's background color:

Good contrast

Acceptable contrast; recognition is still possible

Too little contrast; recognition is not possible

Pixels in an 8-bit grayscale image can have color values ranging from 0 to 255, where grayscale value 0 is absolute black and 255 is absolute white. When you convert your input image to an 8-bit grayscale image, the minimum pixel color value difference between a pixel in the foreground and a pixel in the background should be at least 15.

Note that noise in the image, the use of compression, or similar can make it difficult to determine what the colors of a license plate's characters and background are (see also Physical Environment on page 39 and Undesired Camera Features on page 42).

Lens & Shutter Speed

When configuring cameras' lenses and shutter speeds for license plate recognition, bear in mind the following:

- **Focus:** Always make sure the license plate is in focus when images are to be used for license plate recognition.

- **Auto-iris:** If using an auto-iris lens, always set the focus with the aperture as open as possible. In order to make the aperture open, you can use ND filters or—when the camera supports manual configuration of the shutter time—the shutter time can be set to very short.

    o *ND Filters* (a.k.a. *Neutral Density filter*s or *gray filters*) basically reduce the amount of light coming into a camera; effectively working as "sunglasses" for the camera. ND filters thus affect the exposure of images (see also Physical Environment on page 39).

- **Infrared:** If using an infrared light source, note focus may change when switching between visible light and infrared light. You can avoid the change in focus by using an infrared compensated lens, or by using an infrared pass filter. Note that when using an infrared pass filter, an infrared light source is required—also during daytime.

- **Vehicle speed:** When vehicles are moving while recorded for license plate recognition, cameras' shutter time should be short enough to avoid motion blur. A rule of thumb for determining the longest suitable shutter time is:

    o **Vehicle speed in km/h:** Shutter time in seconds = 1 second / (11 × max vehicle speed in kilometers per hour)

    o **Vehicle speed in mph:** Shutter time in seconds = 1 second / (18 × max vehicle speed in miles per hour)

where / denotes "divided by" and × denotes "multiplied by."

The following table provides guidelines for recommended camera shutter speeds at different vehicle speeds:

Shutter time in seconds	Max. vehicle speed in kilometers per hour	Max. vehicle speed in miles per hour
1/50	4	2
1/100	9	5
1/200	18	11
1/250	22	13
1/500	45	27
1/750	68	41
1/1000	90	55
1/1500	136	83
1/2000	181	111
1/3000	272	166
1/4000	363	222

Physical Environment

When mounting and using cameras for license plate recognition, bear in mind the following environmental factors:

- **Much light:** Too much light in the environment can lead to overexposure or smear.

  - *Overexposure* is when images are exposed to too much light, resulting a in a burnt-out and overly white appearance. To avoid overexposure it is recommended that you use a camera with a high dynamic range and/or use an auto-iris lens. *Iris* is 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.

  - *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). In general, CCD imagers with large surfaces are less sensitive to smear than CCD imagers with small surfaces. Cameras with CMOS imagers (a different type of sensors, with a higher noise immunity) are less sensitive to smear than cameras with CCD imagers.

License plate image with smear

- **Little light:** Too little environmental or external lighting can lead to underexposure.

  - *Underexposure* is when images are exposed to too little light, resulting in a dark image with hardly any contrast. When auto-gain cannot be disabled (for more information about gain, see Undesired Camera Features on page 42) or when you are not able to configure a maximum allowed shutter time for capturing moving vehicles (see Lens & Shutter Speed on page 38), too little light will initially lead to

gain noise and motion blur in the images, and ultimately to underexposure. Underexposure can be avoided by using sufficient external lighting and/or by using a camera which has sufficient sensitivity in low-light environments without using gain. In general, cameras which have CCD imagers with large surfaces are more light-sensitive than cameras which have CCD imagers with small surfaces.

- **Infrared:** Another popular way of overcoming difficult environmental lighting conditions is to use artificial infrared lighting combined with an infrared-sensitive camera with an infrared pass filter. Retroreflective license plates are particularly suitable for use with infrared lighting.

  - o *Retroreflectivity* is achieved by covering surfaces with a special reflective material which sends a large portion of the light from a light source straight back along the path it came from. Retroreflective objects appear to shine much more brightly than other objects; at night they can thus be seen clearly from considerable distances. Retroreflectivity is frequently used for road signs, and is also used for different types of license plates.

- **Weather, etc.:** Snow, very bright sunlight, etc. may require special configuration of cameras.

- **Plate condition:** Vehicles may have damaged license plates. License plates may occasionally have been damaged deliberately in attempts to avoid detection. Vehicles may also simply have dirty license plates.

- **Camera condition:** Camera lenses may accumulate dirt over time.

Physical Positioning of Cameras

When mounting cameras for license plate recognition, bear in mind the following:

- **Single-line rule:** Mount the camera in such a way that you are able to take an image of a single line license plate recorded by the camera, and draw a horizontal line that crosses both the left and right edge of the license plate:
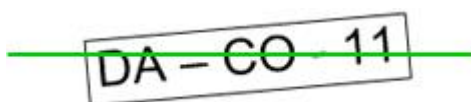
Acceptable mounting
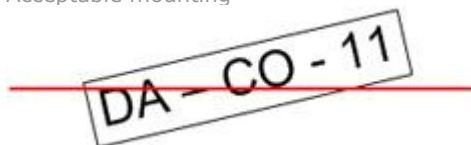
Incorrect mounting

- **Plate in image center:** Mount the camera in such way that an ideal image of the license plate is captured when the license plate is in the center of the recorded image.

- **Vertical angle:** The maximum vertical view angle of a camera used for license plate recognition is 30 degrees:

- **Horizontal angle:** The maximum horizontal view angle of a camera used for license plate recognition is 25 degrees. In most systems the horizontal angle is somewhere between 15 and 20 degrees.
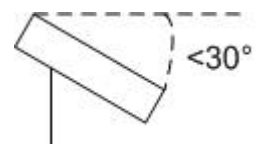
- **Blocking objects:** Avoid possible blocking objects in the view path of the camera, such as pillars, barriers, fences, gates, etc. Remember that barriers, gates, etc. are likely to be moveable between different positions.

Resolution

The term *pixels per stroke* is used to define a minimum requirement for license place recognition. The following illustration outlines what is meant by *stroke*:

Because the thickness of strokes depends on country and plate style, measurements like pixels/cm or pixels/inch are not used.

The resolution for best license plate recognition performance should be at least 2.7 pixels/stroke.

- For single line US plates (plate width 30.5 cm; stroke width around 0.7 cm) this typically means that the plate width in the image must be at least 130 pixels.

- For single line European style plates (plate width 52 cm; stroke width around 1 cm) this typically means that the plate width in the image must be at least 170 pixels.

When vehicles are moving when recorded, and an interlaced camera is used, only a half of image can be used (only the even lines). This means that the resolution requirements almost must be doubled.

- For single line US plates (plate width 30.5 cm; stroke width around 0.7 cm) this typically means that the plate width in the image must be at least 215 pixels.

- For single line European style plates (plate width 52 cm; stroke width around 1 cm) this typically means that the plate width in the image must be at least 280 pixels.

FAQ: What is 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.

Interlaced image of a moving car

Unwanted Camera Features

When configuring cameras for license plate recognition, bear in mind the following:

- **Automatic gain adjustment:** One of the most common types of image interference caused by cameras is gain noise.

  - *Gain* is basically the way in which a camera takes a picture of a scene and distributes light into it. If light is not distributed optimally in the image, the result is gain noise.

Controlling gain requires that complex algorithms are applied, and many cameras have features for automatically adjusting gain. Unfortunately, such features are not always helpful for cameras used for license plate recognition. It is therefore recommended that you configure your cameras' auto-gain functionality to be as low as possible. Alternatively, disable the cameras's auto-gain functionality altogether.

License plate image with gain noise

Tip: In dark environments, gain noise can also be avoided when your external lighting is sufficient.

- **Automatic enhancement:** Some cameras use contour, edge or contrast enhancement algorithms to make images look better to the human eye. However, such algorithms can interfere with the algorithms used in the license plate recognition process. It is therefore recommended that you disable cameras' contour, edge and contrast enhancement algorithms whenever possible.

- **Automatic compression:** High compression rates can have a negative influence on the quality of license plate images. When a high compression rate is used, more resolution (see page 41) is required in order to achieve optimal license plate recognition performance. If JPEG compression is used, it will have almost no negative influence on license plate recognition performance, as long as the images are saved with a JPEG quality level of 80% or above, and images have normal resolution, contrast and focus as well as a low noise level.

Left: License plate image saved with a JPEG quality level of 80% (i.e. low compression); acceptable
Right: License plate image saved with a JPEG quality level of 50% (i.e. high compression); unacceptable

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 Dacolian LPR Plugin

Removing the Dacolian LPR plugin will also remove the ability to use the XProtect Analytics Administrator application for Dacolian license plate recognition.

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 #] Dacolian LPR* 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 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, in this case the Dacolian LPR plugin.

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 Corporate, 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 CDs/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 a 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.

milestone

The Open Platform Company