

FSM-IP Network Video Recorder



Installation and Operation Manual



P/N: 06-521
Rev: 3, 06/19

Fike[®]
Video Analytics Corporation

DEVELOPED BY**Fike Video Analytics Corporation**704 SW 10th Street

Blue Springs, Missouri 64013-0610 U.S.A.

Phone: 844-345-3843

COPYRIGHT NOTICE

Copyright © 2014. All rights reserved.

Fike Video Analytics Corporation copyrights this manual and products it describes. You may not reproduce, transmit, transcribe, or any part of this manual without express, written permission from Fike Video Analytics Corporation.

This manual contains proprietary information intended for distribution to authorized persons or companies for the sole purpose of conducting business with Fike Video Analytics Corporation. If you distribute any information contained in this manual to unauthorized persons, you have violated all distributor agreements and we may take legal action.

TRADEMARKSFike Video Analytics Corporation® is a registered trademark of Fike Corporation.

Table of Contents

1.0 Features	2
2.0 System Architecture	3
3.0 Bandwidth and Storage Calculations	4
3.1 Number of Channels	4
3.2 Image Quality	4
3.3 Frame Rate	4
3.4 Peak Bandwidth Conditions	5
3.5 Estimating Storage Requirements	5
4.0 Getting Started.....	6
4.1 Connecting the Server.....	6
5.0 FSM-IP NVR Software	7
6.0 Configure Firewall	9
7.0 Stopping and Starting the NVR	10
8.0 How to PING	11
9.0 Configuring Server and Cameras.....	12
9.1 Server Properties	13
9.1.1 Security	13
9.1.2 Operator (Guard) Account.....	13
9.1.3 Admin Account	13
9.1.4 Server Security.....	13
9.1.5 Channel Editor	14
9.1.6 Channels Section	14
10.0 Conclusion.....	16

1.0 Features

FSM-IP is the core Network Video Recording (NVR) server designed to work primarily with the Fike Video Analytics IP video flame and smoke detection cameras and the Fike Video Analytics video management software. FSM-IP can manage up to 32 cameras and connect to an unlimited number of monitoring workstations. It provides the digital storage for constant recording of the video images and allows on-request playback of prerecorded videos at multiple workstations simultaneously. FSM-IP runs on a dedicated computer and once configured does not require any direct human interface such as keyboard, mouse, or monitor to operate. The FSM-IP NVR is a server that manages the Fike Video Analytics IP network cameras and has the following features:

- Handles up to 32 Fike Video Analytics IP network cameras
- Provides continuous video recording for each Fike Video Analytics IP camera
- Circular recording capacity of 3TB or 6TB (sized to end user request)
- Stores and marks the events (flame, smoke and motion) that are reported by each camera
- Provides access to live and recorded video for each channel over an IP connection
- Manages the camera configuration (sensitivités, zones, etc.)
- Supports multiple connections from Fike Video Analytics video management software workstations
- System can be built to Mil-spec (ruggedized)

Once configured, FSM-IP will connect to the cameras every time the NVR is turned on. These connections will be maintained until the server is shut down, or reconfigured by the user. In case of the loss of any camera connection, FSM-IP will register an alarm. The alarm conditions registered by the attached Fike Video Analytics IP cameras will be also cataloged and stored.

2.0 System Architecture

In its basic configuration the system will consist of at least one NVR, one or more Fike Video Analytics IP cameras, and a workstation running the Fike Video Analytics video management software, Figure 1. In order for the FSM-IP NVR to function properly and communicate with a video management software workstation and the Fike Video Analytics IP cameras, they should all share the same high-speed local area network (LAN). The remote workstations can be located on a different network and will communicate normally as long as the NVR is accessible over a TCP connection. The majority of network traffic will occur at the path from the Fike Video Analytics IP cameras to the FSM-IP NVR.

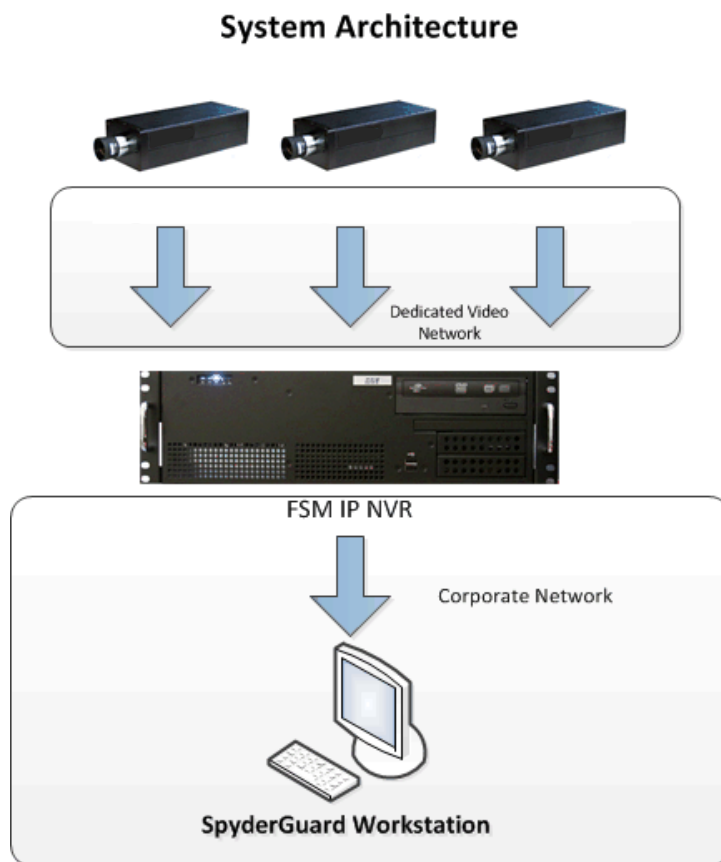


Figure 1: Diagram of System Architecture.

The NVR will manage multiple network cameras constantly storing acquired video. The guard(s) can remotely access these videos as well as live pictures via the video management software workstation. The built in algorithms along with the video management software highlight single cameras of interest and create a visual and audible alarm.

3.0 Bandwidth and Storage Calculations

For optimal allocation of bandwidth, FSM IP supports separate networks for video traffic in the form of 2 Network Interface Cards (NICs). Bandwidth of a particular network is a limited resource and overloading the network may result in dramatic decrease of data throughput and overall performance. This overload would result in dropped video frames and a sluggish response from the video management software. Bandwidth planning is extremely important so that you do not overload your network with video data traffic. Before getting to actual calculations for peak bandwidth usage, we need to discuss the tools available to help control how much bandwidth each camera will be using. Several factors can affect the bandwidth needed to transport the video.

Among those are:

1. Number of channels
2. Image quality
3. Frame rate

3.1 Number of Channels

Although the total number of channels in the system is the result of the installation requirements, correct allocation of the resources will be necessary for larger channel counts. Concentrating all the traffic of a multi server job over one network may result in severe performance deterioration. Therefore, care should be taken when multi NVR installations are considered with total channel counts exceeding 32. In such cases, each NVR should be configured to support independent subnets that handle its respective cameras.

3.2 Image Quality

The higher the image quality, the larger the frame size. Each Fike Video Analytics IP camera provides adjustable image quality. The image quality will have a large impact on the average camera frame's size. This setting is accessible through the web manager on each camera under the operator context (see IP Camera Operations Manual). Valid image quality values are 25% to 100%, where 100% will produce the largest and highest quality images. Due to the nature of MJPEG compression, the gains from increasing compression will be dependent upon image content. The more detailed the image content, the less compressible the image becomes. An example frame at an image quality of 100% compresses to 110KB, at 80% it can be compressed to 40K, and at 25% the same image was compressed to 12K. The cameras default image quality is 80%. On average a single frame at 80% quality will be around 60K. To change the image quality, see the Fike Video Analytics IP Camera Operations Manual.

3.3 Frame Rate

As more frames are transmitted, more bandwidth will be required. The FSM-IP NVR will open and maintain a connection to each camera so it can receive frames and status information. The rate at which a Fike Video Analytics IP camera is feeding frames is configurable and varies based on activity in the view of the camera. The server configuration provides two rates: for active and inactive state. The inactive state is when no motion is present within the cameras field of view. The active state is when motion is visible in the field of view or the camera is in an alarm state. The default state is 5 Frames Per Second (fps) for active and 0.5 fps for inactive states. This design conserves bandwidth by only streaming frames to the server when there has been a significant change to the image.

3.4 Peak Bandwidth Conditions

The peak condition is a worst case scenario when each camera transmits at the maximum frame rate. Although hypothetical, such condition should be taken into account when designing the network. Particularly important is the network path between the Fike Video Analytics IP cameras and the FSM-IP server. Exceeding capacity of this network will result in reduced frame rate and sluggish response at the video management software workstations. It is highly recommended that this network be dedicated for the camera-server connection since running it close to capacity can compromise other connections that share the same network.

To calculate peek bandwidth:

Peek Bandwidth = <total cameras> x <active FPS> x <average frame size>

Assuming that each camera has the same frame rate and average frame size and considering default values, each camera will require:

1 x 5fps x 60KB = 300KBps or approximately 3 Mbps (Megabit per second)

Assuming you have an isolated network just for cameras we can make some assumptions about the number of cameras you can support at peek bandwidth usage on your network.

10Meg Network

3 cameras (default settings)

100Meg Network

33 cameras (default settings)

1000Meg Network

333 Cameras (default settings)

*Note that any single FSM-IP NVR doesn't support more than 32 cameras.

If your network is not exclusively for the Fike Video Analytics IP cameras then you will need to factor in the additional usage consumption into your calculations.

3.5 Estimating Storage Requirements

Unlike estimates for the bandwidth where we were assuming worst case (maximum frame rate), for storage estimations such extremes are not necessary. The average frame rate provided by the camera will depend on physical activity at the location but generally unless some constantly moving machinery is involved, the conservative frame rate could be assumed as an average of active and inactive frame rates. Assuming default frame rates: 5/0.5 fps, the average frame rate is 2.75 and with an average frame size of 60KB will require 600 Mb per channel per hour. For a 16 camera system the storage requirement will be 230 GB per day (24 hour). On a 3TB server (2,100 (1) GB banks) the 16 cameras would be recorded continuously for 9 days. The larger 6TB server (4,200 (1) GB banks) would record the 16 cameras continuously for 18 days

4.0 Getting Started

This section will guide you through unpacking, installation and configuration of the FSM-IP NVR. Then it will explain how to establish the connection to the Fike Video Analytics IP cameras and the video management software workstation.

The following equipment is necessary to set up the system

1. FSM-IP NVR
2. One or more Fike Video Analytics IP camera
3. Dedicated monitoring workstation
4. Network infrastructure equipment

At this point we assume that the Fike Video Analytics IP cameras are installed in place and connected to an Ethernet network. We also assume that the Fike Video Analytics IP camera static IP addresses are set up without conflict¹. For proper camera configuration refer to the Fike Video Analytics IP Camera Operations Manual.

4.1 Connecting the Server

FSM-IP is equipped with two CAT-5 NIC ports [Figure 2] just for purpose of separating the IP camera network (usually an isolated subnet) from the user interface network (usually the end users corporate network) [Figure 1].

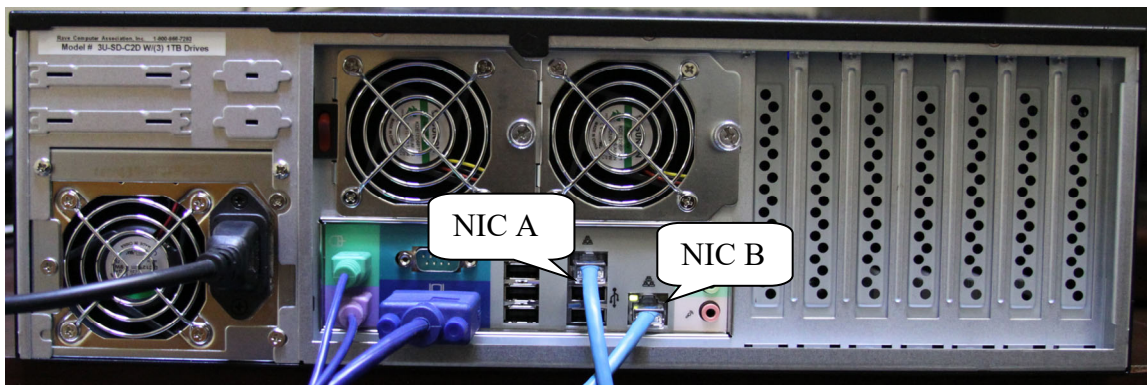


Figure 2: Network Interface Card CAT5 connectors on the back plane of the server

¹ Address assignment may be managed by network administrator

5.0 FSM-IP NVR software

Your FSM-IP NVR comes loaded with the NVR software and preconfigured with the appropriate amount of video storage banks. The software is designed to automatically start when the server is turned on. If power is lost to the server, the server is configured to start up and the server software will automatically run when power is returned. The default IP address of the server is 192.168.0.1 with a sub mask of 255.255.255.0. Depending on the desired IP address scheme, the camera(s) and NVR IP addresses may need to be changed to communicate. Once the Fike Video Analytics IP cameras have been configured with their unique IP addresses and installed to cover the hazard area you can install and configure the NVR server.

The FSM-IP NVR server should be installed in a secure and suitable environment. A suitable environment would be an environment free of excessive dust, moisture, vibration and the extremes of heat and/or cold. Slide Rails are provided to rack mount the NVR in a server cabinet. The cameras are then attached to the server through a CAT 5 or greater cable through the Local Area Network (LAN).

To configure your FSM-IP server you will need to set an appropriate IP address so you can communicate with the Fike Video Analytics IP cameras and add the camera channels to the servers devices file. The devices configuration file identifies what camera(s) the NVR should be looking for and then records the video feed and alarm information from the specified cameras. To change the servers IP address, select the *Control Panel* from the *Start* menu. In the *Control Panel* select *Network Connections*, Figure 3, and right click on *Local Area Connections* and select *Properties*, Figure 4.

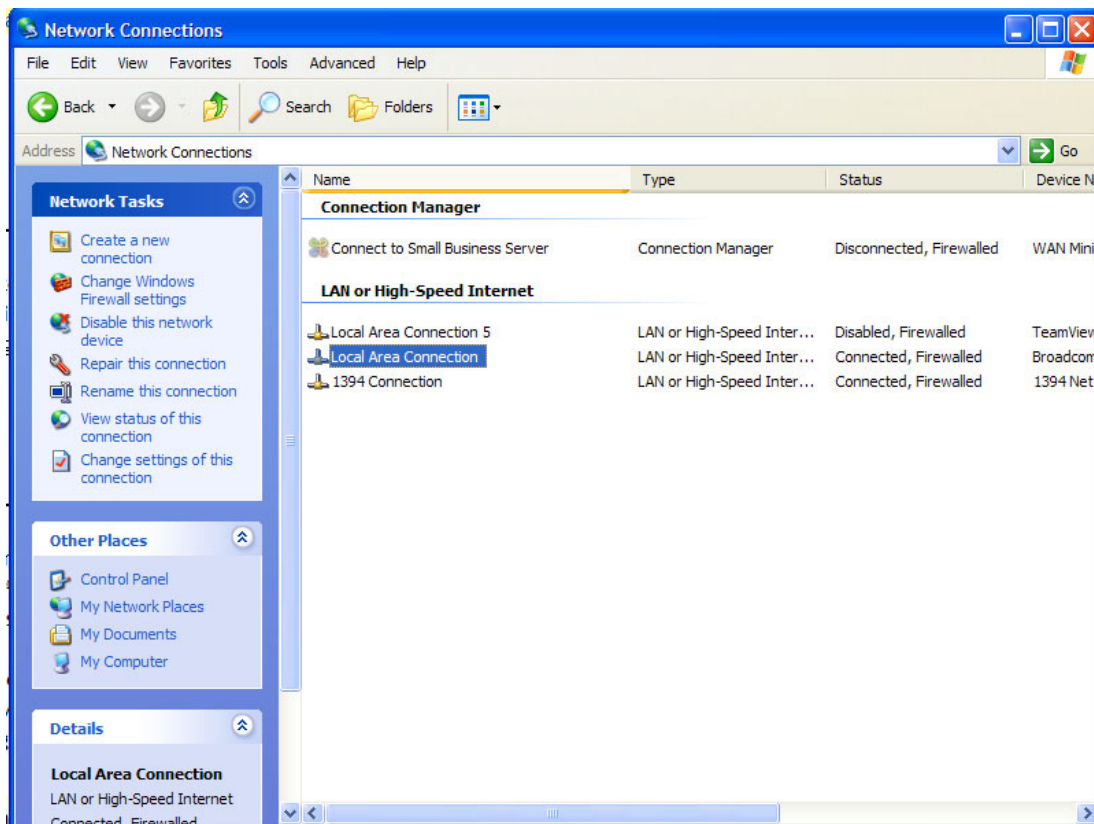


Figure 3: Network Connections Window

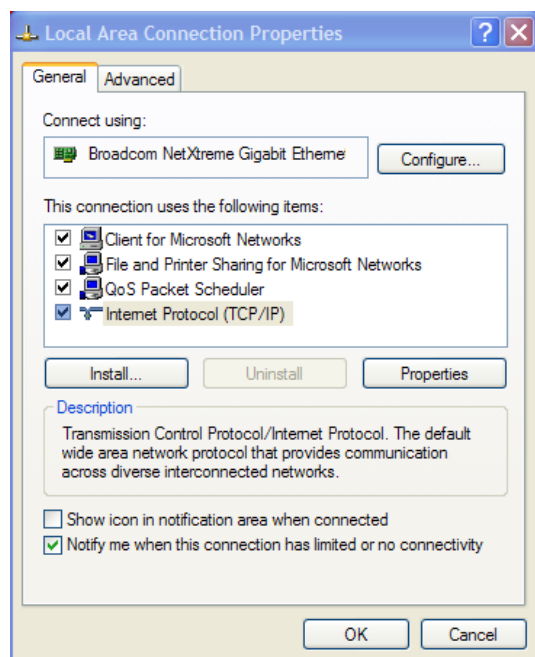


Figure 4: Local Area Connections Properties Window

Select *Internet Protocol (TCP/IP)* and click *Properties*, you can now set a new FSM-IP NVR server IP address, Figure 5.

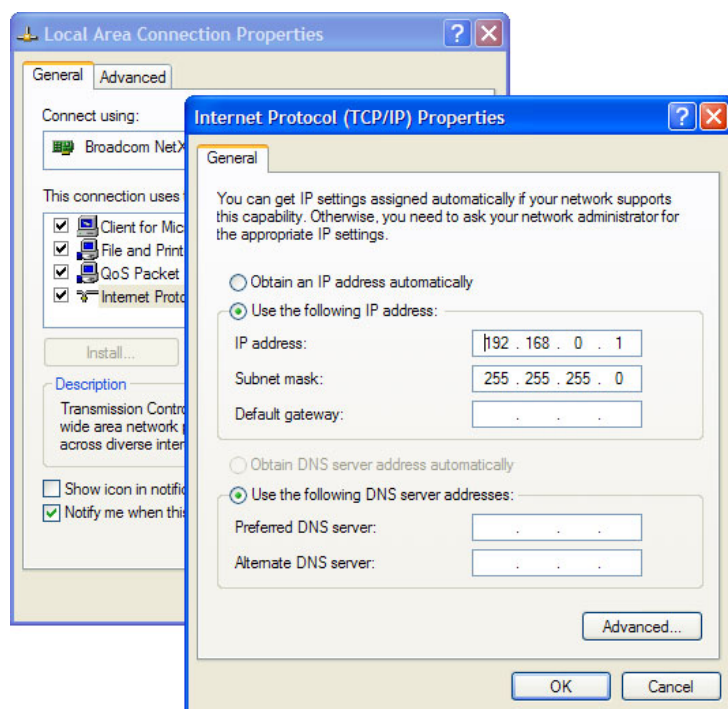


Figure 5: Internet Protocol (TCP/IP) Properties.

6.0 Configuring Firewall

In Windows XP, Vista, and Windows 7 operating systems the default settings of the firewall may prevent connection of the video management software workstation to the NVR. To ensure connectivity, changes to the Firewall configuration may be required. To do so open *Control Panel/Windows Firewall* and select the *Exceptions* tab. Click *Add Program* and select *Browse*, Figure 6.

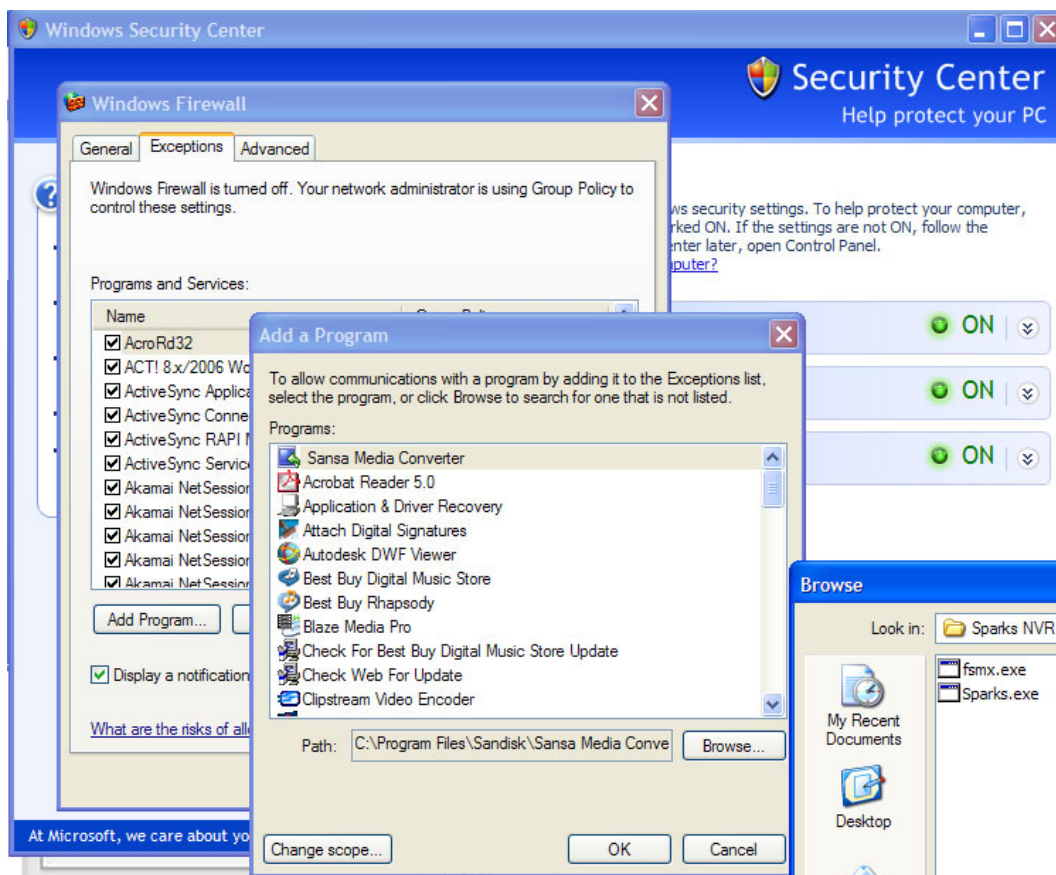


Figure 6: Use the browse feature in the *Add a Program* window when adding a firewall exception.

Select the following file: **C:\Program Files\axonX Fike\Sparks NVR\fsmx.exe** and click *Open*, Figure 7. You may also want to select the following file: **C:\Program Files\Fike Video Analytics\SpyderGuard-IP\SpyderGuardIP.exe** and click *Open*. You may also have to open the default communication port 5010. To add the port select, *Add Port* and provide a name (ie. SigniTalk) and the port (5010), select TCP and OK.

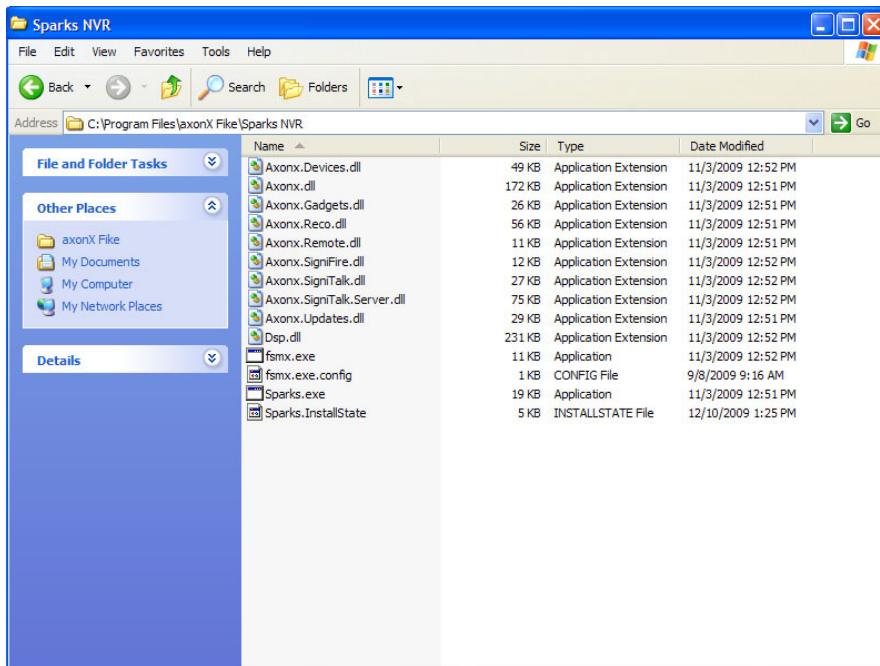


Figure 7: Location of the Sparks NVR and fsmx executable files.

7.0 Stopping and Starting the NVR

By default the installer configures the NVR to start automatically when the FSM-IP NVR boots. You can also manually stop and start the NVR service by choosing *Control Panel/Administrative Tools/Services*, right-clicking on *Sparks NVR Runtime* in the list of all available services and choose *Start* or *Stop* in the context menu, Figure 8.

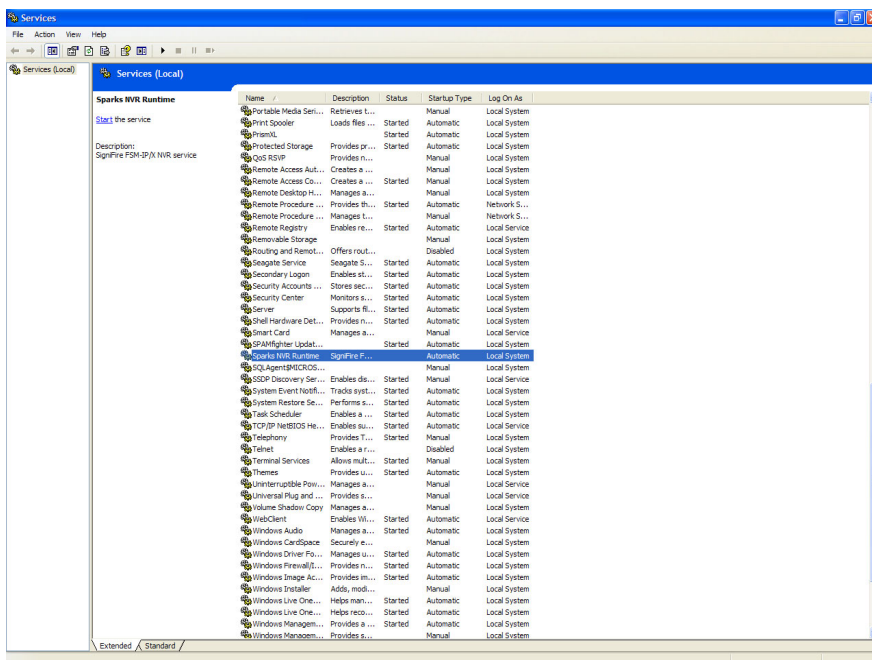
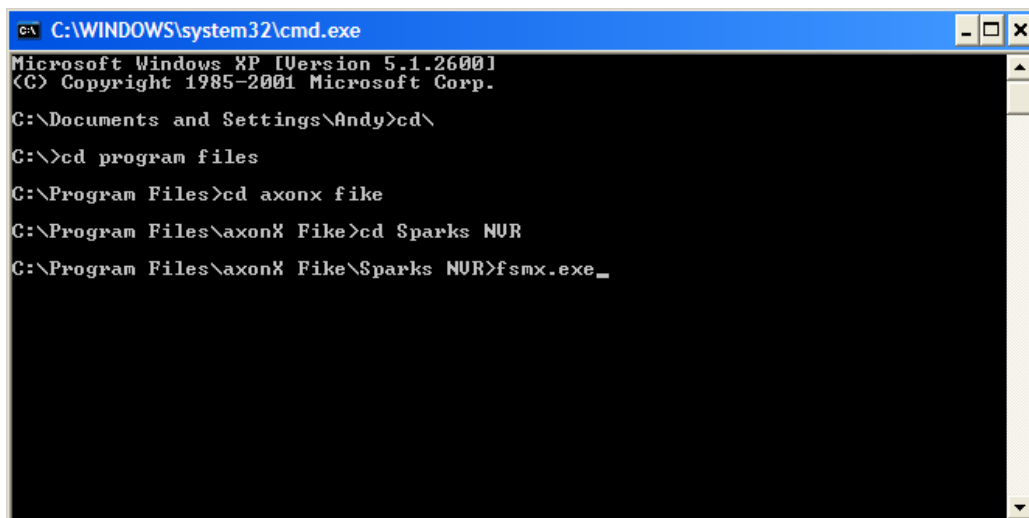


Figure 8: Sparks NVR Runtime Service.

In addition to stopping and starting, the NVR Program (fsmx.exe) executable in the services menu can be started using DOS. This would only be done while trouble shooting. To start the program in DOS, ensure that the services has been stopped. Open up the DOS window and type the location of the fsmx executable file C:\Program Files\axonX Fike\Sparks NVR, Figure 9.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

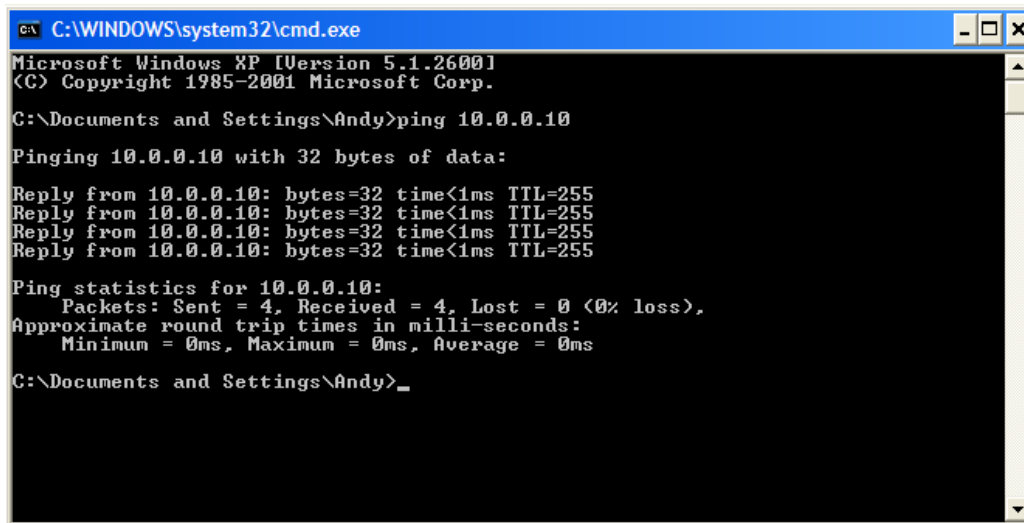
C:\Documents and Settings\Andy>cd\
C:\>cd program files
C:\Program Files>cd axonx fike
C:\Program Files\axonX Fike>cd Sparks NVR
C:\Program Files\axonX Fike\Sparks NVR>fsmx.exe_
```

Figure 9: Starting the NVR server software using the DOS command prompt.

8.0 How to PING

The “PING” tests the connection between two network nodes by sending packets to a host and then reporting the time it takes to get a response. It is a useful tool to determine if a network connection exists between a camera and the NVR as well as between the NVR and a video management software workstation. The nodes can be in a Local Area Network, Wide Area Network or anywhere on the internet. Ping (named after the submarine echo location) uses the simplest packet type. The response is done by the communication subsystem (TCP/IP) portion of the Operating System. It does not need any applications to be running, does not access any files and needs no configuration and has almost no impact on any other activity. It does require all of the hardware, gateways, routers, firewalls, name servers and intermediate hosts to be working. If the ping is successful and you cannot access the target host with a browser, NVR, or video management software, it's most likely not the network connection. Like all diagnostics, it is best to use ping in a working configuration to understand how it is supposed to work. You can ping your PC using "ping 127.0.0.1". When first setting up your PC, changing your network or if browsing the internet doesn't work use ping to validate your equipment and configurations. To PING:

- Open the command window by clicking *START*, then *RUN*. Type *CMD*, and press Enter or click OK.
- Type "ping hostname" or "ping IPaddress". For example, to ping the google main web server, type "ping www.google.com". To have your PC ping itself type "ping 127.0.0.1"
- Press "Enter", see ping Output, Figure 10.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Andy>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:

Reply from 10.0.0.10: bytes=32 time<1ms TTL=255
Reply from 10.0.0.10: bytes=32 time<1ms TTL=255
Reply from 10.0.0.10: bytes=32 time<1ms TTL=255
Reply from 10.0.0.10: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Andy>_
```

Figure 10: Using the DOS command prompt to ping an IP address on the LAN.

9.0 Configuring Server and Cameras

A channel is a representation of a camera within the server. Once configured, the server stores this information necessary to establish and maintain the network connection with the camera(s) in its internal configuration files. If any of the cameras were offline at the time the server starts, FSM-IP will make continuous attempts to establish connection while logging disconnect event.

To add the cameras to the NVR, you can use three methods. The first and easiest method is to use the Fike Video Analytics video management software. The VMS software is the Fike Video Analytics user interface that connects to each server so a user can view the cameras, edit camera settings, and view archived events. The server editor in VMS software is used to add an existing FSM-IP server into the current configuration. To add a server to the current configuration select the “Servers” tab and then click the “Add Server” toolbar button. The follow dialog box will be displayed, Figure 11:

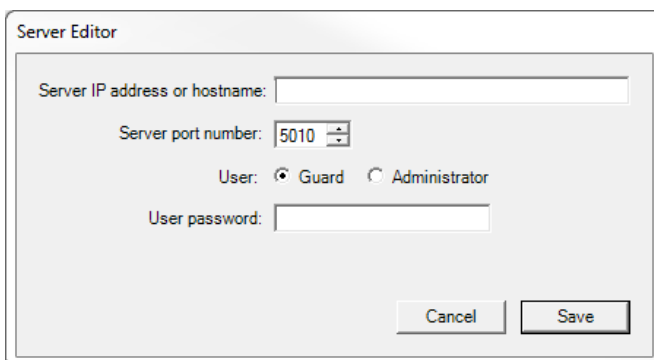


Figure 11: Adding a Server to the Video Management Software.

- **IP Address/Hostname**
Enter the IP address or hostname of the FSM-IP server you want to add.
- **Port Number**
Enter the port number of the FSM-IP server; default port number is 5010. You must ensure that this port number is not blocked by a firewall on the computer running the FSM-IP server software.

- **User**
Select the user access level you want to connect to the FSM-IP server. FSM-IP has two security profiles: guard and admin. The guard profile is not allowed to edit channel or server properties.
- **Password**
If security is enabled you must enter the correct password for the profile you want to use. If security is not enabled you can connect as either profile without the password being required.
- **Confirm Password**
Confirm the password; if no password is required this field can be left blank.

9.1 Server Properties

The Server Properties Editor is used to edit different aspects of an FSM-IP server. It is important to understand that all the server properties are stored on the server and not in the video management software configuration.

Any changes to server properties will be immediately saved on the server; however enabling security will not force existing clients to authenticate. You will need to restart the server or force all clients to reconnect because changing server security is not retroactive.

9.1.1 Security

The FSM-IP server supports a basic form of security similar to the Fike Video Analytics IP cameras. There are two built-in accounts each with their own password that provide access to the server with different privileges.

9.1.2 Operator (Guard) Account

The operator account grants read-only access to the server. In this mode an operator can view cameras, alarms and videos but can't change server or channel properties.

9.1.3 Admin Account

The admin account grants full access to the server. In this mode an admin can access all the features of the server.

9.1.4 Server Security

By default security is not enabled and no account selection or password is required to access the server. Security can be enabled through the video management software and once enabled you will be required to select a user account type and enter the correct password. See Video Management Software Operations Manual for details. To edit a server's properties select the "Servers" tab and then click the "Properties" toolbar button. The following dialog box will be displayed, Figure 12:

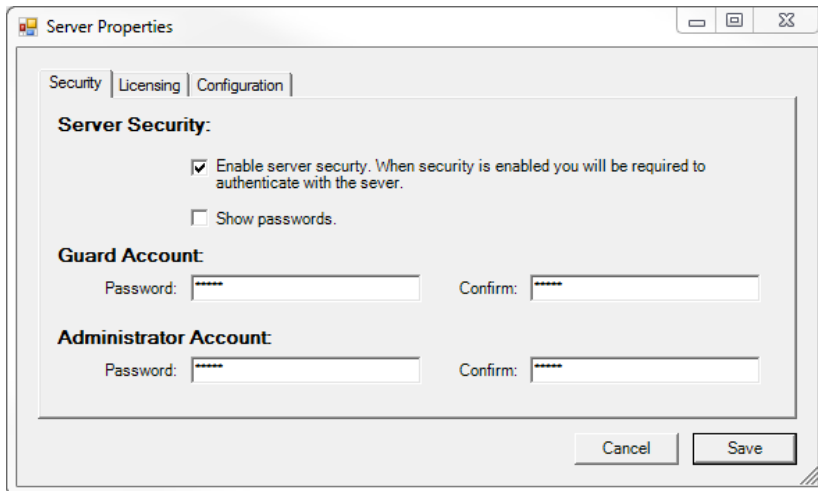


Figure 12: Configuring Server Security

- The Security Tab is used to enable and disable server security. You must enter and confirm a password for the guard and admin profiles if you enable security.
- The Show Passwords option is strictly a video management software client feature and has no bearing on server security. It is meant to enable an admin to recover the password in the event it is forgotten.

9.1.5 Channel Editor

Channel settings are stored on the physical camera and cached on the server that owns the channel. The server cache expires every 5 minutes by default. To access a channel's setting you can select a camera from the channel list and select the "Properties" button on the channel toolbar.

9.1.6 Channels Section

The channels section of the "Servers" tab displays all the channels of the currently selected server.

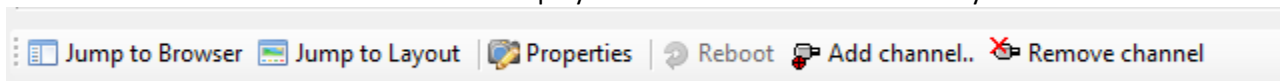


Figure 13: Channel Toolbar

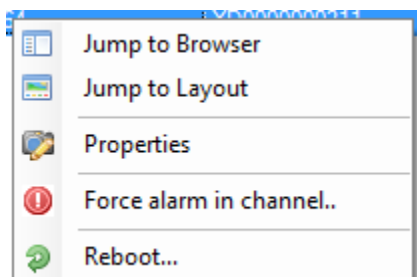


Figure 14: Channel Menu

- **Jump to Browser**
Switches to the Browser tab and displays the first camera in the org tree with this channel bound to it.
- **Jump to Layout**
Switches to the Browser Layout tab and displays the first org item in the org tree with this channel as a child.
- **Properties**
Loads the channel properties dialog box
- **Reboot**
Reboots the camera
- **Add Channel**
Looks for Fike Video Analytics IP cameras on the network and allows the user to select the camera to add to the server.

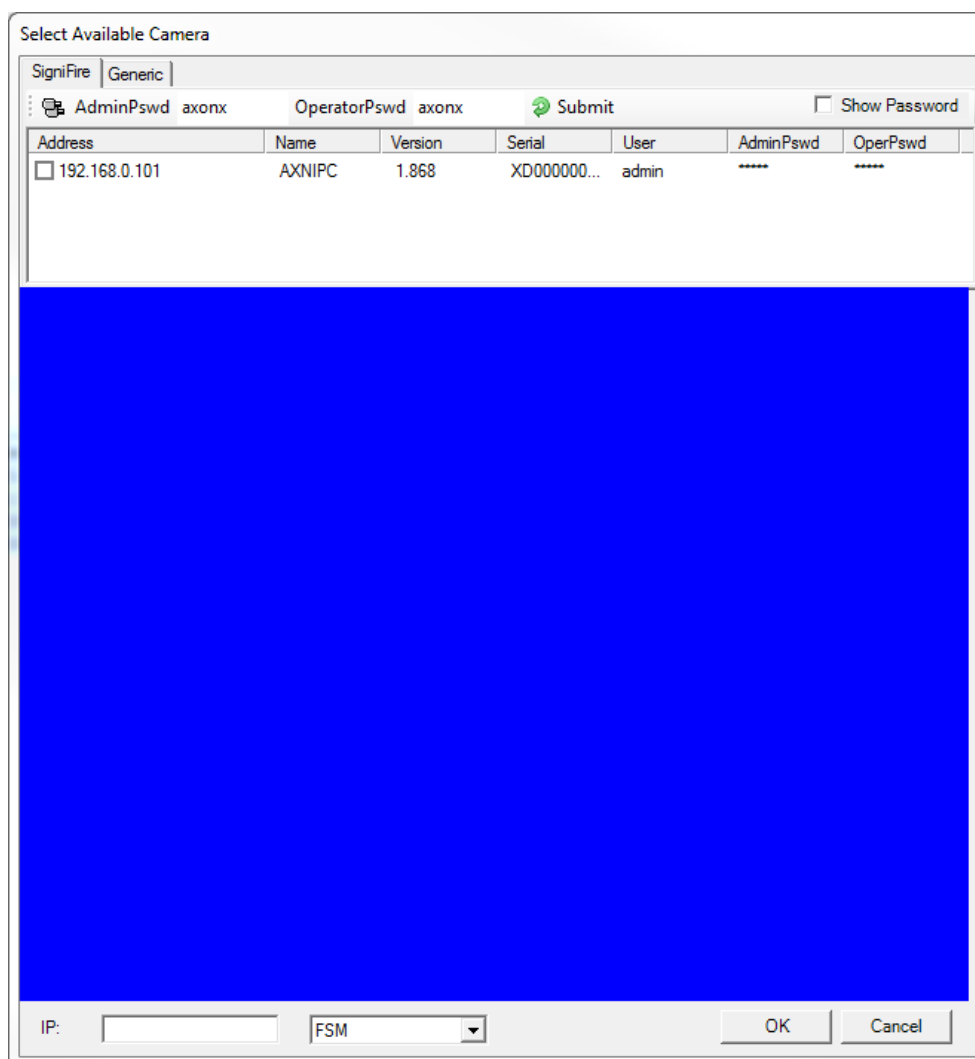


Figure 15: Channel Selection Window.

- **Remove Channel**
Removes the selected channel
- **Remove All**
Removes all the channels attached to the server











	Channel	State	Status	Name	Address	Version	Serial
	1	Online	Normal	SigniFire IP	10.0.0.105	1.836	XD0000000552
	2	Online	Normal	SigniFire IP	10.0.0.106	1.836	XD0000000553
	3	Online	Normal	SigniFire IP	10.0.0.107	1.836	XD0000000557
	4	Online	Normal	SigniFire IP	10.0.0.102	1.836	XD0000000412
	5	Online	Normal	SigniFire IP	10.0.0.103	1.836	XD0000000411
	6	Online	Normal	SigniFire IP	10.0.0.104	1.836	XD0000000416
	7	Online	Normal	SigniFire IP	10.0.0.108	1.836	XD0000000558
	8	Online	Normal	SigniFire IP	10.0.0.109	1.836	XD0000000556
	9	Online	Normal	SigniFire IP	10.0.0.110	1.836	XD0000000551
	10	Online	Normal	SigniFire IP	10.0.0.147	1.842	XD0000000535

Figure 16: Channel Details

- **Channel**
The unique channel ID assigned to the camera by the server.
- **State**
Online/Offline
- **Status**
The alarm status of the camera
- **Name**
The name of the camera
- **Address**
Provides the IP address of the camera
- **Version**
The firmware version running on the camera
- **Serial**
The serial number of the camera

10.0 Conclusion

Once the desired cameras are connected to the server, the monitoring workstations can be configured and attached to the server and the system commissioning can occur. Please refer to the Fike Video Analytics Video Management Software Operations Manual and IP Camera Operations Manual for further assistance.

Revision History

Revision	Date	Revision Description
0	06/09	Initial Release
1	07/10	Changed from Ada programming language to .NET framework
2	01/15	Company name change from AxonX to Fike Video Analytics Corporation.
3	06/19	<ol style="list-style-type: none">1. Revised to replace references to SigniFire with Fike Video Analytics video management software.2. Deleted Section 9.2 NetCamVue.3. Deleted Section 9.3 Telnet.4. Updated document to latest Fike document standard.



Fike[®]
Video Analytics Corporation

CONTACT US

Fike Video Analytics Corporation
704 SW 10th Street
Blue Springs, Missouri 64013-0610 USA
Tel: +001 844-345-3843
www.Fike.com

For a list of contact information for Fike offices around the world, visit the [Global Locations](#) section of Fike.com