Embedded Video Gateway

Configuration and management guide for SerVision HVG400, UVG400, MVG200, MVG400, CVG, and CVG-M Video Gateway models

March 2014
Trademarks & Copyright

Trademarks

All trademarks mentioned in this manual are the sole property of their respective manufacturers.

Copyright

SerVision Ltd., Jerusalem, Israel
www.servision.net  •  info@servision.net
© 2014 SerVision Ltd. All rights reserved.

Notice

Information in this document is subject to change without notice. SerVision Ltd. assumes no responsibility for any errors that may appear in this manual. Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be copied or reproduced in any form, or by any means, electronic or mechanical, for any purpose, without the express written permission of SerVision Ltd. SerVision Ltd. makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability or fitness for a particular purpose.
# Table of Contents

## Getting Started
- About this Guide 5
- About Client Software 6
- Before You Begin 6
- Installing SVMultiClient 7
- Opening the Configuration Utility 8
- Overview of the Interface 10
  - Top-Level Menu Options 10
  - Status Bar 11
- Using the Configuration Utility 11
- Opening the Configuration Remotely 14
- Opening the Configuration Manually 14

## Configuring System Settings
- General System Settings 17
  - About the General System Settings 17
  - Configuring General System Settings 21
- Configuring a CCTV Monitor (TV-Out) 25
  - Configuring the Monitor to Display Video from the Video Gateway 26
  - Configuring the Monitor to Play Prerecorded Video 30
- Setting the Unit Time 33
  - Updating the Date and Time Manually 35
  - Configuring Automatic Time Setting 37
- LAN Settings 38
- Modem 40
  - Video Gateway with Router 41
  - CVG-M 45
- WiFi 47
  - Configuring the Unit to Connect to WiFi Access Points 47
  - Removing an Access Point from the List 52
  - Turning WiFi Off 52
  - Configuring the Unit to Function as an Access Point 53
- Network Priorities 54
- Port Forwarding 55
- Proxy and DDNS Settings 57
- Authentication 60
- SMS and E-mail Notifications 61
  - SMS Message Templates 66
  - Testing Notification Settings 67
- Automatically Uploading Video to an AVV Server 67
  - Viewing the List of Files on the AVV Server 72
  - Viewing Video from the AVV server 73
  - Disabling AVV 75
- FTP Server Settings 75
- Schedules 77
  - Configuring a Standard Weekly Schedule 79
  - Defining Holiday Schedules 81
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining a New Schedule Row</td>
<td>84</td>
</tr>
<tr>
<td>Audio Settings</td>
<td>86</td>
</tr>
<tr>
<td>Configuring Microphone and Speaker Volume</td>
<td>87</td>
</tr>
<tr>
<td>GPS</td>
<td>89</td>
</tr>
<tr>
<td>Configuring GPS</td>
<td>89</td>
</tr>
<tr>
<td>Erasing Recorded GPS Data</td>
<td>91</td>
</tr>
<tr>
<td><strong>Configuring Camera Settings</strong></td>
<td>92</td>
</tr>
<tr>
<td>About Brightness and Contrast Settings</td>
<td>92</td>
</tr>
<tr>
<td>Configuring Video Cameras</td>
<td>92</td>
</tr>
<tr>
<td>Configuring PTZ</td>
<td>96</td>
</tr>
<tr>
<td>Video Motion Detection (VMD)</td>
<td>97</td>
</tr>
<tr>
<td>About VMD Regions</td>
<td>97</td>
</tr>
<tr>
<td>About VMD Event Settings</td>
<td>97</td>
</tr>
<tr>
<td>About Responses to VMD Events</td>
<td>98</td>
</tr>
<tr>
<td>Configuring VMD Settings</td>
<td>98</td>
</tr>
<tr>
<td>Configuring Video Lost</td>
<td>103</td>
</tr>
<tr>
<td>Video Recording Settings</td>
<td>105</td>
</tr>
<tr>
<td>Configuring Video Recording</td>
<td>106</td>
</tr>
<tr>
<td>Advanced Recorder Settings</td>
<td>107</td>
</tr>
<tr>
<td>Restoring Default Recording Settings</td>
<td>111</td>
</tr>
<tr>
<td>Erasing Recorded Video</td>
<td>114</td>
</tr>
<tr>
<td>Erasing All Recorded Video from a Camera</td>
<td>114</td>
</tr>
<tr>
<td>Erasing All Recorded Video from the Storage Media</td>
<td>115</td>
</tr>
<tr>
<td>Restoring the Default Disk Allocation</td>
<td>117</td>
</tr>
<tr>
<td><strong>Configuring Sensor and Activator Settings</strong></td>
<td>120</td>
</tr>
<tr>
<td>Configuring Sensors and Activators</td>
<td>120</td>
</tr>
<tr>
<td>Configuring Sensor 1 to Switch Outlines</td>
<td>126</td>
</tr>
<tr>
<td>Configuring a Sensor to Control CCTV Display</td>
<td>127</td>
</tr>
<tr>
<td>Configuring an Activator as a Power Switch</td>
<td>128</td>
</tr>
<tr>
<td>Configuring Vehicle-Behavior Sensors</td>
<td>129</td>
</tr>
<tr>
<td>Configuring a Geo-Fence Sensor</td>
<td>129</td>
</tr>
<tr>
<td>Configuring a Speed-Limit Sensor</td>
<td>146</td>
</tr>
<tr>
<td>Configuring an Idle Monitor</td>
<td>147</td>
</tr>
<tr>
<td>Configuring a G-Force Sensor</td>
<td>148</td>
</tr>
<tr>
<td><strong>Defining Alternate Outlines</strong></td>
<td>150</td>
</tr>
<tr>
<td>Creating an Outline</td>
<td>150</td>
</tr>
<tr>
<td>Activating Outlines Manually</td>
<td>155</td>
</tr>
<tr>
<td><strong>Saving Configuration Changes</strong></td>
<td>157</td>
</tr>
<tr>
<td>Discarding Changes</td>
<td>159</td>
</tr>
<tr>
<td>Restoring Default Settings</td>
<td>160</td>
</tr>
<tr>
<td><strong>Connecting to the Video Gateway</strong></td>
<td>164</td>
</tr>
<tr>
<td>Connecting Through SVMultiClient</td>
<td>164</td>
</tr>
<tr>
<td>Connecting through the Configuration Utility</td>
<td>166</td>
</tr>
<tr>
<td>Viewing Events</td>
<td>167</td>
</tr>
<tr>
<td>Viewing Snapshots</td>
<td>169</td>
</tr>
<tr>
<td><strong>System Diagnostics</strong></td>
<td>172</td>
</tr>
<tr>
<td>System Statistics</td>
<td>173</td>
</tr>
<tr>
<td>Testing Remote Connections</td>
<td>174</td>
</tr>
<tr>
<td>Ping</td>
<td>174</td>
</tr>
<tr>
<td>Traceroute</td>
<td>177</td>
</tr>
</tbody>
</table>
SerVision’s embedded Video Gateways are compact Video Gateway units that provide state-of-the-art security functionality for a wide range of environments, from offices and homes to vehicles and other moving platforms. All units feature live video streaming, video recording and playback, motion detection, sensor management, and real-time event notification and device activation. These features can be accessed remotely via PC, PDA, or cellular telephone.

All Video Gateway units can connect to computer networks, including local networks and the internet, using cable-based Ethernet connections. Some models also support wireless network connections via cellular networks and WiFi. In addition, mobile models support GPS tracking, and can be integrated with some third-party fleet-management systems.

The following embedded Video Gateway models are currently available:

- **HVG400**: A four-channel Video Gateway optimized for homes and small offices. The HVG400 features a built-in hard drive capable of storing large quantities of recorded video and supports a cable-based connection to a network.
- **UVG400**: A four-channel Video Gateway that is ideal for deployment in locations where cabled network connections are not available, such as building sites, parking lots, and horse stables. The UVG400 can connect to a network via Ethernet, cellular, or WiFi and contains a built-in hard drive capable of storing large quantities of recorded video.
- **MVG400**: A four-channel Video Gateway designed for deployment in vehicles such as buses, trains, and delivery trucks. The MVG400 contains a removable hard drive capable of storing large quantities of recorded video. It can connect to cellular and wireless networks, and also supports GPS that enables remote users to locate and track the vehicle in which it is installed.
- **MVG200**: A two-channel Video Gateway designed for deployment in smaller vehicles such as cars, vans, and mini-buses. The MVG200 records video and other data on a removable SD card. It can connect to cellular and wireless networks, and supports GPS tracking.
- **CVG**: A compact, two-channel Video Gateway optimized for streaming live video from indoor locations. The CVG stores video and other data on a removable SD card, and can connect to cable-based networks.
- **CVG-M**: A compact, two-channel Video Gateway optimized for streaming live video from vehicles. The CVG-M can connect to cable-based and cellular networks, and also supports GPS that enables remote users to locate and track the vehicle in which it is installed. It stores video on a removable SD card.

### About this Guide

All Video Gateway models are configured using a browser-based configuration utility that is accessed via PC. This guide explains how to use the configuration utility to configure and manage an embedded Video Gateway unit. The guide assumes the unit is already installed in its intended location, all required devices are connected to it, and it is connected to a power source and a network. For information about installing your Video Gateway unit, please refer to its installation guide.

The following topics related to the configuration utility are covered in this manual:

- Configuring the unit (page 8)
- Connecting to the unit to check that the configuration settings are correct and to view video, snapshots, or event information (page 164)
- Resetting the unit (page 198)
- Diagnosing system problems (page 172)

This guide also includes information about system maintenance and handling problems:

- Upgrading the firmware (page 184)
• Restoring the factory settings of the unit (page 199)
• Troubleshooting (page 202)

Most embedded Video Gateway models can be used in conjunction with a CCTV monitor. The monitor can be used to view video from the cameras connected to the unit. Instructions for viewing video on a CCTV monitor are included in an Appendix to this guide (see Appendix A: Viewing Video on a CCTV Monitor (TV-Out), page 208).

Because this guide relates to a number of different embedded Video Gateway models, certain parts of the manual are only relevant to specific models. Information that only relates to some of the models is color-coded in teal. For example, a paragraph that is only relevant to the MVG200 and CVG-M models would appear like this:

This is an example of a paragraph that only relates to the MVG200 and CVG-M models.

If an entire section is only relevant for particular models, the beginning and end of the section is marked and labels appear at the top of the section. The labels indicate the models for which the section is relevant. For example, a section that is only relevant to the MVG400, MVG200, and CVG-M models would appear like this:

### GPS

Only the MVG400, MVG200, and CVG-M models support GPS position tracking.

The features of the two MVG models, MVG200 and MVG400, are nearly identical. For this reason, they are often referred to collectively as the "MVG." Similarly, a single label may be used to represent both models:

![MVG Models](image)

*Figure 1: Label representing both models of the MVG collectively*

Because the Video Gateway models have slightly different features, their configuration is different in some cases. Screenshots of the configuration utility that appear in this guide may be from a different model than the one you are configuring, and may therefore not exactly match the screens you see. If the screen that is displayed differs significantly from model to model, the name of the model from which the screenshot was taken appears in parentheses in the caption below the screenshot.

### About Client Software

Client software is used for accessing the Video Gateway unit remotely in order to view video and events and control the system in various ways. This guide includes a general overview of SVMultiClient, SerVision’s PC-based client software. A complete user guide for SVMultiClient is available on the SerVision website (http://www.servision.net). SerVision also offers client software for certain cellular telephones, tablet PCs, and PDAs. These applications, and user guides for them, can be downloaded from the SerVision website. In addition, SVControlCenter is a complete control-center solution that includes powerful client features, for enterprises managing sizable numbers of Video Gateways. Additional information about SVControlCenter is available on the SerVision website and from SerVision customer-service representatives.

### Before You Begin

Before the Video Gateway unit can be configured, the hardware should be set up as follows:

• The Video Gateway unit should be installed and connected to a power supply. (Installation guides for all Video Gateway models are available on the SerVision website.)
• All the cameras and optional devices (sensors, activators, etc.) should be connected to the Video Gateway unit and to their power supplies, as necessary.

• A PC should be on the same LAN as the Video Gateway or connected to the unit by a LAN cross cable.

There are two ways that you can connect a PC to the same LAN as an MVG400 or UVG400:

• Using the supplied Ethernet (network) cable, connect the network connector of the PC to one of the Ethernet In connectors on the rear panel of the unit. The PC will then be included in the network managed by the router. (It is preferable to use this method the first time you connect to the unit, before it has been configured.)

• Using the supplied Ethernet (network) cable, connect the Ethernet Out connector on the rear panel of the unit to a LAN connection point. Connect the PC to the same LAN through a different connection point.

**NOTE:** Do not connect a LAN connection point to one of the Ethernet In connectors; if you do, the system will not function properly and will reset itself continuously.

### Installing SVMultiClient

The simplest way to open the Video Gateway’s configuration utility is by using the SVMultiClient application on a PC that is on the same LAN as the Video Gateway (see *Before You Begin*, page 6). Thus, before you begin configuring the Video Gateway, you should install SVMultiClient on the computer that you will use for the configuration tasks.

After the unit is configured, you can check the installation and configuration using the SVMultiClient you installed on the PC (see *Connecting to the Video Gateway*, page 164). If this is successful, you can then install SVMultiClient on a remote computer and connect to the Video Gateway via the internet.

**NOTE:** This chapter explains how to get started using SVMultiClient on a PC that is on the same LAN as the Video Gateway so that you can configure the system and make sure it is working properly. For complete information about connecting to SVMultiClient, locally or remotely, and using SVMultiClient to view video, monitor events, and control devices, please refer to the *SVMultiClient User Guide*.

**📌 To install the SVMultiClient application on the PC:**

1. Download the latest version of the SVMultiClient installation program from the SerVision website ([http://www.servision.net](http://www.servision.net)). The installation file is called `Setup-MultiClient-SV-xxxx.exe` (The software version number appears in place of “xxxx”.)

1. Double-click the installation file. The setup program starts.
   **Note:** If a Microsoft Windows *Security Warning* dialog box is displayed, click **Run**.

2. Follow the on-screen instructions.
   When the installation is completed, a SVMultiClient application icon is placed on your desktop.

*Figure 2: SVMultiClient desktop icon*
Opening the Configuration Utility

This section explains how to work with the configuration utility – how to open it, access its main menu, and navigate to the various configuration screens. The menu options and their settings are described in detail in the following chapters.

When you first open the configuration utility, you should open it through SVMultiClient, as explained in this section. This method of opening the configuration utility is recommended whenever SVMultiClient is on a PC that is on the same network as the Video Gateway (or the PC and the Video Gateway are connected via a LAN cross cable).

No internet connection is required to configure the Video Gateway. Once the network settings of the unit have been configured in such a way that the unit can be accessed remotely via the internet, the configuration utility can also be accessed remotely. For additional information, see Opening the Configuration Remotely, page 14.

NOTE: The configuration utility is compatible with Internet Explorer and Firefox.

To open the configuration utility:

1. Open the SVMultiClient application by double-clicking the desktop icon or by selecting it in the Start menu (Start>Programs>SerVision>SVMultiClient>SVMultiClient).

2. In SVMultiClient, at the bottom of the Connection Panel, click the Search button.

Figure 3: Search button

The Find Gateway dialog box opens, and displays a list of all the SerVision systems connected to the network.
3. Select the Video Gateway and then click **Configure**. A browser window opens and displays the configuration **Login** screen.

4. Fill in the **User Name** and **Password** fields.

   **Note:** By default, the username is **svuser** and the password is **servconf**. Use these values the first time you log into the configuration utility. Once you have logged in, it is recommended that you change these values (see **Authentication**, page 60).

   The **Summary** screen opens:
Overview of the Interface

The configuration utility consists of screens that are displayed on the right side of the window and a Main Menu in a sidebar on the left side of the window.

The Main Menu has a hierarchic tree structure. When you select one of the top level options, lower-level options appear below it in the menu.

Top-level menu options generally open summary screens that display the current settings in a given category and may include links from which you can access some of the lower-level screens in the selected category. Lower-level screens are used to modify configuration settings and manage the system.

Top-Level Menu Options

The following top-level menu options are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays a summary of the system's settings and status</td>
</tr>
<tr>
<td>Cameras</td>
<td>Configuration of video settings for each camera, including PTZ settings (remote camera control), VMD (Video Motion Detection), and recording settings</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
Sensors | Configuration of sensors and activators
Outlines | Configuration of sets of different camera and sensor settings that can be activated either manually or automatically in response to sensor events or according to a fixed schedule
System | • Configuration of general system settings, including network settings, unit date and time, authentication, configuration of SMS and e-mail notifications, and TV-Out settings
 | • Saving configuration changes on the unit and restarting the unit
Diagnostics | Tools for monitoring and testing the system
Client | Viewing lists of events that were detected, selecting events to download to an FTP server, viewing live snapshots from a camera

## Status Bar
A status bar at the top of the screen contains the following elements:

- **Model**: Video Gateway model number
- **Version**: Firmware version
- **Outline**: Name of the current outline (see **Defining Alternate Outlines**, page 150)
- **Logout** button; click to log out of the configuration utility and display the **Login** screen again
- **Help** button; click to open the SerVision website in a browser window. The website includes information about configuring and working with your Video Gateway system, including the most up-to-date version of this manual (under **Support->Documentation->Manuals and Product Overviews**)

### Using the Configuration Utility
Typically, the configuration process proceeds as follows:
To configure a Video Gateway unit:

1. In the Main Menu, click one of the top-level options, e.g., Cameras or Sensors. The selected summary screen opens.

2. Click an option in the Main Menu or a link in the summary screen to open the desired lower-level screen. The screen opens.

3. Modify the settings in the settings in the screen as necessary, and then click Update to store them on the unit.

Figure 9: Update button

The changes are saved in a temporary cache on the unit, and an Update Confirmation (ATTENTION) message appears at the lower left of the screen, below the Main Menu.

Figure 10: Update confirmation message
Note: If the update confirmation message does not appear, or an error message appears, all changes made since the last successful update of the page are discarded.

4. To modify additional settings, navigate to the relevant screen and make the changes as necessary. Click Update in each screen when you are finished modifying its settings. (You can continue modifying the settings in the same screen, if necessary; just be sure to click Update before you navigate to a different screen to ensure the settings are saved as they are displayed.)

5. When you have updated all the settings as necessary, do one of the following:
   - In the update confirmation message, click “Click here to go to Save Settings page.”
   - In the Main Menu, under System, click Save Settings.

The Save Settings screen opens:

![Figure 11: Save Settings screen](image)

6. In the Save Settings screen, click Save Changes to System. The unit stores the changes permanently, and the System Restart Page screen opens:

![Figure 12: System Restart Page screen](image)
7. Click Restart System. The unit restarts, and the changes are implemented. You are automatically logged out of the configuration utility.

**Note:** Most changes to the settings in the configuration screens only take effect on the Video Gateway unit after they are saved and the unit is restarted, as describe in steps 5–7. For additional information, see Saving Configuration Changes, page 157.

**Note:** For security reasons, a configuration session times out after 15 minutes. If the configuration utility is open with no user activity (pages loaded) for more than 15 minutes, you must perform the login procedure again to continue configuring the Video Gateway unit. Configuration changes that were made during the timed-out session are not discarded, as long as Update was clicked in the relevant screen before the time-out occurred.

**Opening the Configuration Remotely**

Once the unit has been configured for remote client access via the internet (see LAN Settings, page 38), you can also access the configuration utility remotely via the internet. To do this, all you need is a PC that is connected to the internet. You can then access the configuration utility in one of the following ways:

- **Through SVMultiClient:** Connect to the Video Gateway and use SVMultiClient to access the configuration utility, as explained below. (For additional information about working with SVMultiClient, please refer to the SVMultiClient User Guide.)

- **Manually through a browser:** Enter the address and port in the Address field of a browser window, as described under Opening the Configuration Manually, page 14.

Both of these methods can also be used to access the configuration utility over the internet through a proxy connection.

**To access the configuration utility remotely through SVMultiClient:**

1. Connect to the Video Gateway through SVMultiClient.

   **Note:** SVMultiClient’s Search function does not work over the internet. Therefore, you will have to manually add and configure the connection to the Video Gateway. For information about how to do this, please refer to the SVMultiClient User Guide.

2. In the Connection Panel (left panel) of SVMultiClient, select the Video Gateway.

3. At the bottom of the Connection Panel, click the Config button. A new browser window opens, and automatically connects to the configuration utility login page for the Video Gateway.

   **Note:** If you cannot connect remotely through port 10000, the login page will not appear at this point, and the browser will display an error message instead. Change the port number in the Address field of the browser from 10000 to the port that is set in the router’s port forwarding settings (see General System Settings, page 17), and press Enter to reload the page. The login page should then appear. For additional information, see Opening the Configuration Manually, below.

   **Note:** If more than one SerVision Video Gateway is connected to the internet via the same router, each of them must use a different port. When you click Config in SVMultiClient, the browser automatically connects to port 10000. As a result, SVMultiClient may initially connect you to the wrong Video Gateway unit. In this case, you should manually correct the port number in the Address field of the browser, as explained in the previous note.

**Opening the Configuration Manually**

The configuration utility can be opened manually in a browser using the IP address and port of the unit. This is particularly useful in situations in which you cannot open the configuration utility through SVMultiClient. This is most likely to occur when you are opening the configuration utility remotely and either do not have access to SVMultiClient or cannot connect to the unit remotely through port 10000.
To open the configuration utility manually, you must know the network address (IP or hostname) of the Video Gateway and the port allowing access to the configuration utility. The required network address depends on whether you are accessing the configuration utility through a local connection (through the same LAN or through an Ethernet cross cable) or a remote connection (through the internet):

- **Local connection**: The network address is the private IP address of the Video Gateway on the local network. This can either be its dynamic IP, or, if it has one, its static IP. The port is 10000.

- **Remote connection**: The network address is the public IP or hostname of the router through which the Video Gateway connects to the internet. The port is the port that allows access to the configuration utility via port forwarding.

If you connect through a proxy connection, you must also know the network address and port of the proxy server.

**To open the configuration utility manually:**

1. Open a web browser.

2. In the **Address** field of the browser, enter the IP address and system port number of the Video Gateway, as follows:

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct (local or remote)</td>
<td><a href="http://IP:port">http://IP:port</a></td>
</tr>
<tr>
<td></td>
<td>For example, if the Video Gateway’s IP address is 192.168.1.210 and you are connecting on port 10000, enter <a href="http://192.168.1.210:10000">http://192.168.1.210:10000</a>, as in figure 13:</td>
</tr>
<tr>
<td></td>
<td><img src="image1" alt="Figure 13: Address for configuring a unit with a static IP" /></td>
</tr>
<tr>
<td>Proxy</td>
<td><a href="http://Proxy-IP:Proxy-port/Video">http://Proxy-IP:Proxy-port/Video</a> Gateway name/Video Gateway port/</td>
</tr>
<tr>
<td></td>
<td>For example, if the proxy server’s IP address is 111.111.1.2, its port number is 9111, the name of the Video Gateway is CVG_1, and its port is 10000, enter <a href="http://111.111.1.2:9111/CVG_1/10000/">http://111.111.1.2:9111/CVG_1/10000/</a>, as in figure 13:</td>
</tr>
<tr>
<td></td>
<td><img src="image2" alt="Figure 14: Address for configuring a unit via a proxy server" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Be sure to include the slash (/) at the end of the address.</td>
</tr>
</tbody>
</table>

3. Press **Enter**. The configuration utility **Login** screen opens.

4. Log into the configuration utility as usual (see page 9).
Configuring System Settings

System settings include system-wide settings, such as the name of the unit, date and time settings, and network configuration.

The **System Summary** screen summarizes the current system settings and provides links to some of the system configuration screens in which the system settings can be modified. It also includes information about the Video Gateway unit and the network, and, depending on the configuration settings, may include buttons that you can use to test the current e-mail and SMS notification settings.

![Screen Shot](image)

**Figure 15: System Summary screen (MVG)**

The following system-configuration screens are available:

- **General**: Unit name, port number, and activation of certain options (see page 17)
- **TV-Out**: Configuration of a closed-circuit monitor (CCTV) connected to the Video Gateway (see page 25)
- **Date & Time**: Automatic and manual time setting (see page 33)
- **LAN**: Ethernet network settings (see page 38)
- **Modem**: Cellular modem configuration (UVG400, MVG, and CVG-M only; see page 40)
- **WiFi**: Wireless network connection and access-point settings (UVG400 and MVG only; see page 47)
- **Network Priorities**: Ranking the available network connections for outgoing communication from the unit to other networks, to indicate which connections should be tried first (UVG400 and MVG; see page 54)
- **Port Forwarding**: Configuring ports that allow external devices to connect to devices within the local network managed by the Video Gateway’s router (UVG400 and MVG only; see page 55)
- **Proxy and DDNS**: Proxy and DDNS settings (see page 57)
- **Authentication**: Usernames and passwords for accessing and configuring the unit (see page 60)
• SMS & E-mail: Event notification settings (see page 61)
• AVV: Configuration of automatic uploading of video to an FTP server (see page 67)
• FTP: Configuration of manual uploading of video to an FTP server (see page 75)
• Schedules: Configuring the unit to automatically switch the running outline at specified times (see page 77)
• Power Saving: Configuring sleep-mode (in development, for use with certain control-center applications; MVG only)
• Audio: Configuring microphones and speakers (see page 86)
• GPS: Configuring GPS settings (MVG and CVG-M only; see page 89)
• Save Settings: Saving configuration changes (see page 157)
• Restart: Restarting the unit in order to fully implement configuration changes or improve system performance (see page 198)

🔗 **To open the System Summary screen:**

• In the **Main Menu**, click **System**.

**NOTE:** If Content mode is enabled in the TV-Out settings, a warning message appears at the top of the System Summary screen:

**SYSTEM SUMMARY**

**WARNING:** THE SYSTEM IS RUNNING IN CONTENT MODE. ANY STREAMING WILL AUTOMATICALLY PAUSE THE CONTENT PLAYBACK

<table>
<thead>
<tr>
<th>SYSTEM STATISTICS</th>
<th>Memory</th>
<th>DSP</th>
<th>HD Size</th>
<th>HD Model</th>
<th>CARPET</th>
<th>AES KEY</th>
<th>Video Rate</th>
<th>Video Codec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>64MB</td>
<td>72MHz</td>
<td>VDC-25000BP-V2.05STI</td>
<td>TFL-1_192 BT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For additional information, see *Configuring the Monitor to Play Prerecorded Video*, page 30.

### General System Settings

The general system settings are the basic settings for the unit: the name of the unit, the port it uses for communication, video resolution and type, and activation of certain optional features.

### About the General System Settings

This section contains background information about the general system settings.

### Ports

The unit has two access ports:

• Port 10000, which is intended for configuration and is always open for incoming connections.
• System port, which is intended for client connections, and can be configured. The default number of this port appears on the sticker on the underside of the unit. (It is usually 9988.) You can configure this port as necessary to suit the requirements of your network.

**NOTE:** If port forwarding in your network cannot be set up for port 10000, you can use the system port for remote configuration as well as client connections.

**Video Resolution**

The Video Gateway can capture video in one of the following resolutions:

- **VGA:** This resolution is the standard used by digital screens such as computers and cellular phones. When VGA is selected, the full-screen resolution is 640x480 pixels. Available smaller screen sizes are SIF (one quarter of full screen; 320x240 pixels) and QSIF (one sixteenth of full screen; 160x120 pixels).

- **D1:** This resolution is the standard used by analog screens such as televisions. When D1 is selected, full-screen resolution is 704x480 pixels for NTSC systems and 704x576 pixels for PAL systems. Available smaller screen sizes are CIF (one quarter of full screen; 352x240 pixels for NTSC systems and 352x288 pixels for PAL systems) and QCIF (one sixteenth of full screen; 176x120 pixels for NTSC systems and 176x144 for PAL systems).

VGA normally displays properly even on analog equipment such as CCTV screens. If your system supports both resolutions, it is recommended that you select VGA resolution because it requires slightly less system resources.

**Ignition-Off Shut-Down**

The **Ignition** settings define whether the MVG or CVG-M unit should automatically shut down when the vehicle ignition is turned off and, if so, how long the unit should continue operating after the ignition is turned off before it shuts down.

**Download Optimizations**

Downloading recorded video uses system resources that would otherwise be available for other functions such as recording or streaming live video. Download optimization settings are used to tweak the allocation of system resources between downloading and other system processes.

These optimization settings are most important for mobile Video Gateways, which may be subject to vastly different network conditions at different times. For example, if a bus is on the road, it typically only has access to a cellular connection, which has very limited bandwidth, but when it is the bus yard, it probably also has access to a high-speed WiFi network. In this case, downloading of the recorded video can be scheduled for times when the bus is in the yards. Since recording video is only necessary when the bus is on the road, it is best to suspend recording while downloading is being performed, because this speeds up the downloading process.

The following download-optimization options can be selected:

- **Enabled:** Prevents the unit from initiating transmission of a new stream of recorded video to a client device, and from beginning to download live or recorded video to a client device, when video is already being downloaded from the unit. Live streams can be initiated, and all processes that are already in progress (streaming of live or recorded video to a client or to a connected CCTV monitor, and downloading of video) continue uninterrupted, unless one or more of the download-optimization options described below are selected.

- **Stop Recording on Download:** In addition to the above, stops all video recording on the unit when video is being downloaded from the Video Gateway. This option increases the download speed, because it allocates more of the unit’s resources to the download task. However, it also means that there may be gaps in the recorded video at the times that the video is downloaded.
• **Close All Tasks on Download**: Prevents the unit from performing any other jobs – accepting new connections, streaming live or recorded video, recording video, or downloading other video – when downloading is in progress.

• **Block New Connections while Downloading**: Prevents the unit from accepting any new connections from clients while downloading of recorded video is taking place. When this option is selected, transmission of new live or recorded video streams to client applications does not begin while downloading is underway, but existing streams are not closed. When this option is not selected, the process of downloading may take somewhat longer to be completed. In addition, the framerate of video displayed in the client may be reduced at times while the download is in progress.

• **Disable TV-Out While Downloading**: If a CCTV monitor is connected to the Video Gateway, stops streaming of video to the monitor while downloading of recorded video is taking place

### Additional System Settings

A number of other system settings can be configured in the **General System Settings** screen:

• **Video Authentication**: Adds a digital signature to each frame of video captured by the system. This signature makes it possible to identify frames that have been tampered with. When a SerVision client application plays video that has a digital signature and discovers a frame that has been changed from its original state, the status of the stream indicates that the stream was modified. (Note: Only the current versions of SVMultiClient and the Player support this feature.)

• **Outline Switching**: Defines whether the system can activate different outlines automatically and, if so, what type of trigger will cause the system to switch to a different outline, sensor events (from Sensor 1) or a schedule. If neither type of automatic outline switching is selected, you can manually change the active outline at any time. For additional information, see Defining Alternate Outlines, page 150.

• **Network Speed Optimization**: Activates zero-latency handling of video packets. Activating this option may increase the transmission speed of video from the Video Gateway to client PCs that are on the same LAN as the Video Gateway. This feature is not recommended for use with other types of client connections (internet, cellular, etc.). In addition, it is only recommended for use if video transmission speed is problematic. It usually has a more marked effect on video streaming than on video downloading.

• **Network TCP Optimization**: Opens all sockets with TCP_NODELAY activated. Activating this option may increase the transmission speed of video from the Video Gateway to client PCs that are on external networks – internet, cellular, etc. This feature is not recommended for use with clients that are on the same LAN as the Video Gateway. In addition, it is only recommended if video transmission speed is problematic. It usually has a more marked effect on video streaming than on video downloading.

• **SMS on System Start**: Sends SMS notifications to all SMS recipients whenever the Video Gateway starts running. For information about defining SMS recipients, see SMS and E-mail Notifications, page 61.

• **ADAM Sensors**: Enables the activation of sensors that are connected to the Video Gateway unit through an ADAM module. For additional information, see Configuring Sensor and Activator Settings, page 120.

• **IA Sensors and Activators**: Enables the activation of sensors and activators that are connected to the Video Gateway unit through an IA 3126-2 relay board. For additional information, please refer to your unit’s installation manual.

• **Maximum Recording Length**: Automatically erases recorded video after a specified period of time.

• **Publish System Name**: Sends the name and IP address of the Video Gateway to the ARP system of the local network so that the ARP system can translate the name of the Video Gateway to its IP address. This enables local users to access the Video Gateway using its name.

• **Ignore VGA in RT**: Tells the Video Gateway not to send VGA video streams (of live or recorded video) to client applications; when a client requests a VGA stream, the stream is sent in a lower-resolution, although the VGA image size is retained. Activating this option enhances the stability of the stream when bandwidth is limited, such as when the Video Gateway transmits video streams over a cellular connection. This option does not affect video downloading; video can be downloaded in full VGA resolution even if this option is selected.
• **Real Time Bitrate Control:** Tells the Video Gateway to monitor the video transmission, identify situations in which packets are not being transmitted quickly enough because of bandwidth limitations, and automatically modify the bitrate of the video to suit the available bandwidth. Activating this option enhances the stability and quality of the stream when bandwidth is limited, such as when the Video Gateway transmits video streams over a cellular connection. This option does not affect video downloading; video can be downloaded in full VGA resolution even if this option is selected.

• **Time Stamp on Snapshot:** Imprints a timestamp indicating when the picture was taken before downloading a snapshot to a client.

• **Allow Only Encrypted:** Tells the Video Gateway to encrypt all video data before transmitting it. When this option is selected, clients cannot connect to the Video Gateway unless AES encryption is turned on in the client application.

  **Note:** If clients connect to the Video Gateway through a proxy server, when this option is selected, the video data is transmitted from the Video Gateway to the proxy server in encrypted form. If you want it to be encrypted when it is transmitted from the proxy server to clients, you must select **Encrypt Proxy Communication** in the **Proxy and DDNS Settings** screen. For additional information, see **Proxy and DDNS Settings**, page 57.

  **Note:** For information about AES encryption, see **Modifying the AES Key**, page 193.

• **Event on Ignition:** Generates an Ignition event whenever the vehicle ignition is turned on.

• **Maximum Allowed Streams:** By default, the Video Gateway can transmit up to 20 video streams at one time. This option can be used to further limit the number of simultaneous video streams that can be transmitted. This may be useful, for example, if the local network to which the Video Gateway is connected cannot support so many video streams at one time. If the maximum number of streams has been reached, clients requesting additional streams from the Video Gateway receive an error message saying "Stream not available."
Configuring General System Settings

To adjust the general system settings:

1. In the **Main Menu**, under **System**, click **General**. The **General System Settings** screen opens:

![General System Settings screen](image)

Figure 16: General System Settings screen (MVG)

2. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>Assign a name to the Video Gateway unit (up to 20 Unicode (UTF-8) characters). This name is used to identify the unit in client applications such as SVMultiClient, in SMS and e-mail notifications, in AVV file names, and on the proxy. <strong>Note</strong>: Spaces and underscores in the name may cause problems with various network functions, such as e-mail notifications, proxy, and DDNS. Therefore, it is recommended not to include any spaces or underscores in the name.</td>
</tr>
<tr>
<td>System Port</td>
<td>Fill in the client access port of the Video Gateway unit.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
| **Note:** If you want to access the unit remotely and cannot set up port forwarding for port 10000 in your network, you can also access the configuration utility using this port. |  |
| Video Resolution | Select the video resolution (VGA or D1). VGA is recommended for most applications.  
**Note:** If you change the video resolution, all recorded video is erased from the unit. |  |
| Video Mode | Select the video format (PAL or NTSC) used by the camera.  
**Note:** NTSC is generally used in North America. PAL is standard in most other locations. For additional information, consult the camera documentation.  
**Note:** If you are connecting a CCTV monitor to the Video Gateway, ensure that the monitor supports the video mode selected here. Some SECAM monitors will also work when the PAL video mode is selected.  
**Note:** When D1 video resolution is selected, and you change the video mode, all recorded video is erased from the unit. |  |
| Ignition (MVG and CVG-M only) | Select this option if you want the unit to power down automatically whenever the ignition is turned off. If you do not select this option, the unit operates continuously as long as it has a power supply.  
**Note:** This setting only affects the unit if the unit is connected both directly to the battery and to the ignition. Otherwise, the unit operates continuously as long as it has a power supply. (For additional information, please refer to the unit’s installation guide.) |  |
| Ignition Countdown (MVG and CVG-M only) | Select the amount of time that the unit should continue operating after the vehicle ignition is turned off, in seconds.  
**Note:** This setting only affects the unit if the unit is connected both directly to the battery and to the ignition. Otherwise, the unit operates continuously as long as it has a power supply. (For additional information, please refer to the unit’s installation guide.)  
**Note:** This field only appears if the Ignition checkbox is selected. |  |
| Download Optimizations | Select this option if you want to activate any of the download optimization settings. If this option is selected, while downloading is in progress the Video Gateway will fill new requests from clients for live-video streaming, but it will not fill new requests for playback of recorded video or for downloading of other video.  
When this checkbox is selected, additional fields are added to the screen; these fields allow you to further configure the download-optimization settings, as explained below. For additional information, see Download Optimizations, page 18. |  |
| Stop Recording on Download | Select this option to stop all video recording when video is being downloaded from the Video Gateway.  
**Note:** This field only appears if Download Optimizations is enabled. |  |
| Close All Tasks on Download | Select this option to stop all other actions – accepting new connections from clients, streaming live or recorded video, recording video, and other downloading jobs – when downloading is in progress.  
**Note:** This field only appears if Download Optimizations is enabled. |  |
| Block New Connections while Downloading | Select this option to prevent the streaming of new live or recorded video streams to a client application while downloading of recorded video to a PC is taking place.  
**Note:** This field only appears if Download Optimizations is enabled. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable TV-Out while Downloading</td>
<td>Select this option to stop streaming to the CCTV monitor connected to the Video Gateway while downloading of recorded video to a PC is taking place. <strong>Note:</strong> This field only appears if Download Optimizations is enabled and if TV-Out is enabled (see Configuring a CCTV Monitor (TV-Out), page 25).</td>
</tr>
<tr>
<td>Video Authentication</td>
<td>Select this option if you want the system to include a digital signature in each video frame streamed and/or recorded by the unit. The signature can be used to identify streams that were tampered with. <strong>Note:</strong> This option increases the load on the system resources slightly, so it is advisable to activate it only if it is truly required.</td>
</tr>
<tr>
<td>Outline Switching</td>
<td>Select one of the following types of triggers for activating different outlines:</td>
</tr>
<tr>
<td></td>
<td>- <strong>None:</strong> No automatic outline switching – outlines can only be switched manually using the configuration utility (see Defining Alternate Outlines, page 150)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sensor:</strong> Makes it possible to use Sensor 1 events as triggers for outline switching (see Configuring Sensor and Activator Settings, page 120)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For CVG and CVG-M models, this option should not be selected if the sensor connector (In1) is used to control the display on a connected CCTV monitor. For additional information, please refer to the unit’s installation guide.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Schedule:</strong> Makes it possible to schedule outline switching (see Schedules, page 77)</td>
</tr>
<tr>
<td>Network Speed Optimization</td>
<td>If video from the unit will be viewed primarily or exclusively on PCs that are on the same LAN as the unit, select this option to minimize the streaming delay within the LAN. That is, when this option is selected, live video will be played as close to real time as possible. Clear this option if live video will be viewed remotely via the internet or a modem connection.</td>
</tr>
<tr>
<td>Network TCP Optimization</td>
<td>If video from the unit will be transmitted primarily or exclusively to client devices that are not on the same LAN as the unit, select this option to minimize the streaming delay. That is, when this option is selected, live video will be played as close to real time as possible. Clear this option if live video will be viewed primarily on devices that are on the same LAN as the Video Gateway.</td>
</tr>
<tr>
<td>SMS on System Start</td>
<td>Select this option if you want the unit to send SMS notifications whenever it starts running.</td>
</tr>
<tr>
<td>SBox Sensors (MVG and CVG-M only)</td>
<td>[Not currently in use.</td>
</tr>
<tr>
<td>ADAM Sensors</td>
<td>If sensors are connected to the unit through an ADAM module, select Enabled. This makes it possible to activate and configure the sensors. For additional information, see Configuring Sensor and Activator Settings, page 120.</td>
</tr>
<tr>
<td>IA Activators Used</td>
<td>If activators are connected to the unit through an IA relay board, select the number of activators that are connected to the board. For additional information, please refer to the unit’s installation guide.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
IA Sensors Used | If sensors are connected to the unit through an IA relay board, select the number of sensors that are connected to the board. For additional information, please refer to the unit’s installation guide.

Maximum Recording Length | If you want recorded video to be erased automatically after a specified period of time, select the desired time period. A day is defined by the system as beginning at midnight. For example, if you select “1,” the system saves all video that was recorded from midnight yesterday on. Video that was recorded before midnight yesterday is automatically erased.

**Note:** When video is erased in this way, the storage space it occupied on the unit’s storage media is not made available for additional recordings.

Publish System Name | Select this option if you want the name of the Video Gateway to be recognized on the LAN to which the Video Gateway is connected. When this option is selected, users on the LAN can connect to the Video Gateway using either its name or its local IP address. When this option is not selected, only the IP is recognized in the LAN.

Ignore VGA in RT | Select this option to prevent the Video Gateway from streaming video in VGA resolution. When this option is selected, the Video Gateway sends clients video streams in SIF resolution when they request VGA. This option should be selected when the Video Gateway is streaming video via a low-bandwidth connection such as a cellular connection.

Real-Time Bitrate Control | Select this option to allow the Video Gateway to automatically modulate the bitrate of video streams to suit the available bandwidth of the connection.

Timestamp on Snapshot | Select this option to include a timestamp in all snapshots that are saved from video streams.

Allow Only Encrypted | Select this option to transmit all video to clients in encrypted form, by preventing clients from connecting to the Video Gateway if they are not using AES encryption.

**Note:** The client essentially controls whether the Video Gateway transmits video to it in encrypted form or not; the Video Gateway transmits encrypted video whenever the client requests it.

**Note:** For information about encrypting video that is transmitted to a proxy server, see *Proxy and DDNS Settings*, page 57.

Event on Ignition (MVG and CVG-M only) | Select this option if you want an event to be generated by the system whenever the ignition of the vehicle is turned on.

Maximum Allowed Streams | By default (when **Disabled** is selected), the Video Gateway can transmit up to 20 video streams simultaneously. To further limit the number of simultaneous streams, select the maximum number of simultaneous streams. (You can choose values between 1 and 10.) Reducing the number of simultaneous streams may improve stream stability and quality when the video is transmitted over low-bandwidth networks such as cellular networks.

---

3. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see *Saving Configuration Changes*, page 157).
Configuring a CCTV Monitor (TV-Out)

If a video monitor is connected to your Video Gateway, you must activate and configure it before you can see video on it. The monitor can be used for one of two purposes: to view video from the Video Gateway, or to play prerecorded video content that is stored on the unit, such as movies or ads.

**NOTE:** For information about setting up a CCTV monitor, please refer to your unit’s installation guide.

**NOTE:** TV-Out makes use of the same system resources as the unit’s video recorder. As a result, the global framerate available for recording is reduced somewhat when TV-Out is enabled. For additional information about recorder framerates, see Advanced Recorder Settings, page 107.

To enable a CCTV monitor connected to the Video Gateway unit:

1. In the Main Menu, under System, click TV-Out. The TV-Out Settings screen opens:

![TV-Out Settings screen](image)

*Figure 17: TV-Out Settings screen*

2. Select Enabled. The fields required to configure the monitor display are added to the screen.
Figure 18: TV-Out settings displayed (MVG)

Note: TV-Out cannot be enabled if recording framerates are very high (see Advanced Recorder Settings, page 107). In this case, if you attempt to enable TV-Out, a TV-Out Disabled message will be displayed:

Figure 19: TV-Out Disabled message

3. Configure the monitor as explained in the next sections (Configuring the Monitor to Display Video from the Video Gateway, below, and Configuring the Monitor to Play Prerecorded Video, page 30).

Configuring the Monitor to Display Video from the Video Gateway

A CCTV monitor connected to the Video Gateway unit can be used to display live video from the unit in various ways, as configured in the TV-Out Settings screen. If the monitor has a touch screen, or the supplied mouse is connected to the unit, the display can be changed on the fly and recorded video can be played back.
To configure the CCTV monitor to display video from the Video Gateway:

1. In the **TV-Out Settings** screen, under **Display Mode**, select **Normal**. The fields required to configure the monitor to display video from the Video Gateway are added to the screen:

   ![Figure 20: TV-Out settings for Normal display (MVG)](image)

2. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display type</td>
<td>Select the desired layout for the video display on the monitor:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Split Screen</strong>: Divides the screen so that video from all the cameras is visible all the time</td>
</tr>
<tr>
<td></td>
<td>- <strong>Full Screen – Camera #</strong>: Displays video from the specified camera in full-screen mode</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Display</strong>: Does not display any live video; instead, only a menu is displayed. The display can be controlled from the menu (if the monitor has a touch screen or a mouse is connected to it).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Full Screen – Rotate</strong>: Loops through all of the cameras, displaying each in full-screen mode for the number of seconds specified under <strong>Rotate delay</strong></td>
</tr>
<tr>
<td>Rotate delay</td>
<td>If you selected the <strong>Full Screen – Rotate</strong> display type, specify the number of seconds you want the video from each camera to be displayed before it is replaced with video from the next camera.</td>
</tr>
</tbody>
</table>

   **Note:** This field only appears if the **Full Screen – Rotate** display type is selected.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Display Switch Via Sensor   | Select this option if a switch is connected to the relevant sensor connector on the unit (In6 on the HVG400; In4 on the MVG400, and UVG400; In1 on MVG200, CVG, and CVG-M models), and you want to use the switch to cycle through the various display types.  
**Note:** This option is only fully activated if it is selected here and configured in the appropriate sensor configuration screen (for HVG400, MVG400, or UVG400, the Sensor 4 configuration screen; for MVG200, CVG, or CVG-M, the Sensor configuration screen), as described under Configuring a Sensor to Control CCTV Display, page 127.  
**Note:** On MVG200, CVG and CVG-M models, this option should not be selected if the sensor connector (In1) is used for an outline switch. For additional information, please refer to the unit’s installation guide. |
| Cameras                     | Select the cameras that will be accessible via the monitor. Cameras that are not selected do not appear in the monitor at all. Video from these cameras cannot be viewed on the monitor and the cameras cannot be configured through the monitor.                                                                                                                           |
| Display Camera Name in Live Video | Select this option if you want the name of the camera to be displayed in the camera pane when live video is played on the monitor.  
**Note:** Displaying names on the monitor requires extra system resources and may impede performance.  
**Note:** If the name of a camera contains characters from non-Latin alphabets such as Hebrew or Arabic, or accented characters, those characters are not displayed properly on the monitor. In this case, you can select both this option and Display Camera Number (see below) in order to display the index of the camera (1, 2, 3, or 4) instead of its name. |
| Display Camera Name in Playback | Select this option if you want the name of the camera to be displayed in the camera pane when recorded video is played on the monitor.  
**Note:** Displaying names on the monitor requires extra system resources and may impede performance.  
**Note:** Recorded video can only be played on the monitor if touch or mouse support is enabled (see step 6 below). Otherwise, this option has no effect.  
**Note:** If the name of a camera contains characters from non-Latin alphabets such as Hebrew or Arabic, or accented characters, those characters are not displayed properly on the monitor. In this case, you can select both this option and Display Camera Number (see below) in order to display the index of the camera (1, 2, 3, or 4) instead of its name. |
| Display Timestamp in Playback | Select this option if you want the date and time to be displayed in the camera pane when recorded video is played on the monitor.  
**Note:** Displaying timestamps on the monitor requires extra system resources and may impede performance.  
**Note:** Recorded video can only be played on the monitor if touch or mouse support is enabled (see step 6 below). Otherwise, this option has no effect.  
**Note:** If the name of a camera contains characters from non-Latin alphabets such as Hebrew or Arabic, or accented characters, those characters are not displayed properly on the monitor. In this case, you can select both this option and Display Camera Number (see below) in order to display the index of the camera (1, 2, 3, or 4) instead of its name. |
| Display Camera Number        | If you chose to display the camera name for live and/or recorded video, select this option to display the camera number instead of its name. This is particularly useful if the name contains non-Latin characters that are not displayed properly on the monitor.  
**Note:** This option has no effect if neither Display Camera Name in Live Video nor Display Camera Name in Playback is selected.                                                                                                                                 |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Recording Status</td>
<td>Select this option if you want the recording status to be displayed at the bottom of the screen at all times. The recording status indicates whether recording is taking place as it should be, and, if it is, displays the current recording status of each camera in the system. For additional information, see Recording Status Display, page 236.</td>
</tr>
</tbody>
</table>

3. If you want any other text to be displayed on the monitor, such as your company name or an advertisement, under Display Text, select Enabled. A text field is added to the screen. Enter the text you want to display in the text field. The text will be displayed on the monitor at the bottom of the screen, in the center.

![Text field](image)

*Figure 21: Text field*

4. Under Display Color, select the color in which on-screen text should be displayed. You can choose one of five preset colors or select any color you wish by specifying its RGB hexadecimal code, as follows:
   - To select one of the preset colors: from the dropdown list, select Yellow, Orange, Black, Blue, or Red.
   - To specify a hexadecimal code: from the dropdown list, select Other. The fields required to specify the color are added to the screen. The hexadecimal code field displays the hexadecimal code of the currently selected color. The code consists of three two-digit hexadecimal numbers, for the red, green, and blue components of the color, respectively. The current color is displayed as the background to the Test Color button.

![Hexadecimal code field](image)

*Figure 22: Hexadecimal number field*

Type the desired hexadecimal code into the field. To see what the color looks like, click Test Color.

*Note:* For more information about RGB hexadecimal codes, click the link below the fields.

5. Under Speaker, select one of the following audio playback options (for playback of recorded video):
   - None: Do not play attached audio when recorded video is played.
   - Internal: Play attached audio from the unit’s built-in internal speaker when recorded video is played.
   - External: Play attached audio from the external speaker plugged into Aout when recorded video is played.

*Note:* This option only effects playback of recorded video streams that have audio attached (i.e., a microphone attached to the Video Gateway is linked to the camera recording the video stream).

6. Under Control, select one of the following options:
   - None: Users cannot control the monitor display; video will be displayed in accordance with the selected Display Type (see above). This option should be chosen if the monitor does not have a touchscreen, and a mouse is not connected to the Video Gateway. You can also use it to disable the touch feature of a touchscreen or to disable a connected mouse.
Note: If you select this option, skip to step 9.

- **Mouse**: Enable control of the monitor display using the mouse connected to the Video Gateway.

  **Note**: This option is not available for MVG, CVG, and CVG-M models.

- **Touchscreen type**: If the monitor has a touchscreen, select the type of touchscreen from the list.

  **Note**: Only the types of screens listed are supported. It is recommended to consult SerVision technical support before purchasing a monitor with a touchscreen, to ensure that the protocol used by the monitor is supported. If the touchscreen is not supported, video will be displayed in accordance with the selected **Display Type**, but the touch controls will not work.

If you selected either Mouse or a type of touchscreen, the **Screensaver** field is added to the screen.

7. If you want a screen saver to be turned on when there is no user input (the touchscreen has not been touched or the mouse has not been moved) for a period of time, under **Screensaver**, select **Enabled**. The fields required to define the time period are added to the screen:

   ![Screen Saver Settings](image_url)

   **Figure 23: Screensaver settings**

8. Under **Timeout**, specify the period of time that must pass without user input before the screensaver is activated.

   - Under **Hours**, fill in the number of hours in the timeout period.
   - Under **Minutes**, fill in the number of minutes in the timeout period.

   For example, according to the settings in the figure above, in which **Hours** is “0” and **Minutes** is “10,” the screensaver is turned on whenever there is no user input for ten minutes.

9. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).

### Configuring the Monitor to Play Prerecorded Video

A CCTV monitor connected to the Video Gateway unit can be used to play prerecorded video that is stored on the unit, such as movies or ads. Only video in the Video Gateway's standard format, SMF, can be played. If you want to use a CCTV monitor for this purpose, SerVision can provide you with a video-converter that you can use to convert your video files to the required format. Once the video is converted, you can download the files to the Video Gateway unit’s storage medium.

**NOTE**: For information about converting video files to SMF format and downloading them to the Video Gateway unit, please contact SerVision technical support.

When this feature is enabled, the CCTV monitor automatically plays all the SMF files that are stored on its storage media in the location allocated for this purpose, one after the other, in a continuous loop. You must configure how much of the storage medium is allocated for these files (in GB), as explained below. This is the maximum amount of video data you can place on the storage medium for playing on the CCTV monitor. The amount you allocate will no longer be available for recording video from on-site.

**WARNING**: Since enabling this mode causes the system to reallocate the space on the storage medium, all recorded video stored on the Video Gateway when you enable this option is erased.

This feature requires a large amount of system resources. At times, the resources required may not be available because they are being used for the other functions of the unit may, such as recording video and transmitting video...
streams to clients. When this occurs, playing of video in the CCTV monitor is temporarily suspended. It resumes automatically when the resources are once again available.

**NOTE:** For additional information about this option, please contact SerVision technical support.

**To configure the CCTV monitor to play video from the Video Gateway:**

1. In the **TV-Out Settings** screen, under **Display Mode**, select **Content**. The fields required to configure the monitor to play the prerecorded video are added to the screen:

   **Figure 24: TV-Out settings for Content playback (MVG)**

2. Under **Disk Allocation for Content**, select how many GBs of storage space to allocate to the prerecorded video you want to play back in the CCTV monitor.

3. Click **Update**. A warning message appears, reminding you that this feature may take resources away from other system functions.
Figure 25: Warning message

**NOTE:** When Content mode is enabled, this warning message appears every time you open the TV-Out Settings screen.

4. In the message, click **OK**.

5. Open the Save Settings page. A warning message appears in the page, informing you that all existing recording on the unit will be erased when you save the settings.

Figure 26: Warning message on Save Settings page

6. Select **Save Changes to System**.
7. In the **Save Settings** screen, click **Save Changes to System**. The unit stores the changes permanently, all recorded video on the unit is erased, and the **System Restart Page** screen opens:

8. Click **Restart System**. The unit restarts, and the changes are implemented.

**Setting the Unit Time**

The unit has a built-in battery-backed clock that keeps track of the date and time even when the unit is turned off. It is important to ensure that the time on the unit is accurate whenever the system is running; all video recordings include timestamps that are derived from the unit’s time, and playback relies on these timestamps. An inaccurate clock can lead to misunderstandings when playing recorded video. Moreover, the unit will not record if the time on it is invalid.

The clock can be set by manually synchronizing its time with the time on the PC on which the configuration utility is running. This should be done when the system is first set up.

Like most clocks, the unit's clock has a tendency to drift slightly over time. Therefore, the time should be updated at frequent intervals. The time can be updated manually at any time. The unit can also be configured to update its clock automatically by connecting to an NTP time server at specified intervals. This option only works when the unit has access to one or more NTP time servers, either public ones on the internet or locally-installed ones on the LAN. Public NTP servers can be used free of charge and can be easily accessed when the unit has internet access. MVG and CVG-M units can also be configured to update their clocks from GPS servers.

In addition to the time itself, the general time settings – time zone and daylight savings time (summer time) – should always be configured correctly. The time zone and daylight-savings settings should be set correctly before the clock is set. (After setting the time zone, be sure to click **Update** and restart the unit before manually updating the time.) Daylight savings time can be activated manually or configured for automatic activation. When daylight savings time is activated, the time on the unit clock is set one hour ahead of the time in the selected time zone.

**To set the general time settings:**

1. In the **Main Menu**, under **System**, click **Date & Time**. The **Date & Time Settings** screen opens:

![Date & Time Settings screen (MVG)](image)

**Figure 27: Date & Time Settings screen (MVG)**

**Note:** The current date and time recorded on the clock of the Video Gateway unit appear in the **System Time** field.
2. Under **DST Control Type**, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Lets you activate and deactivate daylight savings time manually. When this option is selected, the <strong>Enabled</strong> checkbox appears below the <strong>DST Control Type</strong> field. Select this checkbox when daylight savings time begins, and clear it when daylight savings time ends.</td>
</tr>
<tr>
<td>Automatic</td>
<td>Lets you define a rule for the automatic activation and deactivation of daylight savings time. For example, you can specify that daylight time should be activated on the last Sunday of March. When this option is selected, the <strong>Start</strong> and <strong>End</strong> lines appear below the <strong>DST Control Type</strong> field. In the <strong>Start</strong> line, specify the start date of daylight savings time; in the <strong>End</strong> line, specify the end date.</td>
</tr>
<tr>
<td>Automatic Floating</td>
<td>Lets you specify the start and end dates of daylight savings time. When this option is selected, four pairs of <strong>Start Date</strong> and <strong>End Date</strong> fields appear below the <strong>DST Control Type</strong> field. Use them to define up to four daylight-savings-time periods (covering the next four years).</td>
</tr>
</tbody>
</table>

**Figure 28: Manual DST settings**

**Figure 29: Automatic DST settings**

**Figure 30: Automatic-Floating DST settings**

**Note:** When daylight savings time is activated or deactivated automatically, the change is implemented at midnight at the beginning of the selected day. For example, if you select Saturday, it is implemented at midnight between Friday and Saturday.

**Note:** When daylight savings time is activated, the time on the unit clock is set one hour ahead of the time in the selected time zone.

3. Under **Time Zone**, select the time zone in which the Video Gateway is located.

4. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see *Saving Configuration Changes*, page 157).
Updating the Date and Time Manually

You should set the unit date and time manually when you first set up the system and when the Video Gateway has not been used for a while. If you cannot or do not want to implement automatic time setting, you should also update the time manually whenever the date and time are no longer accurate.

You can see the current date and time settings of the Video Gateway unit and of the PC in the Date and Time Settings screen: the time on the Video Gateway unit is shown in the System Time field and the time on your computer is shown in the PC Time field. Before you manually set the date and time on the Video Gateway unit, make sure the date and time on the PC are correct and that the time zone and daylight-savings settings are the same on the unit and on the PC.

The system stores time in GMT format. Because of this, it is very important to ensure that the time zone and daylight savings time settings are identical on the PC and the Video Gateway. For example, if the PC is located in New York, the system should be set to use GMT-5:00 (Eastern Time). If daylight savings time is in effect in New York at the time, daylight savings time must be activated on the Video Gateway or the GMT conversion will not be accurate and the time entered on the unit will not be correct.

Because time setting must be performed immediately to be accurate, the unit is automatically updated as soon as the Sync time with PC button is clicked. (The unit should still be reset manually to fully implement the new time setting.) If other configuration changes were made – including daylight savings time and time zone settings – it is best to save the changes before using the sync feature (it is not necessary to restart the system). For additional information about saving configuration changes, see page 157.

Under certain circumstances, resetting the time may make it impossible to view some recorded video, including some video that is recorded after the time is set.

To update the time on the Video Gateway unit manually:

1. Make sure the date, time, and time zone on the PC are correct.
   
   **Note:** The current date and time recorded on the clock of the Video Gateway unit appear in the System Time field.
   
   **Note:** If you have made other changes to the configuration, save them before continuing.

2. In the Date and Time Settings screen, click the Sync time with PC button. The date and time on the Video Gateway unit are set to match the date and time on the PC, a confirmation message appears at the top of the screen, and the System Restart Page is displayed with a confirmation message on the lower left of the screen.
Figure 31: System Restart Page after manual time updating

In two cases, the screen that is displayed may differ from the one in figure 31: if there were unsaved updates when the time was synchronized, and if the clock was set ahead more than about 15 minutes. For information about handling these cases, see page 36.

3. Click Restart System. The unit restarts, and the time on the unit is fully updated. You are automatically logged out of the configuration utility, and a confirmation message appears:

Figure 32: Restart confirmation message

Note: To continue configuring the unit, click the link in the message and log into the configuration utility again.

Note: If you do not reset the unit at this time, the time setting is partially implemented. The next time the unit is reset, the time change is fully implemented.

Under normal circumstances, after you click the Sync time with PC button, the System Restart Page appears as in figure 31. However, if you made changes to other configuration settings before you updated the time, and did not yet save them on the unit (i.e., you clicked Update in one or more of the screens, but did not yet save the changes in the Save Settings page), the System Restart page will include a message: “You have changes that need to be saved. Click here to go to update page.”
To save unsaved changes after the time was synchronized:

1. Click the message. The Save Settings page opens.

2. In the Save Settings page, click Save Changes to System, and then, in the System Restart page, click Restart System.

In addition, if the unit clock was set ahead more than about 15 minutes during synchronization, instead of the System Restart page, a message indicating that your configuration session has expired may appear. This does not mean that the time was not reset correctly. However, you should still restart the unit to fully implement the update, as follows:

To fully implement the time synchronization when the session expired during the process:

1. Log into the configuration utility again.

2. Navigate to the System Restart page and click Restart System.

Note: If you made changes to other configuration settings before you updated the time, and did not yet save them on the unit (i.e., you clicked Update in one or more of the screens, but did not yet save the changes in the Save Settings page), navigate to the Save Settings page, click Save Changes to System, and then, in the System Restart page, click Restart System.

Configuring Automatic Time Setting

The Video Gateway can automatically keep its clock up to date by connecting to an NTP time server at specified intervals. If you are configuring an MVG or a CVG-M, you can choose to use a land-based time server (on the internet or on a local network) or GPS-based time synchronization for this purpose.

NOTE: If the Video Gateway unit is not connected to the internet most or all of the time, does not have GPS support, and cannot connect to an alternative local time server, this feature will not keep the unit time accurate.

The default configuration includes a number of internet time servers to which the Video Gateway can connect in order to check the time. The unit automatically attempts to connect to a time server at regular intervals. Each time it
attempts to connect, it begins with the first server listed. If it fails to connect to that server, it tries the next on the list, and so on. If you wish, you can replace any or all of the time servers on the list with other time servers, or add additional time servers, to a maximum of ten servers. The list can include time servers on the internet and on a local network.

For the MVG and the CVG-M, you can choose to use GPS-based time synchronization if GPS is enabled for the unit (see Configuring GPS, page 89). When you choose this option, the unit clock is constantly updated via GPS.

To enable automatic NTP-based time setting:

1. In the Date & Time Settings screen, if the GPS Time field appears, clear the Enabled checkbox.
   
   Note: The GPS Time field only appears for the MVG and CVG-M, and only if GPS is enabled in the General System Settings screen (see Configuring GPS, page 89).

2. Under Update Frequency, select the interval between time checks, in hours.

3. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

To enable automatic GPS-based time setting on the MVG or CVG-M:

1. In the Date & Time Settings screen, under GPS Time, select the Enabled checkbox.

2. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

To disable all automatic time setting:

1. In the Date & Time Settings screen, if the GPS Time field appears, clear the Enabled checkbox.

2. Under Update Frequency, select Disabled.

3. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

To specify other time servers when NTP-based time-setting is enabled:

1. In the Date & Time Settings screen, under Time Servers, add the IP addresses or hostnames of additional time servers to the list, or replace existing IP addresses or hostnames with those of the time servers you want to use, as required.

   Note: Most time servers use port 123. If a time server you want to use uses a different port, you must specify the port after the IP address or hostname. (Separate the address and the port with a colon (:). For example: 192.168.1.15:345)

2. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

LAN Settings

The LAN settings define how the Video Gateway should connect to a cabled LAN – a local network to which it is physically connected through an Ethernet network cable (connected to the Ethernet Out connector). These settings are only relevant if the unit is connected to an external network via Ethernet cable. (For information about connecting the unit to an external network, please refer to the unit’s installation guide.)

Note: MVG400 and UVG400 units have a built-in router. The LAN settings described here define how the router connects to the external LAN, not how the unit connects to the internal LAN managed by its router. The connection between the unit and the router is handled automatically by the system and does not require any configuration (see Port Forwarding, page 55).
The **LAN Settings** screen is used to select a connection method – static IP or DHCP – for the Video Gateway to use when connecting to a LAN. If a static IP is to be used, you must find out what IP to use, and what the appropriate network settings are for the IP, before you begin: This information can be acquired from your network administrator. If you want to be able to connect to the unit remotely through the LAN connection (to view video and/or to modify the unit’s configuration) it is not generally recommended to use a dynamic IP address.

**NOTE:** If your network has a firewall, make sure that the port used by the unit (configured under **General System Settings**, see **Ports**, page 17), and port 10000, are forwarded from the gateway (router) to your Video Gateway for incoming communication.

**To adjust the LAN settings:**

1. In the **Main Menu**, under **System**, click **LAN**. The **LAN Settings** screen opens:

   ![LAN Settings screen](MVG400)

   **Figure 34: LAN Settings screen (MVG400)**

2. For the MVG400 and UVG400, under **Router**, select **Enable**.

   For the CVG and CVG-M, if the unit is connected to an external *SerVision* router, under **Router**, select **Enable**. **Do not** select this option if the unit is connected to any other type of router.

   **Note:** The **Router** field does not appear for HVG400 models.

3. If you want a dynamic IP address to be assigned to the unit by a DHCP server on the LAN, select the **Enable Dynamic IP (DHCP)** checkbox.

   **Note:** If this field is selected, you may not be able to access the unit remotely because the DHCP-assigned IP may change from time to time.

   **Note:** If this field is selected, the **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Server** fields are not relevant and are hidden.

4. If the unit will have a static IP address, clear the **Enable Dynamic IP (DHCP)** checkbox. The fields required to configure the LAN settings are added to the screen.
Figure 35: Static IP settings

Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Specify the static IP address of the unit on the cabled LAN. The address should conform to the standards of the LAN.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Modify the LAN subnet mask as necessary. The subnet mask should be the one the LAN uses.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Fill in the IP address of the gateway through which the LAN connects to the internet. If you do not know the IP address of the gateway, consult the network administrator or your ISP. <strong>Note:</strong> If this field is not filled in correctly, external network services will not be available through this network. These include accessing the unit remotely (even through proxy and DDNS services), SMS, e-mail notifications, and other services.</td>
</tr>
<tr>
<td>DNS</td>
<td>Fill in the IP address of the DNS server. A DNS server enables you to enter names instead of IP addresses for the proxy and DDNS servers. The DNS server may be operated by your internet provider (home installation) or on your network (some office installations). If you do not know the IP address of the DNS server, consult the network administrator or the ISP. <strong>Note:</strong> If this field is not filled in correctly, you will not be able to specify IP addresses as host names. For example, the address of the SMTP e-mail server will have to be defined as IP numbers. In addition, DDNS will not perform updates if there is no valid DNS address.</td>
</tr>
</tbody>
</table>

5. Click **Update** and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

---

**Modem**

The **Modem** screen is used to configure the way the unit connects to a cellular network. Modem support in models that use SerVision routers (MVG400, MVG200, and UVG) is slightly different from modem support in the CVG-M, which has a built-in modem GSM and therefore does not need a router.

**Note:** If you use a cellular modem to make the Video Gateway accessible remotely, you may have to use a SerVision proxy server to facilitate client connections to the unit. For additional information, see Proxy and DDNS Settings, page 57.
Video Gateway with Router

Modem settings configure the system to use the cellular modem connected to the unit’s USB port. Before you configure the modem, ask your cellular supplier for the correct settings. When the modem is correctly configured, the Video Gateway automatically attempts to establish a connection to the cellular network through it.

When the unit is connected to a cellular network, the Modem status displayed in the System Summary screen, in the network settings, is “Connected,” and the IP address of the Video Gateway on the cellular network is displayed there.

<table>
<thead>
<tr>
<th>SYSTEM SUMMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM STATISTICS</strong></td>
</tr>
<tr>
<td>MEMORY</td>
</tr>
<tr>
<td>DSP</td>
</tr>
<tr>
<td>HD SIZE</td>
</tr>
<tr>
<td>HD MODEL</td>
</tr>
<tr>
<td>CHIPSET</td>
</tr>
<tr>
<td><strong>GENERAL</strong></td>
</tr>
<tr>
<td>SYSTEM NAME</td>
</tr>
<tr>
<td>AUDIO OUT</td>
</tr>
<tr>
<td>VIDEO RESOLUTION</td>
</tr>
<tr>
<td>VIDEO MODE</td>
</tr>
<tr>
<td><strong>PROXY &amp; DNS</strong></td>
</tr>
<tr>
<td>PROXY</td>
</tr>
<tr>
<td>DNS</td>
</tr>
<tr>
<td><strong>DATE &amp; TIME</strong></td>
</tr>
<tr>
<td>MESSAGE TEMPLATE:</td>
</tr>
<tr>
<td>&amp;N, &amp;S ACTIVATED ON &amp;U AT &amp;T</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>TUE, MAR 23 20:01:17 61 44</td>
</tr>
<tr>
<td><strong>NETWORK</strong></td>
</tr>
<tr>
<td>ROUTER IN USE LAN</td>
</tr>
<tr>
<td>WIFI (SSID DEMO)</td>
</tr>
<tr>
<td>MODEM</td>
</tr>
</tbody>
</table>

*Figure 36: System Summary screen showing the Video Gateway connected to a cellular network*

The system can be configured to automatically test the modem connection periodically once it is established. To do this, the unit uses a network feature called LCP to send a test “ping” to the network. If the connection is functioning properly, the network replies with a corresponding “ping” of its own. If the unit receives no response from the network, it assumes the connection is no longer functional, and attempts to reconnect. In most cases, it is recommended that this feature be enabled. This feature is not available on all cellular networks and, as such, it is recommended that you contact your cellular provider for more information as to whether it should be used.

The unit does not have to be restarted before a cellular connection is established. This makes it possible to quickly test the settings. Nevertheless, it is important to save the settings once they are correctly configured. Otherwise, the settings will be erased when the unit is next restarted.
NOTE: Unless you have made other changes to the configuration that require a system restart, it is not necessary to restart the system after the modem settings are saved on MVG and UVG400 units.

To configure the cellular modem connected to the unit:

1. In the Main Menu, under System, click Modem. The Modem Configuration screen opens:

![Modem Configuration screen](image)

**Figure 37: Modem Configuration screen**

2. Under Modem Configuration, select Enabled. The fields required to configure the modem are added to the screen:

![Modem Enabled (GSM settings)](image)

**Figure 38: Modem Enabled (GSM settings)**

3. Under Modem Type, select GSM if it connects to a GSM network, or CDMA if the modem connects to a CDMA network. If you select CDMA, some of the fields are removed from the screen.
4. If you selected **GSM**, fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>If the cellular supplier requires a username, fill in the username.</td>
</tr>
<tr>
<td>Password</td>
<td>If the cellular supplier requires a password, fill in the password.</td>
</tr>
<tr>
<td>APN</td>
<td>Fill in the APN of the cellular network.</td>
</tr>
<tr>
<td>PIN Code</td>
<td>If the SIM card of the modem requires a PIN to establish a connection, select <strong>Use</strong>. The <strong>PIN Code</strong> field is added to the screen. Type the PIN code into the field.</td>
</tr>
<tr>
<td>Dial Number</td>
<td>The phone number that the modem should dial to connect to the internet via the GSM cellular network. This number is normally *99# throughout the world.</td>
</tr>
</tbody>
</table>

5. If you selected **CDMA**, fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>If the cellular supplier requires a username, fill in the username.</td>
</tr>
<tr>
<td>Password</td>
<td>If the cellular supplier requires a password, fill in the password.</td>
</tr>
</tbody>
</table>

6. Fill in the remaining fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCP Echo</td>
<td>Select <strong>Enabled</strong> if you want the system to periodically test the network connection after it is established (see page 41).</td>
</tr>
<tr>
<td>Use CHAP</td>
<td>Select <strong>Enabled</strong> if the cellular supplier uses CHAP authentication.</td>
</tr>
</tbody>
</table>
Configuring System Settings

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Router RST on No Comm | If the connection to the cellular network is frequently lost, and selecting the **Verify** option (see step 8 below) does not solve the problem, select this option. The system will automatically check the router status from time to time, and if the router is not connected to the network, it will restart the router.  

**Note:** The unit continues to function while the router is restarted, so video recording and Event detection are not interrupted.  

**Note:** If you select this option, do not also select the **Verify** option.  

**Note:** If you do not see this option in the **Modem Configuration** screen, you may need to upgrade the router software. For additional information, please contact SerVision technical support. |

7. Clear the **Debug Mode** checkbox unless you are instructed by SerVision technical support staff to select it.

8. If the connection to the cellular network is frequently lost or the quality of the connection is often low, select **Verify** to configure the unit to test the cellular network connection periodically. The fields required to configure this option are added to the screen.  

**Note:** If Router RST on No Comm is selected, do not select this option.

**Figure 40: Verification settings**

Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verification Server | Specify the IP address or hostname of the server that the unit should ping in order to test the connection. This can be any device on the network whose connection you want to test. For example, if you want to ensure that the unit is connected to the internet, enter the URL of a server that can only be accessed via the internet, such as [www.google.com](http://www.google.com).  

If the verification server does not respond to the ping, the unit attempts to reconnect to the cellular network. It continues to try to connect periodically, at the interval specified, until it succeeds.  

**Note:** For additional information about the ping command, see **Ping**, page 174. |
| Interval | Fill in the frequency of the verification tests, in seconds. |

9. Click **Update**. The settings are immediately implemented on the unit. If a modem is connected to the unit, and the configuration settings are correct, the unit attempts to connect to the cellular network through the modem.

10. Save the settings to implement them permanently (see **Saving Configuration Changes**, page 157). It is not necessary to restart the system.
CVG-M

The CVG-M has a built-in cellular GSM modem. The modem settings configure the CVG-M to connect to a cellular network; the settings are implemented if a SIM card is installed in the unit. Before you configure the modem, ask your cellular supplier for the correct settings for the SIM card you are planning to use.

**NOTE:** If the SIM card requires a PIN, configure the modem settings as described below before you insert the SIM card into the unit. Otherwise, the unit may attempt to use the SIM card to connect to the network with an incorrect PIN. Attempts to use the SIM with an invalid PIN may cause the SIM card to be locked.

After you configure the modem settings, you must save them and restart the unit. From this point on, the unit automatically attempts to establish a connection to a cellular network whenever it is not connected to a cable-based network.

**NOTE:** For additional information about acquiring and setting up the hardware required for a cellular connection, please refer to the unit’s installation guide.

To configure the cellular modem:

1. In the **Main Menu**, under **System**, click **Modem**. The **Modem Configuration** screen opens:

   ![Figure 41: Modem Configuration screen](image)

   Figure 41: Modem Configuration screen

2. Select **Enabled**. The fields required to configure the modem are added to the screen.
3. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>If the cellular supplier requires a username, fill in the username.</td>
</tr>
<tr>
<td>Password</td>
<td>If the cellular supplier requires a password, fill in the password.</td>
</tr>
<tr>
<td>APN</td>
<td>Fill in the APN of the cellular network.</td>
</tr>
<tr>
<td>PIN Code</td>
<td>If the SIM card of the modem requires a PIN to establish a connection, select <strong>Use</strong>. The <strong>PIN Code</strong> field is added to the screen. Type the PIN code into the field.</td>
</tr>
<tr>
<td>Dial Number</td>
<td>The phone number that the modem should dial to connect to the internet via the GSM cellular network. This number is normally *<strong>99#</strong> throughout the world.</td>
</tr>
<tr>
<td>Use CHAP</td>
<td>Select <strong>Enabled</strong> if the cellular supplier uses CHAP authentication.</td>
</tr>
<tr>
<td>Sense Proxy</td>
<td>In some cases, when a client connects to a CVG-M via a proxy server, the client can connect to the unit, but it cannot open a video stream from the unit. If this occurs frequently, it may mean the Video Gateway needs to free resources for video streaming periodically. In this case, select this option. The unit will automatically check if it needs to free resources, and, when it does, it will free them to make them available for video streaming.</td>
</tr>
</tbody>
</table>

4. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157). At that time, if the unit is not connected to a cable-based LAN, it will attempt to connect to the cellular network.
WiFi

WiFi settings can configure the system to connect to external access points (hotspots) or to function as an access point for external devices.

**NOTE:** When the unit is configured to function as an access point, it cannot also connect via WiFi to other, external access points.

**Configuring the Unit to Connect to WiFi Access Points**

You can specify up to ten WiFi access points to which you want the router to be able to connect. When WiFi is enabled (and the unit is not configured to function as an access point; see Configuring the Unit to Function as an Access Point, page 53), the router automatically establishes a connection to one of the specified wireless networks if it is within range. If the access point is connected to the internet, the Video Gateway can use this connection to connect to the internet in order to send and receive data.

When the unit is connected to a WiFi network, the WiFi status displayed in the System Summary screen, in the network settings, is “Connected,” and the Video Gateway’s IP in the wireless network is displayed.
In order to connect to an access point, you must supply its service set identifier (SSID), which is essentially the name of the wireless network.

In addition, many access points employ an encryption key to prevent unauthorized connections. If the access point you specify requires an encryption key, you must specify the encryption method (WEP or WPA) and supply the key if you want the unit to connect to the access point.

NOTE: Only WEP and WPA encryption methods are supported. The unit cannot connect to WiFi networks that use other encryption methods.

The unit can save the SSIDs and settings of up to ten access points. If you specify more than one SSID, you can prioritize them to indicate which ones you want the unit to connect to when more than one is in range.

You can configure access points even if no wireless card is connected to the unit, or when the access points are not within range of the unit. When a wireless card is installed, you can use it to help you add access points that are in range. The wireless card detects all of the access points that are within range of its current location and automatically supplies the SSIDs of those access points.

By default, the unit is assigned a dynamic IP address in the wireless network when it connects to the access point. If the unit will only need to use the wireless network for outgoing connections to the internet, this is enough. If you need incoming access to the unit – that is, if you want to be able to access the Video Gateway remotely – you should assign it a static IP address.

After the wireless settings are configured, the unit does not have to be restarted before a wireless connection is established. This makes it possible to quickly test the settings. Nevertheless, it is important to save the settings once they are correctly configured. Otherwise, the settings will be erased when the unit is next restarted.
NOTE: Unless you have made other changes to the configuration that require a system restart, it is not necessary to restart the system after these WiFi settings are saved.

To configure the unit to connect to an access point:

1. In the Main Menu, under System, click WiFi. The WiFi Configuration screen opens. (This may take a minute or two.)

2. Under Turn WiFi Off, clear the Enabled checkbox.

3. If you will be configuring more than one SSID, under Random Selection of SSID, do one of the following:
   - Select Enabled if you want the unit to remain connected to the current access point as long as it can, even if an access point with a higher priority level becomes available.
   - Clear Enabled if you want the unit to disconnect from lower-priority access points when higher-priority access points become available.

4. Under Configured SSIDs, fill in the required information for each access point to which you want the unit to be able to connect, as described in steps 5–9 below.

5. Under SSID, fill in the SSID of the access point.

   Note: If a wireless card is connected to the unit, access points that are detected within range of the unit are listed under SSIDs in Range at the bottom of the screen. Click Add SSID to add a detected SSID to the list of configured SSIDs. (If a detected access point is in the list of configured SSIDs, it does not appear in the list of detected access points.)
6. If the access point requires an encryption key, specify the following:
   - Under **Security**, select the encryption method used by the access point (WEP or WPA).
   - Under **Key**, fill in the encryption key.

7. If you want to assign a static IP to the unit, clear the **DHCP Enabled** checkbox. The fields required to configure the static IP are added to the screen.

**Figure 46: Static IP settings**

Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Specify the static IP address of the unit in the wireless network. The address should conform to the standards used in the wireless network.</td>
</tr>
<tr>
<td>Mask</td>
<td>Fill in the subnet mask used in the wireless network.</td>
</tr>
</tbody>
</table>
| Gateway | Fill in the IP address (on the wireless network) of the gateway used for WAN or internet access.  
If you do not know the internal IP address of the gateway, consult the network administrator.  
**Note:** If this field is not filled in correctly, external network services will not be available through this network. These include accessing the unit remotely (even through proxy and DDNS services), SMS and e-mail notifications, and other network services. |
### Configuring System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Fill in the IP address of the DNS server used by the access point. A DNS server enables you to enter names instead of IP addresses for the proxy and DDNS servers. If you do not know the IP address of the DNS server, consult the network administrator. <strong>Note:</strong> If this field is not filled in correctly, you will not be able to specify IP addresses as host names. For example, the address of the SMTP e-mail server will have to be defined as IP numbers. In addition, DDNS will not perform updates if there is no valid DNS address.</td>
</tr>
</tbody>
</table>

8. If you want the unit to test the connection to this access point periodically, select **Verify**. The fields required to configure this option are added to the screen.

![Verification settings](image)

**Figure 47: Verification settings**

Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Server</td>
<td>Specify the IP address of the server that the unit should ping in order to test the connection. This can be any device on the network whose connection you want to test. For example, if you want to check that the unit is connected to the WiFi network, enter the IP of a PC or other device that is normally connected to the WiFi network. Alternatively, if you want to ensure that the unit is connected to the internet, enter the URL of a server that can only be accessed via the internet, such as the google server (173.194.113.179). If the verification server does not respond to the ping, the unit automatically attempts to reconnect to the access point and, failing that, to other configured access points. <strong>Note:</strong> Enter the server address as an IP number, not as a hostname. <strong>Note:</strong> For additional information about the ping command, see <strong>Ping</strong>, page 174.</td>
</tr>
<tr>
<td>Interval</td>
<td>Fill in the frequency of the verification tests, in seconds.</td>
</tr>
</tbody>
</table>

9. If you would like to change the priority level of the access point, click **Move Up** or **Move Down** as required.

10. Click **Update**. If a WiFi card is connected to the unit, the unit attempts to connect to the configured access points. It connects to the first access point it can. “Connected” appears beside or below the SSID of the access point to which the unit is connected.
Figure 48: Video Gateway connected to "SV-WIFI" access point

If Random Selection of SSID is enabled, the unit remains connected to that access point until the connection is lost. If Random Selection of SSID is cleared, it disconnects from the access point if it can connect to a higher-priority access point.

Note: In some cases, “Connected” may appear even if the Video Gateway has not successfully connected to the network. This usually occurs when the signal is relatively weak, the WiFi antenna is not connected securely to the unit, or the encryption key is incorrect. In these cases, the System Summary screen will list WiFi as “Unavailable.” If the Video Gateway has an IP address in the System Summary screen (as in figure 43 on page 48), you can be sure that it is properly connected to the access point. Complete and accurate information about the Video Gateway's network connections can also be seen in SVMultiClient, in the Statistics window. For additional information, please refer to the SVMultiClient User Guide.

Note: If you install a WiFi card when the unit is running, you must restart the unit to access wireless networks.

11. Save the settings to store them permanently (see Saving Configuration Changes, page 157). It is not necessary to restart the system.

Removing an Access Point from the List

If you do not want the Video Gateway to try to connect to an access point that is in the Configured SSIDs list, you can remove it from the list.

To remove an access point from the list of Configured SSIDs:

1. In the WiFi Configuration screen, in the Configured SSIDs list, delete the SSID of the access point.

2. Click Update, and then save the settings (see Saving Configuration Changes, page 157). It is not necessary to restart the system.

Turning WiFi Off

You can disable all WiFi services without removing the WiFi card from the USB connector or deleting any SSIDs from the Configured SSIDs list. If the Video Gateway is configured to function as an access point (see Configuring the Unit to Function as an Access Point, page 53), this functionality is also suspended when you disable the WiFi services.
**NOTE:** When WiFi is turned off, all SSIDs in the Configured SSIDs list have the status "Not in Range," and the list of access points that are within range does not appear. In the System Summary screen, and in the statistics window of the SVMultiClient, the WiFi network status appears as "Connected, Disabled."

To turn all WiFi services off:

1. In the WiFi Configuration screen, under Turn WiFi Off, select Enabled.
2. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

Configuring the Unit to Function as an Access Point

MVG and UVG400 units can be used as WiFi access points for other devices. This means that other WiFi-enabled devices, such as PCs and smartphones, can connect wirelessly to the local network managed by the units' routers, and, if the units are connected to the internet, these devices can connect to the internet through the local networks. For example, if an MVG is installed in a vehicle and connected to the internet through a cellular network connection, passengers in the vehicle could connect other devices to the MVG's network via WiFi and use the MVG's internet connection to connect to the internet.

In order for a VG unit to function as an access point, you must assign an SSID to it and set its security settings. Devices can connect to the access point in the same way that they would connect to any access point, using its SSID and encryption key.

When the unit is configured to function as an access point, it cannot also connect via WiFi to other, external access points. In this case, all the SSIDs in the list of Configured SSIDs appear as "Not in Range." In the System Summary page, "WiFi" appears as disconnected. In the Statistics window of SVMultiClient, WiFi (WLAN) appears as disconnected, and "AP," followed by the SSID of the Video Gateway, appear below it.

![Figure 49: Statistics window in SVMultiClient showing WLAN as disconnected with AP below it when the Video Gateway is functioning as an access point](image)

To configure an MVG unit to function as an access point:

1. In the WiFi Configuration screen, under Enable WiFi as Access Point, select Enabled. The fields required to configure the access point are added to the screen.
2. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP SSID</td>
<td>Enter the SSID of the unit's WiFi network (i.e., the name of the access point; see page 48)</td>
</tr>
<tr>
<td>AP Authentication Type</td>
<td>Select the type of encryption to use (WEP, WPA, WPA2).</td>
</tr>
<tr>
<td>AP Key</td>
<td>Enter the encryption key to use (i.e., the key the user must use to connect to the WiFi network).</td>
</tr>
</tbody>
</table>

3. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

Network Priorities

If your system is configured to connect to more than one network at a time, it can use any of the available networks for outgoing connections such as connecting to a proxy server or sending an e-mail notification. In this case, you should rank the available networks to indicate which one you would prefer the system to use for outgoing communications. For example, if the unit can connect to both a WiFi network and a cellular network, you would probably want to give the WiFi network priority over the cellular network, because it is faster and cheaper to use. In this case, the system would use the WiFi network whenever it was available; if it was not available, the system would use the cellular network instead.

The unit does not have to be restarted before changes to the network priorities settings are implemented. Nevertheless, it is important to save the settings once they are correctly configured. Otherwise, the settings will be erased when the unit is next restarted.

**NOTE:** You can manually override the selected network priorities for specific types of outgoing communications. When this is possible, the Use field appears in the relevant configuration screen. This field allows you to select a specific network to use for proxy connections, DDNS connections, sending e-mail notifications, and sending SMS notifications. For additional information, please refer to the relevant section of this guide.

**NOTE:** Unless you have made other changes to the configuration that require a system restart, it is not necessary to restart the system after the network priorities settings are saved.
To prioritize the network connections:

1. In the Main Menu, under System, click Network Priorities. The Network Priorities screen opens, and displays the three networks – LAN, WLAN (WiFi), and Cell (Modem) – in their current order of priority (the top network is ranked highest).

![Network Priorities screen]

2. To change the position of a network in the ranking, select the network type and then click Up or Down.

![Moving a network up in the ranking]

3. Click Update. The settings are immediately implemented on the unit.

4. Save the settings to implement them permanently (see Saving Configuration Changes, page 157). It is not necessary to restart the system.

---

Port Forwarding

Port forwarding makes it possible for remote devices to access devices within the unit’s local network. Each device that you want to make accessible to incoming connections is linked with a particular port of the router. To connect to the device remotely, you use the external IP address of the router (the IP address of the Video Gateway on the external network), and the assigned port number.
NOTE: Be sure to assign a static internal IP to the device before you set up port forwarding to it (see Appendix C: Networks Managed by SerVision Routers, page 239).

To configure port forwarding for a device connected to the unit’s router:

1. In the **Main Menu**, under **System**, click **Port Forwarding**. The **Port Forwarding** screen opens and displays a list of the ports that are already open for remote access and the internal IPs of the devices to which they provide access.
   
   **Note:** The system and configuration ports of the unit in the router’s network (see *Ports*, page 17) are defined automatically by the router and cannot be modified.

2. In the next available row in the table, fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The number of the port to assign to the device. You can choose any number in the range 1–65535 that is not already in use.</td>
</tr>
<tr>
<td>IP</td>
<td>The internal IP of the device</td>
</tr>
</tbody>
</table>

3. Click **Update** and then save the settings. They will be implemented after the unit is restarted (see *Saving Configuration Changes*, page 157).
Proxy and DDNS Settings

Proxy services make it possible for clients to connect to Video Gateway units that cannot be accessed directly. Dynamic DNS (DDNS) enables clients to connect to Video Gateway units that do not have fixed public IP addresses.

A proxy server is used to enable client applications to connect to Video Gateway units like the Video Gateway when the connection cannot be directly initiated by the client. Typically, this occurs when the Video Gateway connects to the internet through the cellular network. It may also occur if the Video Gateway connects to the internet through a cable-based connection that does not have a public IP address. The proxy server functions as an intermediary that relays requests and data between the Video Gateway and clients. When you enable the proxy service on a Video Gateway, the Video Gateway initiates a connection with the proxy server and registers with it each time it connects to a network. Clients can then connect to the Video Gateway indirectly by connecting to the proxy server. For additional information about proxy services in general and about proxy servers that are available for use please contact your vendor.

DDNS is designed to facilitate internet connections to systems that use dynamic public IP addresses (see Appendix B: LAN Settings, page 238). When you enable a DDNS on a Video Gateway, the Video Gateway is assigned a name. The Video Gateway registers with the DDNS service each time it connects to the internet, and relays its current public IP address to the service. Client applications connect to the Video Gateway by using its name rather than its public IP address. The DDNS service ensures that the correct public IP address is linked to the name at all times, even when the IP changes.

Three DDNS services are supported by the system: SV-DDNS (SerVision’s DDNS service), No-IP, and DynDNS. For information about the SV-DDNS service, consult your vendor. For information about the No-IP and DynDNS DDNS services, consult their websites (www.no-ip.com and www.dyndns.com).

To modify the Proxy and DDNS settings:

1. In the Main Menu, under System, click Proxy & DDNS. The Proxy and DDNS Settings screen opens:

   ![Proxy and DDNS Settings screen]

2. If you are using a proxy for remote access, under Proxy, select Enabled. The fields required to configure the proxy settings are added to the screen.
Figure 56: Proxy settings

Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use</strong></td>
<td><strong>MVG and UVG400:</strong> Select the network connection to use to connect to the proxy server:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any:</strong> The unit can use any available network connection; it will connect using the highest priority connection available (as defined under Network Priorities; see Network Priorities, page 54).</td>
</tr>
<tr>
<td></td>
<td>- <strong>LAN:</strong> The unit will only use a LAN connection. If none is available, the unit will not connect to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>WiFi:</strong> The unit will only use a WiFi connection. If none is available, the unit will not connect to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Modem:</strong> The unit will only use a Modem connection. If none is available, the unit will not connect to the proxy server.</td>
</tr>
<tr>
<td><strong>HVG400, CVG, CVG-M:</strong></td>
<td>Not currently in use.</td>
</tr>
<tr>
<td><strong>Host/IP</strong></td>
<td>Fill in the IP address or hostname of the proxy server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Fill in the access port of the proxy server. (This port number is defined in the configuration settings of the proxy server.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If Allow Only Encrypted is selected in the General screen, all video is encrypted before it is transmitted to the proxy server. In this case, the port number entered here should be the port for encrypted data. (This port number is defined in the configuration settings of the proxy server.) Note that the proxy server decrypts the encrypted video when it receives it. If you want encrypted video to be sent by the proxy server to clients, you must select the next option, Encrypt Proxy Communication.</td>
</tr>
<tr>
<td><strong>Encrypt Proxy</strong></td>
<td><strong>Communication:</strong> Select this option if you want the Video Gateway to encrypt all video it transmits to proxy servers.</td>
</tr>
</tbody>
</table>

3. If you are using a DDNS service, under DDNS, select Enabled. The fields required to configure the DDNS settings are added to the screen.
Figure 57: DDNS settings
Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Use** | MVG and UVG400: Select the network connection to use to connect to the DDNS server:  
- **Any**: The unit can use any available network connection; it will connect using the highest priority connection available (as defined under Network Priorities; see Network Priorities, page 54).  
- **LAN**: The unit will only use a LAN connection. If none is available, the unit will not connect to the DDNS server.  
- **WiFi**: The unit will only use a WiFi connection. If none is available, the unit will not connect to the DDNS server.  
- **Modem**: The unit will only use a Modem connection. If none is available, the unit will not connect to the DDNS server.  

**HVG400, CVG, CVG-M:**  
Not currently in use. |
| **Type** | Select the type of DDNS service.  
**Note**: If you select No-IP or DynDNS, the Username, Password, and Confirm Password fields are added to the screen, and the Advanced field is removed from the screen. |
| **Hostname** | Fill in the hostname of the DDNS server.  
If you are using either No-IP or DynDNS, these values should have been supplied to you when you set up your account.  
If you are using the SerVision SV-DDNS service, the default hostname is the Video Gateway’s default system name. This name is used when Use system name as hostname is selected. You can modify this name as you wish. To do so, clear the Use system name as hostname checkbox. A text field is added to the screen. Fill in the name you want to use. The name you choose should not include any spaces or underscores. In addition, you should make sure the name is unique. For example, you can include your name or the name of your company in the hostname to ensure it is unique. The complete hostname on the SerVision SV-DDNS server will be composed of the name you type plus .TVG.CC. For example, if you type “JaneSmytheOffice,” the hostname on the server is JaneSmytheOffice.TVG.CC.  
**Note**: Once DDNS is set up, changes to the server name will have no effect on the DDNS settings. |
4. If you are using either the No-IP or the DynDNS DDNS service, fill in the **Username** and **Password** fields. The username and password should have been supplied to you by No-IP or DynDNS when you set up your account there. Under **Confirm Password**, type the password a second time to ensure you typed it correctly.

**Note:** SerVision cannot provide support for problems related to the No-IP or DynDNS DDNS services. For technical support, please contact the service providers.

5. If you are using the SV-DDNS service and you want to change the address of the DDNS server, select **Advanced**. The fields required to specify the server are added to the screen.

![Advanced SV-DDNS settings](image)

Figure 58: Advanced SV-DDNS settings

Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDNS Server</td>
<td>Fill in the IP address or hostname of the SV-DDNS server.</td>
</tr>
<tr>
<td>DDNS Port</td>
<td>Fill in the access port of the SV-DDNS server.</td>
</tr>
</tbody>
</table>

6. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).

### Authentication

Access to the system is controlled by username-password authentication. You can create up to ten users. For each user, you can define a specific combination of system permissions. Users can be assigned any or all of the following permissions:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Video</td>
<td>The user can connect to the unit through a client application and view live video.</td>
</tr>
<tr>
<td>Recorded Video</td>
<td>The user can connect to the unit through a client application and view recorded video.</td>
</tr>
<tr>
<td>Camera Control</td>
<td>The user can connect to the unit through a client application and control cameras using their PTZ controllers. <strong>Note:</strong> The Live Video permission must also be selected in order for the user to make use of this feature.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The user has full access to the unit’s configuration utility and can modify the configuration settings.</td>
</tr>
</tbody>
</table>

By default, two users are defined:

- A user with permissions for all of the system’s features. The default username for this user is **svuser** and the password is **servconf**.
• A user with all client permissions – live video, recorded video, and camera control – but no configuration permission. The default username for this user is **anonymous** and the password is **guest**.

You can modify the default settings and add new users as necessary. It is recommended that you change the default usernames and passwords of both of the default users.

**NOTE:** Multiple users can log into the system simultaneously using the same username and password.

**To modify usernames and passwords:**

1. In the **Main Menu**, under **System**, click **Authentication**. The **Authentication** screen opens. Each row in the screen defines the settings for one user.

   ![Authentication Screen](image)

   **Figure 59: Authentication screen**

2. In each row, define or modify the settings of one user, as necessary:
   - Under **Username**, specify the username of the user.
   - Under **Password**, specify the password for the username.
   - Under **Confirm Password**, specify the password a second time to ensure you entered it correctly.
   - Under **Permissions**, select the permissions you want the user to have.

3. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).

**SMS and E-mail Notifications**

You can choose to send an SMS or an e-mail to a predefined list of people whenever events of specified types are detected.
If you opt to write-protect recorded video (see **Advanced Recorder Settings**, page 107), you can also choose to send an e-mail warning message when the disk space allocated to a recorder is almost full or is entirely full.

In order to use the SMS functionality, you must set up an account with Clickatell (http://www.clickatell.com). In order to send e-mails, you must have a valid SMTP e-mail account that can be used as the “sender” of the e-mail messages.

**NOTE:** Web-based e-mail does not always support SMTP settings.

E-mail notifications and warnings contain standard messages that include the name of the unit and information about the event or situation that caused the message to be sent. Depending on the notification settings of each device, e-mail notifications of events may sometimes include snapshots of the first frame of the event. If full-sized VGA or D1 recording is activated (see **Advanced Recorder Settings**, page 107), you can choose whether images sent with e-mail notifications are sent as standard-sized images (SIF or CIF), or large images (VGA or D1). If AVV is activated (see **Automatically Uploading Video to an AVV Server**, page 67), an image and a link to the uploaded video are always included.

You can specify the text of SMS messages that are sent by defining a *message template*. The template can contain any text you wish. It can also contain variables that will be replaced by the system with relevant values in the actual message. For example, the message can include the name of the recipient, the time, and the name of the device that triggered the event. For additional information, see **SMS Message Templates**, page 66.

Once you have configured the notification settings, you can test them by sending a sample notification. For additional information, see **Testing Notification Settings**, page 67.

This section explains how to configure the settings that make it possible for the system to send notifications. Messages are only sent if the device triggering an event – a camera, sensor, or activator – is configured to send notifications of events or warnings about disk usage. For information on configuring a device to send notifications, see the sections about configuring that type of device:

- **Video Motion Detection (VMD)**, page 97
- **Configuring Video Lost**, page 103
- **Advanced Recorder Settings**, page 107
- **Configuring Sensor and Activator Settings**, page 120
To configure SMS and e-mail notification settings:

1. In the **Main Menu**, under **System**, click **SMS & E-mail**. The **SMS and E-mail** screen opens:

   ![SMS and E-mail screen](image)

   **Figure 62: SMS and E-mail screen**

2. Under **SMS Message Template**, modify the text of the message that should be sent to the SMS recipients on the list, as necessary. The message can contain up to 45 characters, including spaces. It should not include quotation marks of any kind ("", '`, or ``).

   **Note:** The message text can contain variables that are replaced by the system with relevant values in the actual message. For example, the message can include the name of the device that triggered the event. For additional information, see **SMS Message Templates**, page 66.

   The default message includes the recipient’s name, the name of the Video Gateway unit, the name of the device that triggered the event, and the time at which the event was triggered. If the message has been changed from its default version, and you want to replace the current message text with the default text, click **Restore Default Template**.

3. For each recipient of an SMS or e-mail message, under **Recipients**, click **Add**. A row is added to the list of recipients.

   ![New recipient row](image)

   **Figure 63: New recipient row**

   Fill in the fields as follows:
# Configuring System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the person who will receive an SMS or e-mail message when an event occurs (up to 20 characters).</td>
</tr>
</tbody>
</table>
| E-mail / Phone number | Fill in the phone number or e-mail address of the recipient.  
| **SMS:** | Enter the phone number in the international format, with no spaces. The number is made up of the country code, the area code and the phone number.  
| Example: | For the US phone number 212-555-1212, enter +12125551212. |
| **E-mail:** | Enter the e-mail address.  
| Example: | johns@demoserv.net |

**Note:** To send both an SMS and an e-mail to the same person, list the person twice in the list of recipients; fill in the SMS phone number in one of the listings, and the e-mail address in the other listing.

![Figure 64: Recipients list](image)

4. Under **Image Size**, select the size of the JPEG image that will be attached to e-mail notifications that contain images. If the unit is configured to use VGA video resolution, you can choose either full-size VGA or the smaller SIF. If the unit uses D1 video resolution, you can choose either full-size D1 or smaller CIF. For additional information about video resolutions, see Video Resolution, page 18.

![Figure 65: Image Size field](image)

5. If you want to send SMS notifications, under **SMS Connection Information**, fill in the fields as follows:
### Field | Description
--- | ---
Use | **MVG and UVG400:**
Select the network connection to use to connect to the SMS server:
- **Any:** The unit can use any available network connection; it will connect using the highest priority connection available (as defined under Network Priorities; see Network Priorities, page 54).
- **LAN:** The unit will only use a LAN connection. If none is available, the unit will not connect to the SMS server.
- **WiFi:** The unit will only use a WiFi connection. If none is available, the unit will not connect to the SMS server.
- **Modem:** The unit will only use a Modem connection. If none is available, the unit will not connect to the SMS server.

**HVG400, CVG, CVG-M:**
Not currently in use.

Username | Fill in the username of your Clickatell account.
Password | Fill in the password of your Clickatell account.
API | Fill in the API ID of your Clickatell account.
Sender ID | Fill in the Sender ID that was assigned by Clickatell.

**Note:** If you do not have an active Clickatell account, open one at [http://www.clickatell.com](http://www.clickatell.com).

**Note:** SerVision cannot provide support for problems related to the Clickatell service. For technical support, please contact Clickatell.

6. If you want to send e-mail notifications, under **E-mail Connection Information**, fill in the fields as follows:

### Field | Description
--- | ---
Use | **MVG and UVG400:**
Select the network connection to use to connect to the e-mail server:
- **Any:** The unit can use any available network connection; it will connect using the highest priority connection available (as defined under Network Priorities; see Network Priorities, page 54).
- **LAN:** The unit will only use a LAN connection. If none is available, the unit will not connect to the e-mail server.
- **WiFi:** The unit will only use a WiFi connection. If none is available, the unit will not connect to the e-mail server.
- **Modem:** The unit will only use a Modem connection. If none is available, the unit will not connect to the e-mail server.

**HVG400, CVG, CVG-M:**
Not currently in use.

SMTP Server | Fill in the SMTP server of your e-mail account as they appear in your e-mail software configuration.
SMTP Port | Enter the SMTP port number used to send e-mail messages.
Domain Name | Enter the domain name to insert in the *sender* address of the e-mail message. For example, if you want the sender address to be alert@test.com, enter test.com.
### Field | Description
---|---
User Name | Enter the user name to insert in the *sender* address of the e-mail message. For example, if you want the sender address to be [alert@test.com](mailto:alert@test.com), enter **alert**.

SMTP Authentication | If the SMTP server requires authentication, select **Enabled**. The **Username** and **Password** fields are added to the screen.

Username | Fill in the username of your e-mail account as it appears in your e-mail software configuration.

**Note:** This field only appears if SMTP Authentication is enabled.

Password | Fill in the password of your e-mail account as it appears in your e-mail software configuration.

**Note:** This field only appears if SMTP Authentication is enabled.

---

#### E-MAIL CONNECTION INFORMATION

| Use |  
| --- | --- |
| **SMTP SERVER** | smtp.googlemail.com |
| **SMTP PORT** | 25 |
| **DOMAIN NAME** | servision.net |
| **USER NAME** | alert |

**Note:** This field only appears if SMTP Authentication is enabled.

---

**Figure 66: E-mail settings**

**Note:** Internet mail accounts (e.g., Yahoo or MSN) are not supported. A list of free SMTP servers can be found at [http://www.e-easy.com/SMTPServerList.aspx](http://www.e-easy.com/SMTPServerList.aspx).

7. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see *Saving Configuration Changes*, page 157).

### SMS Message Templates

The following codes can be included in SMS message templates:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;S</td>
<td>The name of the sensor or VMD that triggered the event</td>
<td>Front Door</td>
</tr>
<tr>
<td>&amp;U</td>
<td>The name of the Video Gateway unit</td>
<td>Bus-5478</td>
</tr>
<tr>
<td>&amp;T</td>
<td>The time of the event</td>
<td>22 Feb 07 00:17:16</td>
</tr>
</tbody>
</table>

The default message template is:

**&S activated on &U at &T**

If the *Front Door* sensor is triggered, John will receive the following SMS message from the Video Gateway:
Sensor (Front Door) ON activated on Bus-5478 at 22 Feb 07 00:17:16

The recipient name is set in each message to match the name of the recipient as it appears in the **Recipient** list below the message template.

You can modify the default message to suit your requirements. For example, you could enter the following message:

**An event was detected: &S at &T**

In this case, when the *Front Door* sensor is triggered, all the SMS recipients in the list will receive the following message from the Video Gateway:

**An event was detected: Sensor (Front Door) ON at 22 Feb 07 00:17:16**

### Testing Notification Settings

Once the event notification settings are configured, and the settings have been implemented on the unit (i.e., the settings were saved and the unit was reset), you can test the SMS and e-mail settings to ensure that the notifications are sent to the recipients you intended.

#### To send a test message to the notification recipients:

- In the **System Summary** screen, under **SMS & E-mail**, click the **Test E-mail** button or the **Test SMS** button. A sample message is sent to all of the recipients of the specified type of notification.

**Note:** If no recipients are defined for one of the types of notifications, the test button for that type of notification does not appear.

**Note:** Test messages are sent based on the notification configuration settings that are currently defined on the Video Gateway unit. If you make changes to the configuration, but have not yet saved them on the unit and reset the unit, they will not be reflected in the test notifications that are sent.

### Automatically Uploading Video to an AVV Server

You can configure the system to automatically upload recorded video of events from the Video Gateway unit to an AVV (Alarm Video Verification) web server. Once the video has been uploaded, you can access the server via the internet to view the video.

Video of an event can include a few seconds of video from immediately before the event was triggered ("pre-recording") and a few seconds after the event ended ("post-recording"). You can configure the number of seconds of pre- and post-recording to include. Note, however, that the pre-recording video may not be available for upload because it may not have been recorded by the Video Gateway. This can occur if recording from the relevant camera is by-event, and the pre-recording period defined for the camera is shorter than the pre-recording period specified for AVV uploading. The recording settings of the camera are set in the **Camera** screen (see **Configuring Video Recording**, page 106). For additional information, see **Video Recording Settings**, page 105.

If e-mail connection information is configured (see **SMS and E-mail Notifications**, page 61), e-mail notifications are sent to the specified recipients both when the system begins uploading video to the AVV server and when the system successfully completes the upload. The initial e-mail notification includes a picture of the first recorded frame of the event and a link to the relevant video on the AVV server. The second e-mail is a text message that also includes a link to the video on the AVV server. To access the video, you need only click the link in one of the e-mails. You can also access the video on the AVV server by navigating to the download site.
On the MVG and UVG400, video files are sent by the Video Gateway using the highest-priority network connection available. (For information about prioritizing network connections, see Network Priorities, page 54.)

This section explains how to configure the settings that make it possible for the system to upload video to an AVV server. Video is only actually uploaded if AVV is activated in the configuration of the device triggering an event—a camera, sensor, or activator. For information on configuring a device to trigger automatic uploading of events to an AVV server, see the sections about configuring that type of device:

- Video Motion Detection (VMD), page 97
To configure the settings of the AVV server:

1. In the Main Menu, under System, click AVV. The Alarm Video Verifications screen opens:

   ![Alarm Video Verifications screen](image)

   **Figure 69: Alarm Video Verifications screen**

2. Under AVV, select Enabled. The fields required to configure the AVV settings are added to the screen.

   ![AVV screen expanded](image)

   **Figure 70: AVV screen expanded**

3. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Fill in the IP address or hostname of the AVV upload server.</td>
</tr>
</tbody>
</table>
### Configuring System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Same Server for Upload and Download</td>
<td>If the URL for uploading and downloading is the same, select this checkbox. Otherwise, clear this checkbox. The <strong>Download Server</strong> field is added to the screen.</td>
</tr>
</tbody>
</table>
| Download Server                                 | Fill in the IP address or hostname of the AVV download server. The URL must include the network protocol (e.g., *http* or *ftp*).

**Note:** This field does not appear if the **Use Same Server for Upload and Download** is selected.

| Port                                            | Fill in the port used for FTP connections to the AVV server (usually 21). |
| Upload Path                                     | Fill in the path of the FTP directory on the AVV server. The Video Gateway will upload the video files to this directory. |
| Username                                        | Fill in the username required to access the FTP directory on the AVV server. |
| Password                                        | Fill in the password required to access the FTP directory on the AVV server. |
| Download Path                                   | Fill in the path of the HTTP directory on the AVV server. You will download the video files to your PC from this directory. |

4. Under **Recorder Settings**, do one of the following:

   If you want to use the same recorder quality settings for the downloaded video as those used for recorded video that is stored on the Video Gateway, select **Use Default Settings**. Then skip to step 7. Under **Post-Recording**, specify the number of seconds of video from immediately after the event ended to include in the upload.

   - 8.

   If you want to select different recorder quality settings, clear the **Use Default Settings** checkbox. The fields required to configure the recorder settings are added to the screen.

   ![Figure 71: AVV custom recorder settings](image)

**Note:** Default recorder settings are set in the **Camera** screen. For additional information, see **Video Recording Settings**, page 105; **Advanced Recorder Settings**, page 107.

5. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Size</td>
<td>Select the desired frame size for the downloaded video. If the unit is configured to use VGA video resolution, you can choose one of the following:</td>
</tr>
</tbody>
</table>

   - **QSIF**: Small frame (160x120 pixels)
   - **SIF**: Medium-sized frame (320x240 pixels)
   - **VGA**: Large frame (640x480 pixels)

   If the unit uses D1 video resolution, you can choose one of the following:

   - **QCIF**: Small frame (176x120 pixels for NTSC systems and 176x144 for PAL systems)
   - **CIF**: Medium-sized frame (352x240 pixels for NTSC systems and...
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>352x288 pixels for PAL systems)</td>
<td></td>
</tr>
<tr>
<td><strong>D1</strong>: Large frame (704×480 pixels for NTSC systems and 704x576 pixels for PAL systems)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Large frame (VGA or D1) is available only if large-frame recording is activated for one or more of the cameras connected to the Video Gateway. (See Advanced Recorder Settings, page 107.)

For additional information about video resolutions, see Video Resolution, page 18.

**Note:** If you select a frame size that is larger than the frame size of the default recording setting of a camera, the default setting is used and the value you specify is not implemented. For example, if VGA is selected here, and recording for the camera is in SIF, the uploaded video will be in SIF.

**Note:** This setting only affects the resolution of the video uploaded to the AVV server; it does not affect the size of the image attached to the e-mail notification.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPS</td>
<td>Fill in the required framerate for the recordings, in frames per second.</td>
</tr>
</tbody>
</table>

**Note:** If you specify an FPS value that is larger than the FPS value of the default recording setting of a camera, the default setting is used and the value you specify is not implemented.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KBPS</td>
<td>Fill in the required bitrate for the recordings, in kilobits per second.</td>
</tr>
</tbody>
</table>

**Note:** If you specify a KBPS value that is larger than the KBPS value of the default recording setting of a camera, all of the default quality settings are used and the values you specify for maximum size, FPS, and KBPS are not implemented.

6. Under **Pre-Recording**, specify the number of seconds of video from immediately before the event was triggered to include in the upload.

7. Under **Post-Recording**, specify the number of seconds of video from immediately after the event ended to include in the upload.

8. Click **Update**, and then save the settings. The AVV option is added to the camera, sensor, and activator screens. The changes will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

**Note:** You can now configure devices to act as triggers for AVV. A list of devices that are configured to trigger AVV is displayed at the top of the AVV screen.
Viewing the List of Files on the AVV Server

You can view a list of the files on the AVV server by navigating to the http directory on the server. The name of each file indicates the device that detected the event, and the date and start-time of the event. For example:
Office_Security_VMD_(Back_Door)(2)_09_07_2007_20_43_51.svr

To view a list of the video files on the AVV server:

1. In the Address field of a browser, fill in the download address of the video. For example, if your AVV server name is storage.servdemo.net, and the download path is /demo, enter http://storage.servdemo.net/demo/

2. Press Enter. If the download directory requires authentication, a dialog box opens, requesting the username and password.

3. Fill in the username and password, as required, and then click OK. A list of the files stored in the download directory appears in the browser window.
Viewing Video from the AVV server

To view the video that is stored on the AVV server, you download the video to a PC and then play it in SVMultiClient.

To download and view a video file from the AVV server:

1. If you received an e-mail notification of the event, click either the image or the link in the e-mail.
Otherwise, navigate to the download site though the browser as described above, and click the required file in the list.

If the site requires authentication, a dialog box opens, requesting the username and password.

2. Fill in the username and password, as required, and then click **OK**. A dialog box opens, and asks what to do with the video file.

3. Select **Save**. A file selector dialog box opens.
4. Navigate to the location on your PC in which you want to save the video clip file, and then click **Save**. The file is saved in the selected location.

5. Open SVMultiClient.

6. Play the video clip file in SVMultiClient in one of the following ways:
   - Drag the downloaded file to a camera pane in SVMultiClient.
   - In the **Tools** menu, select **Play Downloaded Video**. Navigate to the file, select it, and then click in a camera pane.

   The video clip is played in the camera pane.

   **Note:** For additional information about playing video files in SVMultiClient, please refer to the relevant user guide.

### Disabling AVV

Once AVV uploading has been enabled, you can disable it as follows:

**To disable AVV uploading:**

1. Ensure AVV is disabled for all cameras and sensors connected to the Video Gateway unit.

   **Note:** To do this, in the AVV screen, check the list of devices for which AVV is activated. The list appears below the **Enabled** field if AVV is activated for any devices (see figure 72). For each device in the list, disable AVV in the configuration screen of the device. (For information about how to do this, see the following: on VMD settings, see page 97; on video lost settings, see page 103; on sensor and activator settings, see page 120.)

2. In the **Main Menu**, under **System**, click **AVV**. The **Alarm Video Verifications** screen opens.

3. Under AVV, clear the **Enabled** checkbox. The fields used to configure the AVV settings are removed from the screen.

   **Note:** This checkbox is disabled if AVV is enabled in any VMD or video lost settings, or in the settings of any sensor or activator.

4. Click **Update**, and then save the settings. The AVV option is removed from the camera, sensor, and activator screens. The changes will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).

### FTP Server Settings

You can configure the system to automatically upload snapshots from the Video Gateway unit to an FTP server. This option provides an additional way to back up images of events in real time. It is especially useful when bandwidth limitations make uploading video streams over cellular connections impractical.

Snapshots can be uploaded either at specified intervals, in response to an event, or both. For example, you could configure the Video Gateway to transmit snapshots of all events triggered by Sensor #1, at intervals of 15 seconds, and, in addition, to transmit snapshots from all the cameras every 30 minutes.

This section explains how to configure the system to automatically upload snapshots from all cameras at specified intervals and how to configure the settings that enable the system to upload snapshots of events. In order for snapshots of events to be uploaded, you must also configure the settings of the devices that trigger the events. Snapshots of events are only actually uploaded if FTP is activated in the configuration of a device triggering an event – a camera, sensor, or activator. For information on configuring a device to trigger automatic uploading of event snapshots to an FTP server, see the sections about configuring that type of device:

- **Video Motion Detection (VMD)**, page 97
To configure the settings of the FTP server:

1. In the **Main Menu**, under **System**, click **FTP**. The **FTP Download** configuration screen opens:

```
[FTP Download configuration screen]
```

2. Select the **Enabled** checkbox. The fields required to configure the FTP server settings are added to the screen.

```
[FTP Download enabled]
```

3. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Fill in the IP address or hostname of the FTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Fill in the port used for FTP connections to the FTP server (usually 21).</td>
</tr>
</tbody>
</table>
### Configuring System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Fill in the username required to access the FTP directory on the FTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Fill in the password required to access the FTP directory on the FTP server.</td>
</tr>
<tr>
<td>JPG Upload Interval</td>
<td>Select how frequently snapshots of events should be transmitted to the FTP server. When FTP is activated for a sensor, snapshots from cameras associated with the sensor will be uploaded this frequently. <strong>Note:</strong> The resolution of the snapshots is the same as the resolution of the recorded video of each camera (see Video Recording Settings, page 105).</td>
</tr>
<tr>
<td>Automatic Image Upload</td>
<td>Select how frequently snapshots should be transmitted from cameras (routinely, not in response to events), or select <strong>Disabled</strong> if you do not want any snapshots to be transmitted in this way.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Select the resolution for the snapshots that are uploaded automatically.</td>
</tr>
</tbody>
</table>

4. Click **Update**, and then save the settings. The changes will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

### Schedules

Schedules allow you to configure the unit to automatically switch the running outline at specified times. You can set up standard repeating schedules for routine time periods, such as regular work weeks or the summer months. You can also define special schedules for holidays, both repeating holidays (e.g., New Years Day) and non-repeating holidays (e.g., a presidential visit or the opening ceremony of the Olympics).

The schedule is only implemented by the system if the following conditions are met:

- Multiple outlines are defined for the system (see Defining Alternate Outlines, page 150)
- Schedule-triggered outline-switching is activated in the **General System Settings** screen (see General System Settings, page 17)

**To configure the schedule:**

1. In the **Main Menu**, under **System**, click **Schedules**. The **Schedules** screen opens. If schedule-triggered outline switching is not activated in the **General System Settings** screen, **Inactive** appears in parentheses after the name of the screen. In this case, you can configure the schedule, but it will not be implemented unless you activate schedule-triggered outline switching.
2. Select Enabled. The schedule grid and its controls are displayed.

The upper part of the screen contains the schedule grid. Below it are controls that allow you to attach specific outlines to particular days and times in the grid. Below these, user-defined holidays appear, if any are defined.

Initially, the schedule grid contains a row for each day of the week and a column for each hour of the day. This grid defines the routine schedule for regular work weeks. Each cell in the grid contains two colored rectangles (see figure 80 below). Each of these rectangles represents a half hour – half of the time represented by the entire cell. The color of the rectangle indicates which outline it represents.

The key to the color-coding of the outlines appears below the grid. For example, in figure 80 below, the Default outline is represented in the grid by a red rectangle, the Parking Lot outline by a blue rectangle, the Out of Service outline by a green rectangle, and the Office Closed outline by a gray rectangle. Thus, the top-left cell in the grid says that the Default outline should run from midnight to 12:30 am, and the Out-of-Service outline should run from 1:30 am to 1:00 am.
Figure 80: Color-coded schedule

3. Follow the instructions below to create a basic, repeating weekly schedule and to add holidays to the schedule.

Configuring a Standard Weekly Schedule

This section explains how to set up a basic, repeating weekly schedule of outline implementation.

To define the basic weekly schedule:

1. In the color-coding key, click the name of the outline you want to assign to one or more time slots in the schedule grid. A colored rectangle representing the selected outline is displayed below the key area, under Selected Outline, and the name of the outline is displayed below this. For example, in the figure below, the selected outline is Default, represented by the red rectangle.
2. If you want to apply the outline to the entire week’s schedule, click **Set all schedules to currently selected outline**. All of the rectangles in the schedule grid are switched to the color representing the selected outline.

3. If you want to apply the outline to specific day of the week, click the name of the day in the schedule grid. All of the rectangles in the row are switched to the color representing the selected outline.

4. If you want to apply the selected outline to a rectangular area of the schedule grid (containing multiple rectangles), do the following:
   - Make sure the **Change Multiple Times** checkbox is **selected**.
   - Click one corner of the rectangular area. A border appears around the rectangle.
Click the diagonally opposite corner of the rectangular area that you want to mark. The selected outline is applied to the entire rectangle.

Figure 83: Clicking the diagonally opposite corner of the area

Note: The entire schedule grid, representing full 24-hour days, may not be visible at one time on your screen. Use the horizontal scrollbar at the bottom of the screen to move the display to the right or left so that you can see the relevant times of day.

5. If you want to apply the selected outline to individual half-hour time slots, do one of the following:
   - With the Change Multiple Times checkbox selected, double-click the rectangle representing the time slot.
   - With the Change Multiple Times checkbox cleared, click the rectangle representing the time slot. The rectangle is displayed in the color representing the selected outline.

6. Repeat steps 1–5 as necessary for each type of outline you want to apply to a time slot in the schedule.

7. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

Defining Holiday Schedules

Holiday schedules are essentially exceptions to the standard weekly schedule. When you define a holiday, you can choose to apply an existing day’s schedule to it. For example, you can apply the Sunday schedule to Independence Day. Alternatively, you can create a new day’s schedule and apply the new schedule to one or more holidays. To do this, you add a row to the schedule grid. For example, you could add a row called Business Holiday, define a schedule for it, and then create a holiday called Independence Day to which you apply the Business Holiday schedule (see Defining a New Schedule Row, page 84).

Holiday schedules can overlap. For example, if you create a holiday schedule for the first week of July, and another holiday schedule for July 4th, the two schedules both apply to July 4th. In this case, the system creates a hierarchy of schedules:

- Shorter time periods are given precedence over longer time periods.
- Non-repeating schedules are given precedence over repeating schedules.
- Repeating holiday schedules are given precedence over the standard weekly schedule.

Thus, in the example above, the July 4th schedule will be implemented on July 4th, and the schedule for the first week of July will be implemented on the other days of the week.

To define a holiday:

1. In the Schedules screen, in the Holidays section, click Edit Holidays.

Configuring System Settings
The Holidays screen opens. The screen displays the schedule grid at the top (it is not editable here), and below it, a list of the holidays that are already defined (if any).
2. Click Add Holiday. A blank New Holiday section opens.

3. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the holiday, e.g., New Years Day.</td>
</tr>
<tr>
<td>Start Date</td>
<td>The date of the first day of the holiday.</td>
</tr>
<tr>
<td>End Date</td>
<td>The date of the last day of the holiday. If the holiday only lasts one day, this is the same as the start date.</td>
</tr>
</tbody>
</table>
### Configuring System Settings

#### Defining a New Schedule Row

In addition to the standard rows for the days of the week, you can create custom schedule rows that can be implemented on holidays. For example, you could create a special row with a schedule that is to be applied only on New Years Day.

**To define a new schedule (row):**

1. In the **Schedules** screen, below the schedule grid, click **Add Row**. A new row is added to the grid.
Configuring System Settings

2. In the text field, modify "New Schedule" to define a name for the schedule.

3. Click **Update**. The name of the row is updated.
4. Follow the instructions under *Configuring a Standard Weekly Schedule*, page 79 to select the outlines to implement in each time slot.

**Note:** To assign the new schedule to a holiday, click *Edit Holidays* to open the *Holidays* screen. Follow the instructions above (see *Defining Holiday Schedules*, page 81) for configuring the holiday. The new schedule appears in the holiday configuration section in the *Day* dropdown list.

**Audio Settings**

Audio settings enable and configure the speakers and microphone, as follows:

- **Audio Out settings:** Enable internal and external speakers, and control the volume of the speakers. When the speakers are enabled, remote users can speak into a microphone on a client device and be heard through the unit’s speakers on-site. (SVMultiClient, and most of the cellular client-applications support this feature.)

- **Audio In settings:** Enable the microphone and control its volume. When a microphone is connected and enabled, audio from the site can be heard along with live and recorded video.

**To configure audio settings:**

1. In the *Main Menu*, under *System*, click *Audio*. The *Audio Settings* screen opens:

2. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speaker</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: Disable both speakers.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Internal</strong>: Enable the internal speaker. (If an external speaker is connected to <em>Aout</em>, it is disabled.)</td>
</tr>
<tr>
<td></td>
<td>- <strong>External</strong>: Enable the external speaker. (The internal speaker is disabled.)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Both</strong>: Enable both the internal speaker and the external speaker. (The same audio stream will be played on both speakers at the same time.)</td>
</tr>
</tbody>
</table>

**Note:** This field controls the use of the speakers to play sound that is transmitted from a client device. Even if one or both of the speakers is disabled here, they can still be used to play audio when a CCTV is connected to the Video Gateway. See
## Configuring System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Configuring a CCTV Monitor (TV-Out), page 25.</td>
<td>Note: On the HVG400, even if the internal speaker is enabled here, it can still be turned off by flipping down the Mute switch on the rear of the unit.</td>
</tr>
<tr>
<td>Internal Speaker Volume</td>
<td>Set the output volume for the unit’s built-in speaker, as explained under Configuring Microphone and Speaker Volume, below.</td>
</tr>
<tr>
<td>Input Volume Ch 1 /</td>
<td>Set the input volume for microphones connected to the unit, as explained under Configuring Microphone and Speaker Volume, below.</td>
</tr>
<tr>
<td>Input Volume Ch 2</td>
<td>Note: On CVG and CVG-M models, only channel 1 is supported.</td>
</tr>
<tr>
<td></td>
<td>Note: On the HVG400, if the Which input to use? field appears, the unit only supports one microphone. Select the audio channel to which the microphone is connected from the dropdown list, and then set the input volume for that microphone as described below.</td>
</tr>
</tbody>
</table>

3. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

**Note:** Input volume settings are implemented immediately if you select **Update Now**. However, they are only saved on the unit after you click **Update** and save the settings.

### Configuring Microphone and Speaker Volume

The volume of attached microphones and of the internal speaker can be digitally increased or decreased by the Video Gateway. Microphone volume can be modified to optimize the sound level of audio that is played by client software. Internal speaker volume can be adjusted to suit the location of the Video Gateway unit and the needs of those on-site.

You can choose from 11 levels of amplification. Level 5 means the volume is not modified at all. Levels 0 through 4 cause the volume to be reduced (the smaller the number, the greater the reduction); levels 6 through 10 cause it to be amplified (the greater the number, the greater the amplification). Level 6 is generally optimal for the internal speaker, level 9 for passive microphones, and level 5 for active microphones.

![Volume Levels](image)

You can test the volume settings as you configure them by connecting to the Video Gateway using a client application. Volume levels can be adjusted for testing purposes without resetting the Video Gateway unit.

### Configuring Internal-Speaker Volume

You can optimize the internal-speaker volume settings by testing them as you configure them.

**To configure the volume of the internal speaker:**

1. Make sure someone is near the Video Gateway to listen to sound being transmitted from the speaker.

2. Using a client application that can transmit audio to a Video Gateway (SVMultiClient and some of the cellular client applications), connect to the Video Gateway.

3. Speak into the microphone of the client device and check with the listener to find out if the volume is appropriate. If it is not, adjust the settings as described below until they are satisfactory.

4. In the **Audio Settings** screen, under **Internal Speaker Volume**, select a volume setting.
Configuring System Settings

Figure 91: Speaker volume settings

5. Click **Update Now**. The volume settings are updated on the Video Gateway immediately.

![Speaker Volume Settings](image)

**Figure 92: Update Now button**

*Note:* All of the settings on the page are saved when you click **Update Now**. The volume settings are implemented immediately, and the changes to the other settings are implemented after the unit is restarted (see *Saving Configuration Changes*, page 157). If you modify the volume settings and click the **Update** button in the lower-right corner of the screen, the volume settings are not implemented until the unit is restarted.

6. Repeat steps 3–5 as necessary until the optimal volume setting is selected.

7. Click **Update**, and then save the settings.

Configuring Microphone Volume

You can optimize the microphone volume settings for a particular client by testing the microphone settings as you configure them.

**To configure the volume of a microphone:**

1. Open the client application for which you want to optimize the settings (e.g., SVMultiClient), connect to a live video stream that is linked to the microphone, and listen to the sound. If the volume needs adjustment, adjust it as explained in the following steps.

2. In the **Audio Settings** screen, under **Audio In**, select a volume setting for the microphone. (For HVG400, MVG400, and UVG400 models, which have two microphone connectors, “CH1” sets the volume of the microphone connected to **Ain1**, and “CH2” sets the volume for **Ain2**).

   ![Microphone Volume Settings](image)

   **Figure 93: Microphone volume settings (HVG400, MVG400, UVG)**

   ![Microphone Volume Settings](image)

   **Figure 94: Microphone volume settings (MVG200, CVG, CVG-M)**

3. Click **Update Now** (see figure 92 above). The volume settings are updated on the Video Gateway immediately.
Note: All of the settings on the page are saved when you click Update Now. The volume settings are implemented immediately, and the changes to the other settings are implemented after the unit is restarted (see Saving Configuration Changes, page 157). If you modify the volume settings and click the Update button in the lower-right corner of the screen, the volume settings are not implemented until the unit is restarted.

4. In the client application, listen to the audio from the video stream that is linked to the microphone.

5. Repeat steps 2–4 as necessary until the optimal volume setting is selected.

6. Click Update, and then save the settings.

GPS

GPS makes it possible to track the location of an MVG or CVG-M unit by means of the unit’s built-in GPS receiver. When GPS is enabled on an MVG or CVG-M unit, the unit uses the built-in GPS receiver to check its location at specified intervals. Whenever you are connected to the unit through the SVMultiClient or the SVControlCenter client application, the location data that is received is automatically sent to the client. You can then use the client to view the last detected location of the unit on a map. (For additional information about viewing the unit’s location on a map, and tracking the route taken by the unit, please refer to the SVMultiClient User Guide and the SVControlCenter Guide.)

If you choose to record GPS data, you can use SVMultiClient or SVControlCenter to see the path that was taken by the unit before it reached its last detected location. Recorded data is stored on the unit until the allocated disk space is filled; then, the oldest data is overwritten by the newest data. The unit can store a great deal of GPS data. For example, the MVG400 can store over one million GPS data points – approximately 2 months’ worth of location data when the data is retrieved every 5 seconds.

Configuring GPS

If you have a server that can receive GPS data, MVG and CVG-M units can be configured to send the data to that server at specified intervals. Alternatively, you can send the data to a device connected to the serial port (the RS232/485 connector) of the Video Gateway unit (for additional information about this option, please consult your vendor), or configure SVControlCenter to download it to its database for later use (see the SVControlCenter User Guide).

GPS data can be sent in one or more of the following syntaxes. These syntaxes are part of the NMEA (National Marine Electronics Association) standard that defines the data required to process a GPS location. The available syntaxes are:

- **RMC**: A modified version of Recommended Minimum sentence version C that includes some additional information that is not included in the standard NMEA definition, such as the name of the sending unit. Please consult your vendor for a complete description of this sentence.

- **GGA sentences**: Standard GGA sentences

- **GLL**: Sentences that are compatible with the syntax used by the Galooli fleet-management system (for additional information about this system, see http://www.galooli.com/solutions/galooli-fleet/)

Once the GPS data is received by your NMEA server or a device connected to the serial port, you can use it as you wish – to display in a map, monitor vehicle locations and possible deviations from the intended route – or store the data for future use.

NOTE: SerVision does not provide any software for handling NMEA data that is transmitted to an NMEA server. You must acquire and set up any required software on your own.
To configure the GPS settings:

1. In the GPS Settings screen, under GPS, select Enabled. The fields required to configure the GPS settings are added to the screen:

   ![GPS Settings](image)

   **Figure 95: GPS settings**

2. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS Frequency</td>
<td>Specify how often the unit records its location, in seconds. Recommended value: 5.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Because GPS location recording requires system resources, it is not recommended to increase the frequency. While one check every five seconds is not sufficient for navigation via GPS, it provides ample information for tracking purposes.</td>
</tr>
<tr>
<td>GPS Recording</td>
<td>Select this option to record the results of each GPS location check. This option must be selected if you want to be able to see the route followed by the vehicle, or see where the vehicle was when a particular event occurred, in SVMultiClient.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Clearing this option does not free disk space for other uses.</td>
</tr>
</tbody>
</table>

3. If you want to send GPS data to a server or a device connected to the serial port, under Send GPS Data to Server, select Enabled. The fields required to configure this option are added to the screen:

   ![Send GPS Data to Server](image)

   **Figure 96: Send GPS Data to Server settings**

   **Note:** Whenever this option is enabled, GPS recording is automatically activated and cannot be deactivated.

4. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMC to server</td>
<td>Select this option if you want to send GPS data in RMC syntax to an NMEA server.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RMC to serial</td>
<td>Select this option if you want to send GPS data in RMC syntax to a device connected to the serial port of the Video Gateway unit. The data is sent at 4800 baud, 8 bits, no parity, one stop bit (8N1).</td>
</tr>
<tr>
<td>GGA to server</td>
<td>Select this option if you want to send GPS data in GGA syntax to an NMEA server.</td>
</tr>
<tr>
<td>GGA to serial</td>
<td>Select this option if you want to send GPS data in GGA syntax to a device connected to the serial port of the Video Gateway unit. The data is sent at 4800 baud, 8 bits, no parity, one stop bit (8N1).</td>
</tr>
<tr>
<td>GLL</td>
<td>Select this option if you want to send GPS data to a Galooli server.</td>
</tr>
<tr>
<td>ID</td>
<td>If you selected GLL, enter the Galooli server ID.</td>
</tr>
<tr>
<td>Server address</td>
<td>If you opted to send RMC, GGA, or GLL data to a server, fill in the IP address or hostname of the server.</td>
</tr>
<tr>
<td>Port</td>
<td>If you opted to send either RMC or GGA data to an NMEA server, fill in the port used to by the server to receive NMEA data.</td>
</tr>
<tr>
<td>Sending frequency</td>
<td>If you opted to send RMC, GGA, or GLL data to a server, specify how often the data should be transmitted to the server, in seconds. Recommended value: 30.</td>
</tr>
<tr>
<td>Sending frequency - ignition off</td>
<td>If you opted to send GPS data to a server, and the Video Gateway is configured to continue working after the vehicle ignition is turned off (either for a limited period of time or indefinitely; see page 22), specify how often the data should be be transmitted to the server when the ignition is off.</td>
</tr>
<tr>
<td>RMC history</td>
<td>If you chose to send RMC data, specify how much data should be stored for sending later if the unit fails to send the data to the RMC server.</td>
</tr>
</tbody>
</table>

**Erasing Recorded GPS Data**

Recorded GPS data is normally stored on the unit’s storage media until it is over-written by newer data. You can also erase all GPS data from the unit manually.

*To erase all recorded GPS data from the unit’s storage media:*

- In the **System Summary** screen, under **GPS**, click **Erase GPS Recordings**. The recordings are erased.

![Figure 97: Erase GPS Recordings](image)

**Note:** The **Erase GPS Recordings** button only appears if GPS recording is enabled in the **General System Settings** screen (see **Configuring GPS**, page 89).
Configuring Camera Settings

The **Camera** screens are used to configure the cameras connected to the Video Gateway unit. Settings include the name of the camera; the desired brightness, contrast, and saturation; pan-tilt-zoom (PTZ) settings; audio settings; video-motion-detection (VMD) settings; video-lost settings; and recording settings.

**About Brightness and Contrast Settings**

Brightness and contrast settings affect the camera and not just the display in the client interface. The settings defined in the **Camera** screens are the default settings for video streams from the specified camera. When the video stream is displayed in the client, these settings can be modified. This makes it possible for you to fine-tune the settings while you are viewing the stream.

Modifications that are implemented in the client affect all live and recorded video from the relevant camera until the Video Gateway unit is reset. To implement them permanently, they must be saved in the unit’s configuration. To save settings that are modified in a client application, you must log into the configuration utility and update the settings there, as described below.

**NOTE:** Changes to brightness and contrast settings affect the camera directly, and are thus reflected in all displays of live video from that camera from the time they are implemented. Similarly, video that is recorded from the camera after the changes are implemented is also affected. The brightness and contrast settings that are optimal for a particular monitor may not display as well on other monitors or screens. Therefore, care should be taken when changes are made, and, furthermore, it may not be advisable to save the modified settings on the unit in every case.

**Configuring Video Cameras**

The **Camera Summary** screen summarizes the current settings of each camera in the system, and provides links to the camera configuration screens, in which the camera settings can be modified.

![Figure 98: Camera Summary screen](image)

Each camera in the system is configured in its own configuration screen. The camera configuration screens are accessed from the **Camera Summary** screen.
To open the Camera Summary screen:
- In the Main Menu, click Cameras.

To configure a camera:
1. In the Main Menu, under Cameras, click the camera (e.g., Camera 1 to configure the camera plugged into Vin1). The relevant Camera configuration screen opens:

![Figure 99: Camera configuration screen](image)

2. Select the Enabled checkbox. The fields required to configure the camera settings are added to the screen.
Figure 100: Camera enabled

Note: If **Enabled** is not selected, the camera cannot record and will not appear in client applications.

3. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Type a name for the camera (up to 20 characters). Each of the cameras must have a different name. The camera names are used to identify the camera in client applications. <strong>Note:</strong> If the Video Gateway will be working in conjunction with an SVBackup server, use only English characters in the name.</td>
</tr>
<tr>
<td><strong>Embedded Text</strong></td>
<td>If you want an identifying label to be included in each frame of video that is displayed in a client application, type the text of the label. You can include the variables <strong>&amp;C</strong> and <strong>&amp;S</strong> in the text where you want to insert the camera name and system name. For example, if the camera name is &quot;Front Door&quot; and the system name is &quot;Bus2045,&quot; type &quot;&amp;C camera on &amp;S,&quot; and the label embedded in each frame would say &quot;Front Door camera on Bus2045.&quot;</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Brightness | Adjust the default brightness of the camera. Range: 1–100. These values are used when the Video Gateway unit is started. **Note:** You can also adjust the brightness in the client or in a CCTV monitor (with the touch/mouse enabled) as you view the video stream (see page 92).
Contrast | Adjust the default contrast of the camera. Range: 1–100. These values are used when the Video Gateway unit is started. **Note:** You can also adjust the contrast in the client or in a CCTV monitor (with the touch/mouse enabled) as you view the video stream (see page 92).
Saturation | Adjust the default saturation of the camera. Range: 1–100. Higher saturation produces more vivid colors.

**Note:** Changes to brightness, contrast, and saturation are implemented immediately when Update is clicked.

4. If the camera has PTZ features, and you want to use them to control the camera remotely through a client application, under Camera Control (PTZ), select Enabled. Then follow the instructions below (Configuring PTZ, page 96).

5. Under Audio, select one of the following:
   - **None:** Do not link any audio to the video from this camera.
   - **Channel 1:** Link the audio from the microphone connected to Ain1 to the video from this camera.
   - **Channel 2:** Link the audio from the microphone connected to Ain2 to the video from this camera (HVG400, MVG, UVG400 only).

   **Note:** In HVG400 units that only support one microphone, you will either see Channel 1 or Channel 2 in the dropdown list, depending on which one was activated. For additional information, see the description of the Input Volume field (page 87).

   If you selected None, skip to step 8.

   If you selected either Channel 1 or Channel 2, audio from the selected microphone is available whenever you view live video in a client application. In addition, the fields required to configure recording of audio with recorded video from this camera are added to the screen, and a message appears indicating that audio recording is enabled. This means that audio from the selected microphone is incorporated with all video recorded from the camera.

6. In the audio-recording-enabled message, click **OK**.
7. If you do not want audio to be incorporated with the video recorded from the camera, under Audio Recording, clear the Enabled checkbox.

**Note:** The Audio Quality field is not currently in use. All audio recordings have medium quality.

**Note:** If recording is not activated, this checkbox cannot be cleared.

8. If you want to use the Video Gateway’s VMD features to detect and respond to motion in the camera’s field of view, under Motion Detection (VMD), select Enabled. Then follow the instructions below (Video Motion Detection (VMD), page 97).

**Note:** Be aware that on PTZ-controlled cameras each change of the camera position is interpreted by the VMD system as an event.

9. Configure the unit’s response to interruptions in the transmission of the video signal from the camera to the unit as described below (Configuring Video Lost, page 103).

10. Configure the camera’s recorder as described below (Video Recording Settings, page 105).

11. Click Update. Changes to brightness, contrast, and saturation are implemented immediately. Save the settings to implement them permanently. Save the settings and restart the unit to implement all other changes (see Saving Configuration Changes, page 157).

## Configuring PTZ

This section explains how to configure the pan-tilt-zoom (PTZ) controls of cameras that support these features. Once the controls are configured, the camera can be aimed and zoomed remotely using any of the client applications.

**NOTE:** For information about connecting the PTZ controller to the Video Gateway unit, please refer to the unit’s installation guide.

#### To configure pan-tilt-zoom controls (PTZ) in cameras that support these features:

1. In the Camera configuration screen, under Camera Control (PTZ), select Enabled. The fields required to configure the PTZ settings are added to the screen:

   ![Figure 103: PTZ settings](image)

2. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select the communication protocol used by the camera for PTZ control.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Consult the camera documentation or the camera vendor for this information.</td>
</tr>
</tbody>
</table>

---

**Configuring Camera Settings** 96
### Video Motion Detection (VMD)

When Video Motion Detection (VMD) is enabled, the Video Gateway automatically checks the field of view (FOV) of the camera for changes. When changes are detected, the Video Gateway triggers a VMD event. You can configure the VMD itself, and the event notifications that are generated when VMD events are triggered.

### About VMD Regions

The FOV is divided into regions, and the relative sensitivity of the motion detection can vary from region to region. For example, if a computer monitor in the FOV of the camera causes motion detection events to be triggered unnecessarily, you can choose to mark the region of the monitor for low sensitivity, or even no motion detection, while the rest of the FOV would have high sensitivity. In addition, you can completely black out regions from the FOV if you do not want them included in the video images at all.

If the camera is connected to the Video Gateway, and regions are enabled, the Camera configuration screen shows the current FOV of the camera. Regions that are included in motion detection are marked with a colored \( \times \): blue for low sensitivity, green for medium sensitivity, and red for high sensitivity. Regions that are not included in motion detection are not marked, and regions that are not included in the video images at all are marked with a black \( \times \) on a white background.

**NOTE:** If VMD is enabled, but regions are not, middle sensitivity is applied to the entire FOV.

**NOTE:** If the camera is not connected to the Video Gateway, a blank tan image is displayed. It is recommended that you select the regions for inclusion in VMD when you can see an actual image.

### About VMD Event Settings

A VMD event starts when motion is first detected and ends when there is no motion. However, in many cases what is seen by the human eye as one event can be interpreted by the VMD system as a series of motions with idle periods. When this occurs, a single motion event is broken into a series of short events. On the other hand, a motion event as detected by the VMD system can be exhaustingly long, such as a full day in a busy shop. In this case, we would prefer to break it down into a number of shorter events.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud Rate</td>
<td>Select the baud rate used by the camera for PTZ control.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Consult the camera documentation or the camera vendor for this information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The other connection parameters required by the Video Gateway are: one start bit, one stop bit, no parity, and 8-bit. If the camera uses different parameters, please contact your vendor.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Select the type of connection that is used for the PTZ controls – RS232 or RS-485.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Consult the camera documentation or the camera vendor for this information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If multiple PTZ cameras that use the RS485 connection type are connected to the Video Gateway unit, they must all use the same protocol.</td>
</tr>
<tr>
<td>Camera ID</td>
<td>If the camera is connected using RS485, specify its ID number.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This number must correspond to the camera ID that is set on the camera. Consult the camera documentation for information about setting the camera ID. If multiple PTZ cameras using the RS485 connection are connected to the Video Gateway unit, they must have distinct camera IDs.</td>
</tr>
</tbody>
</table>
To solve these two problems, VMD event detection can be configured to control the length of events using the following parameters:

- **Debounce**: The interval between the end of motion as detected by the unit and the time when the event is defined as ending.
- **Maximum length**: The maximum length of a single event.

Separate events are defined when motion is not detected for a specified debounce interval. For example, if the interval is 15 seconds, event A ends when motion is not detected for 15 seconds, and event B begins if motion is detected again after more than 15 seconds have elapsed. If less than 15 seconds pass at the end of event A before additional motion is detected, event A is extended to include the additional motion.

Separate events are also defined when the maximum event length is reached. For example, if the maximum length of an event is 30 minutes, new events are generated every 30 minutes even if motion was detected without interruption during the entire period.

Consider, for example, a camera that is set up in a train station. During peak hours, there is usually constant motion. During off hours, lengthy intervals between motion events are common. The debounce interval is 30 seconds, and the maximum event length is 1800 seconds (30 minutes). During peak hours, event-triggered recording generates continuous recording because VMD events are constantly detected. However, the video is divided into 30-minute events, making it easy to check the video to see what happened during a particular time range. During off-peak hours, events are typically much shorter, and recording is not continuous.

**About Responses to VMD Events**

You can configure the unit to respond to VMD events in any or all of the following ways:

- Upload video of the event to an AVV server on the internet (see *Automatically Uploading Video to an AVV Server*, page 67). If e-mail notification recipients are defined in the SMS and E-mail screen, an e-mail message is sent to all the recipients when the VMD event begins and a second e-mail is sent when the video is successfully uploaded and is available for downloading by users. The e-mail notification includes a link to the video file on the server and a picture of the event. (Note that the file transfer starts at the end of the VMD event to ensure that it encompasses the entirety of the event.)

- Upload snapshots of the event to an FTP server on the internet (see *FTP Server Settings*, page 75).

- Send VMD event notifications to the SMS and/or e-mail recipients defined for the system (see *SMS and E-mail Notifications*, page 61). E-mail notifications can optionally include a picture of the event, and, if AVV is activated, a link to video of the event.

- Turn an activator on or off.

- Move any PTZ camera connected to the Video Gateway that supports presets to a preset location.

These actions can be implemented when the event begins, when it ends, or both.

**Configuring VMD Settings**

This section explains how to configure VMD settings for a camera.

**To configure video motion detection (VMD):**

1. In the Camera configuration screen, under Motion Detection (VMD), select Enabled. The fields required to configure the VMD settings are added to the screen:
Figure 104: VMD settings

2. If you want to define the level of sensitivity of the motion detection that is implemented in the field of view (FOV), and perhaps specify different levels of sensitivity for different regions of the FOV, under Regions, select Enabled. Otherwise, skip to step 8.

The fields required to define sensitivity levels and regions are added to the screen, and, if the camera is connected to the unit, the current FOV is displayed:

Figure 105: Region sensitivities in the FOV

Note: To update the snapshot of the camera’s FOV, click Reload Snapshot.

Note: If the camera is not connected to the Video Gateway, the FOV is blank.

3. Click the sensitivity level you want to apply to a region or regions of the FOV. The selected level appears below the list under CURRENT. For example, in the figure above, MEDIUM SENSITIVITY is selected.

Note: The following region marks can be used:
### Marking Camera Settings

#### Table: Mark and Description

<table>
<thead>
<tr>
<th>Mark</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue x</td>
<td>Low VMD sensitivity</td>
</tr>
<tr>
<td>Green x</td>
<td>Medium VMD sensitivity</td>
</tr>
<tr>
<td>Red x</td>
<td>High VMD sensitivity</td>
</tr>
<tr>
<td>None</td>
<td>No motion detection</td>
</tr>
<tr>
<td>Black x on white</td>
<td>Region blacked: no video capture</td>
</tr>
</tbody>
</table>

1. If you want to set the entire FOV to the specified sensitivity level, click the relevant sensitivity level, and then click **Set all regions**. The x's marking the entire FOV are colored, or removed, accordingly.

2. If you want to apply the current sensitivity level to a rectangular area of the FOV (containing multiple region markers), do the following:
   - Make sure the **Change Multiple Times** checkbox is **selected**.
   - Click one corner of the rectangular area. A border appears around the region.
   - Click the diagonally opposite corner of the rectangular area. The current sensitivity level is applied to the entire rectangle.

![Figure 106: FOV with border around selected marker](image)

- Click the diagonally opposite corner of the rectangular area. The current sensitivity level is applied to the entire rectangle.
6. If you want to apply the current sensitivity level to individual regions, do one of the following:

- With the **Change Multiple Times** checkbox **selected**, double-click the region.
- With the **Change Multiple Times** checkbox **cleared**, click the region.

An x of the color representing the selected sensitivity level appears on the image (or the x is removed from the area, if the current sensitivity level is "Motion Disabled").

7. Repeat steps 3–6 as necessary for each type of sensitivity level you want to apply to a region of the FOV.

---

**Figure 107: Sensitivity level applied to selected rectangle**

---

8. Under **Debounce**, specify the minimum interval between events, in seconds. Range: 3–30 seconds. If motion is detected, and then ceases, the motion detection event is only closed if this amount of time has passed without any motion.

**Example:** Motion is detected at 3:15:05 and continues until 3:15:45. After this, motion is not detected again until 3:16:10, 25 seconds after it was last detected. If the debounce interval is 15 seconds, two separate VMD events are triggered. If, on the other hand, the debounce interval is 30 seconds, only one VMD event is triggered, beginning at 3:15:05 and continuing past 3:16:10.

**Tip:** If a lot of motion is likely to be detected by the camera, it is best to specify a relatively long debounce interval, so that the system does not generate a very long list of short events.
9. Under **Maximum Event Length**, specify the maximum length of a VMD event, in seconds. Range: 60–86400 seconds (1 minute – 1 day). If motion is detected continuously for longer than this period of time, a new event is automatically generated at the end of this interval.

10. Under **On Motion Detected**, select the actions that the Video Gateway should perform if motion is detected, as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AVV</strong></td>
<td>Select this option to have the Video Gateway send video of the event to an AVV server for downloading. The video is uploaded to the site defined in the AVV screen, in the format defined there (see <em>Automatically Uploading Video to an AVV Server</em>, page 67), and e-mail notifications are sent to all e-mail recipients (see <em>SMS and E-mail Notifications</em>, page 61).&lt;br&gt;&lt;br&gt;<strong>Note:</strong> The upload of the video clip begins at the end of the motion event. Nevertheless, the first e-mail notification is sent when the event is first detected. Thus, the video clip may not be available yet when you receive this e-mail notification. A second e-mail notification is sent when uploading is completed.&lt;br&gt;&lt;br&gt;<strong>Note:</strong> This feature only works if recording (either event-triggered or continuous) is activated for the camera (see <em>Video Recording Settings</em>, page 105).&lt;br&gt;&lt;br&gt;<strong>Note:</strong> This option only appears if AVV is activated for the Video Gateway (see <em>Automatically Uploading Video to an AVV Server</em>, page 67).</td>
</tr>
<tr>
<td><strong>FTP</strong></td>
<td>Select this option to have the Video Gateway send snapshots of the event to an FTP server.&lt;br&gt;&lt;br&gt;<strong>Note:</strong> This option only appears if FTP is enabled for the Video Gateway (see <em>FTP Server Settings</em>, page 75).</td>
</tr>
<tr>
<td><strong>SMS</strong></td>
<td>Select this option to have the Video Gateway send SMS notifications when a motion event is detected. Messages are sent to the recipients specified in the SMS and E-mail screen, in the format defined there (see <em>SMS and E-mail Notifications</em>, page 61).</td>
</tr>
<tr>
<td><strong>E-mail</strong></td>
<td>Select the desired type of e-mail notification, as follows:&lt;br&gt;&lt;br&gt;• <strong>None</strong>: Do not send e-mail notifications when a motion event is detected.&lt;br&gt;&lt;br&gt;• <strong>Text only</strong>: When a motion event is detected, send e-mail notifications. Include a text message in the e-mail, but do not attach any images to the message.&lt;br&gt;&lt;br&gt;• <strong>Text &amp; image</strong>: When a motion event is detected, send e-mail notifications that include both a text message and a picture of the first frame of the event.&lt;br&gt;&lt;br&gt;<strong>Note:</strong> E-mail messages are sent to the recipients specified in the SMS and E-mail screen, in the format defined there (see <em>SMS and E-mail Notifications</em>, page 61).&lt;br&gt;&lt;br&gt;<strong>Note:</strong> If AVV is selected, Text &amp; image is automatically selected for this field, and cannot be disabled. A single e-mail containing both the standard notification text and the AVV notification is sent at the beginning of each event. In addition, a text-only e-mail is sent when the file transfer is completed.&lt;br&gt;&lt;br&gt;<strong>Note:</strong> If AVV was once selected, and has since been cleared, Text &amp; image remains selected for this field until the selection is changed manually. If it is not changed, AVV is not activated, but notifications with snapshots are sent at the beginning of each event.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Activator 1 | Select the action that each activator should perform when a motion detection event begins:
- **Turn on**: Set the activator line to "high."
- **Turn off**: Set the activator line to "low."
- **None**: Do not change the activator’s setting.

**Note:** For additional information about working with activators, see *Configuring Sensor and Activator Settings*, page 120.

**Note:** The Activator 2 field only appears for the HVG400, MVG, and UVG400.

Activator 2 | 
Go To Preset | All PTZ cameras connected to the Video Gateway that support presets are listed below this heading. If you want one of these cameras to automatically aim at a preset location when a motion detection event begins, beside the name of the camera, select the number of the preset location.

**Note:** Preset locations are defined and assigned numbers using a client application such as SVMultiClient. For additional information, please refer to the relevant client application guide.

**Note:** If no PTZ cameras are connected to the unit, this field does not appear.

11. Under **On Motion Ended**, select the actions that the Video Gateway should perform when a motion detection event ends, as described above.

### Configuring Video Lost

The Video Gateway monitors the camera connections. If the video signal from a camera is lost – i.e., the Video Gateway is not receiving video from it, either because of a malfunction in the camera, or because the camera has been disconnected from the unit or from its power source – the unit can respond in any or all of the following ways:

- Upload video of the event to an FTP server on the internet (see *Automatically Uploading Video to an AVV Server*, page 67). If e-mail notification recipients are defined in the **SMS and E-mail** screen, an e-mail message is sent to all the recipients when the Video Lost event begins and a second e-mail is sent when the video is successfully uploaded and is available for downloading by users. Each e-mail notification includes a link to the video file on the server and a picture of the event.

- Send event notifications to the SMS and/or e-mail recipients defined for the system (see *SMS and E-mail Notifications*, page 61). If AVV is activated, e-mail notifications include a link to video of the event that includes the seconds preceding the time when the video signal was lost (the *pre-record*; see *Video Recording Settings*, page 105). Video-Restored e-mail notifications can optionally include a picture of the event.

- Turn an activator on or off.

- Move any PTZ camera connected to the Video Gateway that supports presets to a preset location.

These actions can be implemented when the event begins, when it ends, or both.

**To configure video lost detection:**

1. In the **Camera** configuration screen, under **Video Lost**, select the actions that the Video Gateway should perform if video reception from the camera is interrupted, as described below.
Figure 109: Video Lost settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **AVV** | Select this option to have the Video Gateway send video of the seconds preceding the video-lost event to an AVV server for downloading. The video is downloaded to the site defined in the AVV screen, in the format defined there (see Automatically Uploading Video to an AVV Server, page 67), and e-mail notifications are sent to all e-mail recipients (see SMS and E-mail Notifications, page 61).

**Note:** Two e-mail notifications are sent – one when the event is first detected, and the other when uploading of the video to the AVV server is completed. Thus, the video clip may not be available yet when you receive the first e-mail notification.

**Note:** This feature only works if recording (either event-triggered or continuous) is activated for the camera (see Video Recording Settings, page 105).

**Note:** For video-restored events, a few seconds of video following the restoration of the video connection are recorded.

**Note:** This option only appears if AVV is activated for the Video Gateway (see Automatically Uploading Video to an AVV Server, page 67).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SMS** | Select this option to have the Video Gateway send SMS notifications when a video-lost event is detected. Messages are sent to the recipients specified in the SMS and E-mail screen, in the format defined there (see SMS and E-mail Notifications, page 61).

| E-mail | Select the desired type of e-mail notification, as follows:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Do not send e-mail notifications when a video-lost (or video restored) event is detected.</td>
</tr>
<tr>
<td>Text only</td>
<td>When a video-lost (or video restored) event is detected, send e-mail notifications. Include a text message in the e-mail, but do not attach any images to the message.</td>
</tr>
<tr>
<td>Text &amp; image</td>
<td>When a video-restored event is detected, send e-mail notifications that include both a text message and a picture of the first frame after video was restored.</td>
</tr>
</tbody>
</table>

**Note:** This option is not available for video-lost notifications.

**Note:** E-mail messages are sent to the recipients specified in the SMS and E-mail screen, in the format defined there (see SMS and E-mail Notifications, page 61).

**Note:** For video-restored notifications, if AVV is selected, Text & image is automatically selected for this field. A single e-mail containing both the standard notification text and the AVV notification is sent at the beginning of each event. In addition, a text-only e-mail is sent when the file transfer is completed.

**Note:** For video-restored notifications, if AVV was once selected, and has since been
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activator 1</td>
<td>Select the action that each activator should perform when a video-lost event begins:</td>
</tr>
<tr>
<td>Activator 2</td>
<td>- Turn on: Set the activator line to &quot;high.&quot;</td>
</tr>
<tr>
<td></td>
<td>- Turn off: Set the activator line to &quot;low.&quot;</td>
</tr>
<tr>
<td></td>
<td>- None: Do not change the activator’s setting.</td>
</tr>
<tr>
<td>Note:</td>
<td>For additional information about working with activators, see Configuring Sensor and Activator Settings, page 120.</td>
</tr>
<tr>
<td>Note:</td>
<td>The Activator 2 field only appears for the HVG400, MVG, and UVG400.</td>
</tr>
<tr>
<td>Go To Preset</td>
<td>All PTZ cameras connected to the Video Gateway are listed below this heading. If you want one of these cameras to automatically aim at a preset location when a video-lost event begins, beside the name of the camera, select the number of the preset location.</td>
</tr>
<tr>
<td>Note:</td>
<td>Preset locations are defined and assigned numbers using a client application such as SVMultiClient. For additional information, please refer to the relevant client application guide.</td>
</tr>
<tr>
<td>Note:</td>
<td>If no PTZ cameras are connected to the unit, this field does not appear.</td>
</tr>
</tbody>
</table>

2. Under **On Video Restored**, select the actions that the Video Gateway should perform when a video-lost event ends – when the Video Gateway begins to receive a video signal from the camera again – as described above.

## Video Recording Settings

The Video Gateway can record a video stream from each camera connected to it. Each stream is called a “recorder.” Creating a recorder allocates space on the storage media of the Video Gateway unit for the video stream that is to be recorded. Recorded video can be downloaded from the storage media for viewing and saving on the client or for viewing on a CCTV monitor (when touch/mouse is enabled).

The available space on the storage media limits how much disk space can be allocated for each recorder. You can choose what should be done when the disk space allocated for a recorder is used up: either the earliest part of the recording is discarded and overwritten by the current recording, or recording stops until you erase the recordings manually.

Video can be recorded continuously or only when triggered by events. Event-triggered recording can be used to minimize disk usage, so that more time can be covered by a recorder before its allocated disk space is used up. For example, a second of high-quality recording requires about 16 KB of disk space. For a full day of high-quality video recording, this translates into 1.3 GB of disk space. By contrast, if there are 25 events in a day, and the recorder records 20 seconds for each event, only 8 MB of disk space are needed for the day.

VMD, sensor, and activator events can function as triggers for event-triggered recording. Each recorder can be configured to respond to VMD events detected by the camera from which the recorder records or from any of the sensors connected to the Video Gateway.

When an event occurs, it is often useful to see what happened immediately before and after it. For this reason, event-triggered recording can be configured to record a set number of seconds before and after each event (“pre-record” and “post-record”). To accomplish this, the Video Gateway always records the specified number of pre-record seconds, and then discards this data if no events are detected. For example, if the pre-record is five seconds, the system always stores the last five seconds of video. If an event is detected, this video is saved as the pre-record recording. Otherwise, it is deleted. The total recording time for each event is the sum of the pre-record time, the time of the event itself, and the post-record time.

Another way you can control the disk usage is through the recording *quality* settings. The system supports three standard quality levels, high, medium, and low. The lower the quality setting, the less disk space is required for...
each second of recording. Obviously, some stream quality is lost when lower quality settings are used. All three standard quality settings produce recordings in SIF size when the unit’s video resolution is VGA and recordings in CIF size when the video resolution is D1 (see Video Resolution, page 18). High quality is the optimal recording configuration, and is recommended for use whenever possible. For information about the framerates and bitrates used for the standard quality levels, see Advanced Recorder Settings, page 107.

Configuring Video Recording

This section explains how to configure video recording settings for a camera.

**To set up video recording for a camera:**

1. In the Camera configuration screen, under Recording Type, select the desired type of recording, as follows:
   - **Continuous:** Recording takes place all the time, regardless of whether events occur or not
   - **By Event:** Recording only takes place when an event occurs
   - **None:** Recording is not activated for the camera

   If you select **By Event**, the fields required to configure the event-triggered recording are added to the screen:

   ![Figure 110: Settings for event-triggered recording](image)

   **Figure 110: Settings for event-triggered recording**

2. Under Recording Quality, select the recording quality (High, Medium, or Low).

   **Note:** For information about the data rates represented by the standard quality levels and about selecting custom recording quality settings, see Advanced Recorder Settings, page 107.

   **Note:** The percentage of available recording space that is allocated to the camera is indicated in the screen. (In the illustration above, 24% is allocated to the camera.) This value is set in the Advanced Settings. For additional information, see Advanced Recorder Settings, page 107.

3. If the recorder is event-triggered, select the triggers that will cause the recording to start:
   - **VMD:** If VMD is enabled for the camera (see Video Motion Detection (VMD), page 97), and you want VMD events to trigger event recording, select VMD.
   - **Sensor events:** If you want sensor events to trigger event recording, select the sensors you want to function as triggers. For example, select S1 to use Sensor 1 as a trigger.
   - **Activator events:** If you want activator events to trigger event recording, select the activators you want to function as triggers. For example, select A1 to use Activator 1 as a trigger.

   **Note:** VMD is not automatically selected when it is enabled. Furthermore, if none of the sensors or activators is selected, and VMD is not selected, no recording will take place.

4. If the recorder is event-triggered, fill in the pre-record and post-record values as follows:
- **Pre-record**: The number of seconds before each event that should be included in the recording of the event. Range: 0–9 seconds.
- **Post-record**: The number of seconds following each event that should be included in the recording of the event.

**CAUTION**: When you update the quality or size values in this screen, all the recorded video from this camera that is currently stored on the storage media is deleted.

### Advanced Recorder Settings

Advanced settings allow you to customize the recorder’s video quality settings. You can choose whether or not recordings are automatically erased to make room for new recordings, and set the allocation of disk space among all the recorders connected to the Video Gateway unit.

When advanced settings are activated, you can choose to record larger VGA or D1 frames, or smaller QSIF or QCIF frames, and you can select custom quality settings. Quality is defined by a bitrate/framerate pair. The following table summarizes the recommended settings and the approximate disk usage at each setting. The recommended settings for the SIF and CIF frames are the standard settings used by the system if you do not customize the settings.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Frame Size</th>
<th>High Quality</th>
<th>Medium Quality</th>
<th>Low Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VGA</strong></td>
<td>QSIF (small frame)</td>
<td>10 FPS</td>
<td>6 FPS</td>
<td>4 FPS</td>
</tr>
<tr>
<td></td>
<td>32 KBPS</td>
<td>16 KBPS</td>
<td>8 KBPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>338 MB/day</td>
<td>169 MB/day</td>
<td>84 MB/day</td>
<td></td>
</tr>
<tr>
<td><strong>SIF</strong></td>
<td>(medium-sized frame)</td>
<td>10 FPS</td>
<td>7 FPS</td>
<td>4 FPS</td>
</tr>
<tr>
<td></td>
<td>128 KBPS</td>
<td>48 KBPS</td>
<td>24 KBPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.3 GB/day</td>
<td>506 MB/day</td>
<td>253 MB/day</td>
<td></td>
</tr>
<tr>
<td><strong>VGA</strong></td>
<td>(large frame)</td>
<td>7 FPS</td>
<td>5 FPS</td>
<td>4 FPS</td>
</tr>
<tr>
<td></td>
<td>256 KBPS</td>
<td>128 KBPS</td>
<td>64 KBPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.64 GB/day</td>
<td>1.3 GB/day</td>
<td>675 MB/day</td>
<td></td>
</tr>
<tr>
<td><strong>D1</strong></td>
<td>QCIF (small frame)</td>
<td>10 FPS</td>
<td>6 FPS</td>
<td>4 FPS</td>
</tr>
<tr>
<td></td>
<td>64 KBPS</td>
<td>32 KBPS</td>
<td>16 KBPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>675 MB/day</td>
<td>338 MB/day</td>
<td>169 MB/day</td>
<td></td>
</tr>
<tr>
<td><strong>CIF</strong></td>
<td></td>
<td>10 FPS</td>
<td>7 FPS</td>
<td>4 FPS</td>
</tr>
</tbody>
</table>
## Configuring Camera Settings

### Table 1: Recommended video quality settings

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Frame Size</th>
<th>High Quality</th>
<th>Medium Quality</th>
<th>Low Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>(medium-sized frame)</td>
<td>160 KBPS</td>
<td>48 KBPS</td>
<td>24 KBPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.6 GB/day</td>
<td>506 MB/day</td>
<td>253 MB/day</td>
<td></td>
</tr>
<tr>
<td>D1 (large frame)</td>
<td>7 FPS</td>
<td>5 FPS</td>
<td>4 FPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>320 KBPS</td>
<td>256 KBPS</td>
<td>128 KBPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3 GB/day</td>
<td>2.64 GB/day</td>
<td>1.3 GB/day</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Bitrate is defined in kilobits per second (KBPS), and framerate is defined in frames per second (FPS).

**NOTE:** At times, real-time demands on system resources may make it temporarily impossible for the system to adhere to the specified quality settings. In this case, the system automatically regulates itself to ensure the best use of available resources. When necessary, it may temporarily lower the framerate of a stream slightly in order to accommodate all of its immediate processing requirements. The quality of individual frames in the stream is not reduced.

**NOTE:** VGA and D1 recording introduces extra load on the unit. Therefore, VGA recording should be used sparingly.

**CAUTION:** When you update the recorder’s frame-size settings, all the recorded video that is currently stored on the storage media is deleted.

By default, the recorders are allocated equal shares of the available disk space. If you wish, you can allocate the disk space differently. For example, if three recorders are event triggered, and the other records continuously, you may wish to allocate 20% of the disk space to the event-triggered recorders, and 75% to the continuous recorder. (It is recommended to leave approximately 5% of the disk space free for management overhead.) This allocation would maximize the recording time available for continuous recording without significantly limiting the disk space available for the recording of events.

Video storage normally follows the FIFO (first-in, first-out) model: when the disk space allocated to a recorder is full, the system automatically erases the earliest recordings from the camera to make space available for new recordings. If this is not desirable, linear recording can be implemented instead. In this case, recording ceases for the camera when the disk space allocated to it is full. Recording from the camera can only be started again after the existing recordings are manually erased (see Erasing Recorded Video, page 114). If you select linear recording, you can choose to receive e-mail notifications when the disk space is nearly full and when it is completely full. When linear recording is selected, (WP) (Write Protection) appears in the Camera Summary screen after the recording type.
**Figure 111:** (WP) indicating linear recording (Write Protection) is selected

**CAUTION:** When you update a recorder's disk allocation or size settings, all the recorded video that is currently stored on the storage media is deleted.

**NOTE:** TV-Out makes use of the same system resources as the unit’s video recorder. As a result, the global framerate available for recording is reduced somewhat when TV-Out is enabled. For additional information, see Configuring a CCTV Monitor (TV-Out), page 25.

**To set advanced recorder settings for a camera:**

1. In the bottom of the Camera configuration screen, under Recorder, select Enable Advanced Settings. The fields required to configure advanced settings are displayed along with the other recorder settings above the checkbox:

**Figure 112: Advanced recorder settings**

2. To modify the disk allocation for this recording stream, under Size on Disk, specify the proportion of the disk space to allocate for the stream, as a percent value.
The percentage that is already allocated for the other cameras is indicated above the field – for example, “33% in use by other recorders.” You can choose to allocate as much of the remaining disk space to this recorder as you wish. For example, if 33% of the total available disk space is already allocated to the other recorders, you could choose to allocate an additional 60% to this recorder. This would mean that 93% of the disk space is allocated to all the recorders together. The sum of the Size on Disk values of all the recorders cannot exceed 98.

**Note:** To modify the allocation of the other recorders, navigate to the Camera configuration screen of each recorder and modify the value in the Size on Disk field there.

**Note:** To reset all disk allocations to their default values, in the Camera Summary screen, click Set Recording Disk Size to Default.

3. If you want to record linearly, select Write Protect. The Warn When ____% Full field is added to the screen.

![Write Protect](image)

**Figure 113: Warn When ____% Full field**

If Write Protect is selected, recording continues until all the allocated disk space is full. To restart recording, you must manually erase the existing recordings (see Erasing Recorded Video, page 114).

If Write Protect is not selected, recording follows the FIFO model: when the disk allocation is full, the earliest recordings from this camera are erased to make room for new recordings. Skip to step 5.

4. In the Warn When ____% Full field, specify whether you want the Video Gateway to send warning messages via e-mail about the availability of storage space, as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No warning messages are sent.</td>
</tr>
<tr>
<td>1 – 99</td>
<td>A warning message is sent when the disk space reaches the threshold defined in this field (e.g., “90” means a message is sent when the disk space is 90% full). An additional message is sent when the disk space is entirely full and recording has ceased.</td>
</tr>
</tbody>
</table>

**Note:** Warning messages are sent to all the e-mail recipients listed in the SMS and E-mail screen (see SMS and E-mail Notifications, page 61).

5. To modify the video quality settings, adjust the values in the following fields as necessary:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Recording size | If the Video Gateway uses VGA resolution, you can choose from the following frame sizes:  
  - VGA: Large picture  
  - SIF: Medium-sized picture  
  - QSIF: Small picture  
If the Video Gateway uses D1 resolution, you can choose from the following frame sizes:  
  - D1: Large picture  
  - CIF: Medium-sized picture  
  - QCIF: Small picture  
  - For additional information, see Video Resolution, page 18. |
Configuring Camera Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Framerate | Enter the desired number of frames per second.  
**Note:** The note in parentheses above the field shows the global system framerate – the maximum number of frames the unit can process per second (from all cameras), and the maximum framerate available for this camera given the framerates that are already allocated to the other cameras in the system. |
| Bitrate | Enter the desired number of bits per second (maximum: 1500 KBPS). |

**Note:** If you select custom video quality settings that exactly match a standard setting, the standard setting is automatically selected. For example, if you select recording size SIF, framerate 10, and bitrate 128, the value of the **Recording Quality** field is automatically switched to High, and advanced settings are hidden from view.

**Note:** The quality settings you select here become the default settings for downloading live video of the size you select. For example, if you select QSIF with a framerate of 8 and a bitrate of 24, these settings become the "High" quality setting for all QSIF streams that are downloaded to client applications.

### Restoring Default Recording Settings

You can choose to restore all the recording settings to their default values. If you do this, the recording settings of all the cameras are restored to the following settings:

- **Recording Type:** Continuous
- **Recording Quality:** High
- **Write Protection:** Off
- **Advanced Settings:** Not enabled

When the default recording settings are restored, all recorded video is erased, and the storage space is allocated evenly among all of the cameras. Other configuration settings are not affected.

**To restore the default recording settings:**

1. In the **Camera Summary** screen, click **Restore Recording Settings to Default**.
You are prompted to confirm that you want to erase all the recordings and restore the disk allocation:

![Confirm restoration prompt](image)

**Note:** This prompt appears even if no recorded video exists.

2. Click **OK**. An *Update Confirmation (ATTENTION)* message appears below the **Main Menu**.

![Update Confirmation message](image)
3. Click Click here to go to Save Settings page. The Save Settings page opens. If any of the cameras were previously configured to record full-screen VGA or D1 frames, or quarter-sized QSIF or QCIF frames, a warning message is displayed. The message lists the cameras that were configured to record in these sizes; the recordings from these cameras will be erased.

![Figure 117: Warning message in Save Settings page](image)

4. Click Save Changes to System. The default recording settings are restored, and the System Restart Page screen opens:

![Figure 118: System Restart Page screen](image)

**Note:** From the time you click Save Changes to System, the existing video recordings become inaccessible. No additional recording can take place until the unit is restarted.

5. Click Restart System. The video recordings from the cameras listed are erased, and the unit restarts. Recording begins again after the unit restarts.
Erasing Recorded Video

Recorded video is normally stored on the storage media until one of the following occurs:

- The video is over-written by newer video.
- You change the recording size or disk allocation settings of one of the cameras (see Advanced Recorder Settings, page 107).

You can also erase all recorded video from the storage media manually in one of the following ways:

- Erase all recorded video from a selected camera
- Erase all recorded video from all cameras but leave the current disk allocation unchanged
- Erase all recorded video from all cameras and reset the disk allocation to its default settings

Erasing All Recorded Video from a Camera

You can choose to erase all the recorded video from a selected camera that is stored on the unit’s storage media. This is particularly useful if you have chosen to record linearly (selected Write Protect in the camera’s advanced recorder settings) and the disk space allocated to the camera is full.

To erase all recorded video from a camera:

1. In the Camera Summary screen, in the Recorder column, in the camera’s row, click Erase.

![Camera Summary Table]

- Erase recorded video from Camera 3

2. You are prompted to confirm that you want to erase the video:
Figure 120: Confirmation prompt

3. Click OK. The recordings are erased, and a confirmation message appears below the Main Menu.

Figure 121: Confirmation that recordings were erased

4. Restart the unit.

Note: No recording will take place from the camera until the unit is restarted (see Resetting the Unit, page 198).

Erasing All Recorded Video from the Storage Media

This section explains how to erase all recorded video from the unit’s storage media without changing the disk space allocated to each recorder.

To erase all recorded video from the unit’s storage media:

1. In the Camera Summary screen, click Erase Recordings. The Erase Recordings screen appears.
2. Select **Confirm Erase**, and then click **Erase**. The contents of the storage media are erased, and a **System Restart** screen is displayed.

3. Click **Restart System**. The unit restarts and recording begins again in accordance with the recording settings defined in the camera configuration. You are automatically logged out of the configuration utility, and a confirmation message appears:
Figure 124: Restart confirmation message

Note: To continue configuring the unit, click the link in the message and log into the configuration utility again.

Restoring the Default Disk Allocation

This section explains how to erase all recorded video from the unit’s storage media and, at the same time, restore the disk space allocation to its default settings.

To restore the default disk allocation:

1. In the Camera Summary screen, click Set Recording Disk Size to Default.

You are prompted to confirm that you want to erase all the recordings and restore the disk allocation:
Configuring Camera Settings

Figure 126: Confirm disk reallocation prompt

2. Click **OK**. An **Update Confirmation** (ATTENTION) message appears below the **Main Menu**.

![ATTENTION][1]

**ATTENTION**
RECORDER SET TO DEFAULT SIZE

![ATTENTION][1]

> CLICK HERE TO GO TO SAVE SETTINGS PAGE

**Figure 127: Update Confirmation message**

3. Click “Click here to go to Save Settings page.” The **Save Settings** page opens, with a warning message displayed:

![Warning message in Save Settings page][2]

**Figure 128: Warning message in Save Settings page**

4. Click **Save Changes to System**. The default disk allocation is restored, and the **System Restart Page** screen opens:

![System Restart Page][3]
Figure 129: *System Restart Page screen*

**Note:** From the time you click *Save Changes to System*, the existing video recordings become inaccessible. No additional recording can take place until the unit is restarted.

5. Click **Restart System**. The existing video recordings are erased, and the unit restarts. After the unit restarts, recording begins again.
Configuring Sensor and Activator Settings

Sensors are devices that detect events such as a door being opened or a light being turned on. Activators are external devices such as alarms and lights that can be turned on when a sensor is activated.

One sensor and one activator can be connected to MVG200, CVG, and CVG-M models. Up to four sensors and two activators can be connected directly to the MVG 400 and UVG400 models, and up to six sensors and two activators can be connected directly to the HVG400.

Up to 16 additional sensors can be connected to Video Gateway units through an ADAM module. Alternatively, additional sensors and activators can also be connected using an IA relay board, but they cannot be configured through the Video Gateway’s configuration utility. For additional information about connecting ADAM modules and IA relay boards, please refer to your unit’s installation guide.

**NOTE:** None of these devices – sensors, activators, ADAM module, or IA relay board – are supplied with the Video Gateway.

In addition, mobile Video Gateways contain built-in sensors that can notify you when vehicles deviate from their prescribed routes, speed, or remain stationary for lengthy periods of time. Some models also support an optional built-in G-Force sensor that is sensitive to extreme or sudden motion and can be used to detect crashes and wild driving.

The Video Gateway can be configured to perform any or all of the following actions when a connected or built-in sensor detects an event or when an activator is activated:

- Record a camera’s video stream (see *Video Recording Settings*, page 105)
- Upload video of the event to an FTP server on the internet (see *Automatically Uploading Video to an AVV Server*, page 67). If e-mail notification recipients are defined in the *SMS and E-mail* screen, an e-mail message is sent to all the recipients when the event begins and a second e-mail is sent when the video is successfully uploaded and is available for downloading by users. The e-mail notification includes a link to the video file on the server and a picture of the event.
- Upload snapshots of the event to an FTP server on the internet (see *FTP Server Settings*, page 75).
- Send Sensor event notifications to the SMS and/or e-mail recipients defined for the system (see *SMS and E-mail Notifications*, page 61). E-mail notifications can optionally include a picture of the event, and, if AVV is activated, a link to video of the event.
- Turn an activator on or off (sensor events only)
- Move any PTZ camera connected to the Video Gateway that supports presets to a preset location (sensor events only)
- Switch to a different outline
- Change the display on a CCTV monitor

These actions can be performed when a sensor becomes active and/or when it becomes inactive. For example, you can configure a sensor such that an SMS notification is sent and an alarm is turned on when it is activated, and the alarm is turned off but no notification is sent when the sensor becomes inactive.

Configuring Sensors and Activators

The **Sensor Summary** screen summarizes the current settings of each sensor and activator in the system, and provides links to the sensor and activator configuration screens, in which these settings can be modified.
Each sensor and activator in the system is configured in its own configuration screen. The configuration screens are accessed from the Sensor Summary screen. Sensors connected to the unit through an ADAM module appear as "External Sensors." They are configured in the same way as sensors connected directly to the unit.

NOTE: External sensors can only be enabled and configured if ADAM Sensors is enabled in the General System Settings screen (see Configuring General System Settings, page 21).

To open the Sensor Summary screen:

- In the Main Menu, click Sensors.

To configure a sensor or activator:

1. In the Main Menu, under Sensors, click the sensor or activator (e.g., Sensor #1 to configure the sensor plugged into In1). The relevant Sensor or Activator configuration screen opens:
2. Select the **Enabled** checkbox. The fields required to configure the sensor or activator settings are added to the screen.

![Sensor configuration screen](image)

*Figure 131: Sensor configuration screen*

![Sensor enabled](image)

*Figure 132: Sensor enabled*
Figure 133: Activator enabled

Note: If Enabled is not selected, the sensor cannot function as an event trigger and will not appear in client applications.

Note: If a sensor is not physically connected to the Video Gateway but is enabled in the Sensor screen, false alarms may be generated.

3. Fill in the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activator Type</strong></td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td><strong>(Activators only)</strong></td>
<td>- <strong>Normal</strong>: An activator is connected to this activator connector on the unit.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Recording Status</strong>: Use this activator to indicate whether video recording is taking place at the moment or not. When it is taking place, the activator appears as &quot;on&quot; in the client application; if no recording is taking place, for any reason (e.g., the cameras are not configured to record continuously, the video signal is lost, or there is a problem with the storage medium), the activator appears as “off.” If a LED is connected to the activator connector on the Video Gateway, the LED will be turned on whenever recording is taking place.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Bypass</strong>: This activator connector on the unit is being used as a switch for the power supplies of other devices connected to the unit (see Configuring an Activator as a Power Switch, page 128).</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>If you select <strong>Recording Status</strong> or <strong>Bypass</strong>, the rest of the fields in the Activator configuration screen are hidden, because they are not relevant.</td>
</tr>
<tr>
<td><strong>Sensor Name / Activator Name</strong></td>
<td>Assign a name to the device (up to 20 characters). Each device must have a different name. The names are used when you view the video via a remote client such as SVMultiClient and in e-mail and SMS notifications.</td>
</tr>
<tr>
<td><strong>Polarity</strong></td>
<td>Select <strong>Reverse</strong> if the normal, inactive state of the sensor is closed – if it is activated from on to off.</td>
</tr>
<tr>
<td><strong>(Sensors only)</strong></td>
<td><strong>Note</strong>: Sensors are either designed to activate from “off to on” (normally open, or standard polarity) or from “on to off” (normally closed, or “reverse polarity”) when an event occurs. Consult the device’s manual to determine its normal state.</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>This field is equivalent to the &quot;Normal Status&quot; field for activators.</td>
</tr>
<tr>
<td><strong>Normal Status</strong></td>
<td>Select the normal, inactive state of the activator.</td>
</tr>
<tr>
<td><strong>(Activators only)</strong></td>
<td><strong>Note</strong>: Activators are either designed to activate from “off to on” (normally open) or...</td>
</tr>
</tbody>
</table>
Field | Description
---|---
| from "on to off" (normally closed) when an event occurs. Consult the device's manual to determine its normal state. **Note:** This field is equivalent to the "Polarity" field for sensors.

| Attach Cameras | Select the cameras to which the device should be linked, if desired. Selecting a camera has the following effects:
|---|---
| • You will be able to configure e-mail notifications of events that were triggered by this device to include images.
| • If you activate AVV for the device, video of events from each of the selected cameras is uploaded to the AVV server.
| • If you activate FTP for the device, snapshots of events from each of the selected cameras are uploaded to the FTP server.
| **Note:** If the camera is configured to record by event, attaching it to a device here does not automatically mean that the device is a trigger that activates recording. The device must be selected as one of the recorder triggers in the camera configuration for this to occur. If it is not selected as a trigger, the Video Gateway may not record the event, and therefore it will not be possible to upload it to the AVV server. For information about defining recorder triggers, see **Configuring Video Recording**, page 106.
| • Events from the device will appear in the client interface under the selected camera as well as under the device. This makes it possible to play back video of the event by dragging and dropping it into a camera pane in SVMultiClient.

4. Under **Notifications**, under **When Sensor On** or **On Activator Activated**, specify the actions that should be performed when the device triggers an event, as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| AVV | Select this option to have the Video Gateway send video of the event to an AVV server for downloading. The video is downloaded to the site defined in the AVV screen, in the format defined there (see **Automatically Uploading Video to an AVV Server**, page 67), and e-mail notifications are sent to all e-mail recipients (see **SMS and E-mail Notifications**, page 61).
| **Note:** Two e-mail notifications are sent – one when the event is first detected, and the other when uploading of the video to the AVV server is completed. Thus, the video clip may not be available yet when you receive the first e-mail notification.
| **Note:** This feature only works if the device is attached to a camera and recording (either event-triggered or continuous) is activated for the camera (see **Video Recording Settings**, page 105).
| **Note:** This option only appears if AVV is activated for the Video Gateway (see **Automatically Uploading Video to an AVV Server**, page 67).

| SMS | Select this option to have the Video Gateway send SMS notifications when the device triggers an event. Messages are sent to the recipients specified in the SMS and E-mail configuration screen in the format defined there (see **SMS and E-mail Notifications**, page 61).

| E-mail | Select the desired type of e-mail notification, as follows:
| --- | ---
| • **None:** Do not send e-mail notifications when an event is detected.
| • **Text only:** When an event is detected, send e-mail
### Field | Description
--- | ---
 |  
notifications. Include a text message in the e-mail, but do not attach any images to the message.  
- **Text & image:** When an event is detected, send e-mail notifications that include both a text message and a picture of the first frame of the event. If multiple cameras are attached to the device, a separate e-mail is sent for each camera. If no cameras are attached to the device, no e-mails are sent.  

**Note:** E-mail messages are sent to the recipients specified in the **SMS and E-mail** screen, in the format defined there (see *SMS and E-mail Notifications*, page 61).

**Note:** If **AVV** is selected, **Text & image** is automatically selected for this field. A single e-mail containing both the standard notification text and the AVV notification is sent at the beginning of each event. In addition, a text-only e-mail is sent when the file transfer is completed.

**Note:** If **AVV** was once selected, and has since been cleared, **Text & image** remains selected for this field until the selection is changed manually. If it is not changed, AVV is not activated, but notifications with snapshots are sent at the beginning of each event.

| Activator 1  
| Activator 2 (Sensors only)  
 | Specify the action that each activator should perform when the sensor triggers an event, as follows:  
- **Turn on:** Set the activator line to "high."  
- **Turn off:** Set the activator line to "low."  
- **None:** Do not change the activator’s status.  

**Note:** These settings are not available for activators.

**Note:** The **Activator 2** field only appears for the HVG400, MVG, and UVG400.

| Load Outline (Sensor 1 only)  
 | If Sensor 1 is a toggle switch that will be used to switch outlines, select **Enabled**, and then follow the instructions under *Configuring Sensor 1 to Switch Outlines*, page 126.

**Note:** This option only appears if **Outline Switching** is set to **Sensor** in the **General Settings** screen (see page 23) and if more than one outline is enabled in the unit’s configuration (see *Defining Alternate Outlines*, page 150).

| TV-Out Display Switch (HVG400: Sensor 6 only; MVG and UVG400: Sensor 4 only; CVG and CVG-M: Sensor 1)  
 | If a push-button switch connected to this sensor connector will be used to change the display on a CCTV monitor connected to the unit, select this option. For additional information, see *Configuring a Sensor to Control CCTV Display*, page 127.

**Note:** This option only appears if **Display Switch Via Sensor** is enabled in the **TV-Out** screen (see *Configuring a CCTV Monitor (TV-Out)*, page 25).

| Presets (Sensors only)  
 | All PTZ cameras connected to the Video Gateway that support presets are listed below this heading. If you want one of these cameras to automatically aim at a preset location when a sensor event begins, beside the name of the camera, select the number of the preset location.

**Note:** Preset locations are defined and assigned numbers using a client application such as SVMultiClient. For additional information, please refer to the relevant client application guide.
5. Under Notifications, under When Sensor Off or On Activator Deactivated, specify the actions that should be performed when an event ends, as described above.

6. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

### Configuring Sensor 1 to Switch Outlines

A toggle switch can be connected to the In1 connector on the Video Gateway instead of a sensor. The switch can be used to toggle between two outlines. For example, if an MVG is installed in a bus, when the bus is parked in the lot, the “Parked” outline – which activates sensors, notifications, and event-triggered recording – can be loaded. When the bus driver begins driving, he or she can flick the switch to load the “Driving” outline, in which sensors and most notifications are deactivated, and recording is continuous.

**NOTE:** This feature can only be activated in the Sensor 1 configuration screen if it is first enabled in the General System Settings screen (see General System Settings, page 17).

**NOTE:** In some cases, an alarm panel may be connected to In1 instead of a toggle switch. In this case, the alarm can perform the same function as the toggle switch – when the alarm is turned on or off, it automatically toggles the active outline as well. For additional information, please refer to the installation guide or consult your vendor.

**To configure Sensor 1 as an outline switch:**

1. In the Main Menu, under Sensors, click Sensor 1. The Sensor #1 configuration screen opens.

2. Select the Enabled checkbox. The fields required to configure the sensor settings are added to the screen.

3. Under When Sensor On, under Load Outline, select Enable. The Outline field is added to the screen.

---

**Figure 134: Sensor #1 configuration screen**

*Note:* Every time the outline is switched, a sensor event is triggered. If notification settings are activated, notifications will be triggered each time the display is changed. For additional information about configuring the notification settings, see Configuring Sensors and Activators, page 120.
4. In the dropdown list, select the name of the outline you want to load when the toggle switch is turned on.

5. Under **When Sensor Off**, under **Load Outline**, select the name of the outline you want to load when the switch is turned off, as described in steps 3–4.

6. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).

### Configuring a Sensor to Control CCTV Display

You can use one of the sensor connectors on the Video Gateway unit to connect a push-button switch to the unit. If a monitor is connected to the Video Gateway, the switch can then be used to change the display in the CCTV monitor. With each press of the button, the display cycles to the next display type, in the following order:

- **Split screen**: The screen is divided into four parts, and live video from each camera is displayed in one of the parts.
- **Camera 1**: Full-screen display of live video from Camera 1
- **Camera 2**: Full-screen display of live video from Camera 2
- **Camera 3**: Full-screen display of live video from Camera 3 (HVG400, MVG, UVG400 only)
- **Camera 4**: Full-screen display of live video from Camera 4 (HVG400, MVG, UVG400 only)
- **Rotate**: Full-screen display that cycles from one camera to the next. (The rotation delay is defined in the **TV-Out Settings** screen; see **Configuring a CCTV Monitor (TV-Out)**, page 25.)
- **None**: A digital clock is displayed, and no video is displayed.

Only one sensor connector can serve this purpose on each unit. The appropriate sensor connector for each model is:

- **HVG400**: In6 (Sensor 6)
- **MVG, UVG400**: In4 (Sensor 4)
- **CVG, CVG-M**: In1 (Sensor 1 – the only sensor connector)

**NOTE:** This feature can only be activated in the relevant **Sensor** configuration screen if it is first enabled in the **TV-Out** screen (see **Configuring a CCTV Monitor (TV-Out)**, page 25).

**NOTE:** On CVG and CVG-M models, this feature should not be used if the sensor is configured to trigger outline-switching.
To configure a sensor as a CCTV display switch:

1. In the Main Menu, under Sensors, click the appropriate sensor (see above). The Sensor configuration screen opens.

2. Select the Enabled checkbox. The fields required to configure the sensor settings are added to the screen.

   ![Figure 137: Sensor #4 configuration screen (MVG, UVG)](image)

   **Note:** Every time the CCTV display is switched, a sensor event is triggered. If notification settings are activated, notifications will be triggered each time the display is changed. For additional information about configuring the notification settings, see Configuring Sensors and Activators, page 120.

3. Select the TV-Out Display Switch checkbox.

4. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

Configuring an Activator as a Power Switch

When a Video Gateway is installed in a vehicle, the cameras and other peripheral devices connected to it usually receive their power directly from the vehicle battery. Normally, the Video Gateway is configured to shut down whenever the vehicle ignition is turned off. Because the peripheral devices do not draw their power from the Video Gateway, they will keep drawing power from the vehicle battery even when the Video Gateway is off. To cause these devices to shut down when the vehicle ignition is turned off, their power supplies can be routed through an activator connector on the unit. When this is done, the activator must be configured to cut off the power supply that is routed through it when the ignition turns off.

To configure an activator as a power switch:

1. In the Main Menu, under Sensors, click the appropriate activator (e.g., Activator #1 if Out1 is being used as the power switch). The Activator configuration screen opens.

2. Select the Enabled checkbox. The fields required to configure the activator settings are added to the screen.

3. Under Activator Type, select Bypass. (All of the other fields in the screen are hidden, because they are not relevant when the activator connector is used in this way.)
4. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

## Configuring Vehicle-Behavior Sensors

Mobile Video Gateway units contain special sensors that can notify you of potentially problematic vehicle behavior on the road: straying from the planned route, speeding, remaining in one location for extended periods of time, and erratic motion.

### Configuring a Geo-Fence Sensor

The geo-fence sensor triggers an event if the vehicle strays from its prescribed route or the region in which it is supposed to remain. It can do this in one of two ways:

- **GPX file:** The system compares the GPS coordinates of the vehicle's current location with those of a region that is defined in a geo-fence (GPX) file. The GPX file can be created using Bing maps and uploaded to the Video Gateway.

- **Perimeter limitation:** The system checks the GPS coordinates of the vehicle's current location to see if it has strayed more than a specified distance from a particular location.

### Creating a GPX File

If you want to define the boundaries of the region in which the vehicle should remain, you must begin by creating a GPX file – an XML file containing the GPS coordinates that define the region.

The easiest way to create a GPX fence file is to use the My Places feature of Bing Maps (http://www.bing.com/maps/). Bing provides two different ways to select the region you want to define in the fence file:

- **Route:** A list of GPS coordinates that define a path from one place to another (a series of line segments created by connecting the coordinates)

- **Area:** A list of GPS coordinates that define the boundaries of a region (a closed shape created by connecting the coordinates on the map)
To create the GPX file in Bing, you mark routes and/or areas on the map. The Bing system stores the GPS coordinates of the routes and areas as "places" in your My Places. When you have marked all of the routes and areas that define the intended range of the vehicle, you can export the information and save it in a GPX file.

NOTE: In GPX syntax, the only real difference between a route and an area is that the first and last coordinates of an area are identical (the last segment closes the polygon), but those of a route are not.

You can save any number of routes and areas in a single GPX file. You can also import routes and areas from more than one GPX file to your Video Gateway, so feel free to create as many GPX files as you find convenient. For example, if your company has two standard delivery routes, you could create a separate file for each of the delivery routes.

NOTE: The following procedure briefly explains how to use Bing to create a GPX file that defines the routes and areas you want to include in your geo-fence area. For complete instructions about how to use the Bing map service, please refer to the Bing documentation.
To create a GPX file using Bing maps:

1. In a browser, open the Bing maps site (http://www.bing.com/maps/) and display the part of the map that represents the region in which the vehicle will be travelling. Zoom in so that you can see the features you want to mark on the map (e.g., roads and towns).

   **Note:** It is recommended to log into Bing before marking routes and areas on the map. Logging in enables you to create lists of places and save them. If you do not have an account, you can create one. To create an account or log into an existing account, in the upper-right corner of the page, click **Sign in**, and then select **Microsoft Account**.

2. On the left side of the page, click **My Places**. The My Places editor opens on the right side of the page.

   ![My Places editor](image)

   **Figure 143: My Places editor**

3. At the bottom of the window, click ![ ](image) to define a route, or ![ ](image) to define an area.

4. In the map, click where you want to begin drawing the route or area, and then move your mouse cursor along the line you want to draw, clicking every time you want to change direction.

   **Note:** If it is difficult to draw the entire route at one time, you can draw it in parts, and include all of the parts in the GPX file. As long as you upload all of the parts to the Video Gateway (see *Uploading Polygons from a GPX File*, on page 134) and include them all in a single itinerary (see *Creating an Itinerary*, page 137), it does not matter if the route is split into parts when you draw it.
Figure 144: Drawing a route

Figure 145: Drawing an area

5. When you get to the last point you want to include in the area or route, double-click the point. An Edit pushpin properties dialog box opens.
6. Under **Title**, enter a name for the item, and then click **Save**. The item is saved in the *Unsaved places* list. **Note:** Do not include any spaces in the name.

7. Repeat the steps above as many times as necessary in order to create all of the routes and areas you want to include in the geo-fence. The items are all saved in the *Unsaved places* list.

8. In the My Places editor, click the **Actions** menu, select **Export**, and then select **GPX**. A dialog box opens.
Configuring Sensor and Activator Settings

9. Select **Save File**. A Windows *Save File* dialog box opens.

10. Navigate to the folder in which you want to save the file, modify the default name of the file if you wish, and then click **Save**. The GPX file is saved.

### Uploading Polygons from a GPX File

Once you have created a GPX file with the routes and areas – the *polygons* – you want to include in the geo-fence boundaries, you can upload the polygons it defines to the Video Gateway. For this purpose, you must use the *Remote Route Selection* utility, which you can open either from SVMultiClient or from SVControlCenter.

**NOTE:** To open the *Remote Route Selection* utility, the client application (SVMultiClient or SVControlCenter) must connect to the Video Gateway with a user account that has full client and configuration permissions. For additional information about user account permissions, see *Authentication*, page 60.

> **To open the Remote Route Selection utility in SVMultiClient:**

1. Connect to the Video Gateway. (For additional information, see *Opening the Configuration Utility*, page 8.)

2. In the **Connection Panel**, expand the Video Gateway.

3. Right-click the GPS device ( ), and select **Extended GPS Controls**. The *Remote Route Selection* utility opens.

---

*Figure 148: Exporting items to a GPX file*
To open the **Remote Route Selection utility in SVControlCenter**:  

1. Make sure SVControlCenter is connected to the Video Gateway. (For additional information, please refer to the SVControlCenter User Guide.)  
2. In the right panel, select the **Maps** tab. The GPS map opens in the right panel, and the GPS tab opens in the left panel.  
3. In the left panel, expand the Video Gateway. The sensors connected to it are listed, and a marker 📍 indicating the current location of the Video Gateway appears on the map.  
4. In the left panel, right-click the GPS sensor, and then select **Extended GPS Controls**. The **Remote Route Selection** utility opens (see figure 150).  

**Note:** Alternatively, in the map, right-click the Video Gateway marker, and then select **Extended GPS Controls** to open the **Remote Route Selection.**
To upload routes and areas from a GPX file to a Video Gateway:

2. Navigate to the GPX file and select Open. The routes and areas it contains are loaded into the utility.
3. Click the Polygons field. The routes and areas defined in the GPX file are listed.
4. Select a polygon you want to upload to the Video Gateway.
5. If the polygon you selected is an area, click Add as Fence. If it is a route, click Add as Route. The polygon is uploaded, and, after a moment, a confirmation message appears.
Figure 153: Confirmation message

6. Click OK. The message closes.

7. Repeat steps 4-5 for each of the polygons you want to upload to the Video Gateway.
   
   **Note:** Each polygon is uploaded to a separate file. To see a list of the geo-fencing files that are currently stored on the Video Gateway, in the upper left of the window, click Query files on unit. For additional information, see Activating a Geo-Fence, on page 138.

8. When you have uploaded all of the polygon files you need, click Reset System. The unit restarts, and a confirmation message appears.

Figure 154: Restart confirmation message

9. Click OK.
   
   **Note:** The Remote Route Selection utility remains open when the unit is restarting. When the unit is running again, you can continue to configure the geo-fencing without reopening the utility.

Creating an Itinerary

Once you have uploaded a polygon to the Video Gateway, you can activate it as the current geo-fence. If the vehicle strays from the region the polygon represents, a geo-fence event is triggered.

If you want to include a number of polygons in the geo-fence region, you can create an itinerary. An itinerary is a collection of polygons that together define a single geo-fence area. For example, if your Video Gateway is installed in a truck that travels between Philadelphia and New York, making stops in Trenton along the way, you could create an itinerary that includes the Philadelphia, Trenton, and New York regions, as well as the routes the truck follows to travel between them. If you then activate the itinerary as the current geo-fence, all the areas in the three regions, as well as those along the routes between them, are merged to create the geo-fence area. Only if the truck is outside of all of those areas is a geo-fence event triggered.

If you wish, you can create multiple itineraries, and store them on the Video Gateway unit. But only one itinerary can be active at a time.

**To create an itinerary:**

1. In the Remote Route Selection utility, in the Create Itinerary section, under Name, enter a name for the itinerary.
   
   **Note:** Do not include any spaces in the name.

2. Under Polygons in itinerary, list all of the polygons you want to include in the itinerary. Separate the polygons with commas, and do not add spaces before or after the commas.
3. Click Add. The itinerary is saved on the Video Gateway, and a confirmation message appears.

![Figure 155: Creating an itinerary](image)

To see the itinerary in the list of geo-fencing files that are on the Video Gateway, in the upper left of the window, click Query files on unit. For additional information, see Activating a Geo-Fence, below.

**Activating a Geo-Fence**

Once the polygons and itineraries are uploaded to the unit, you can select one of them to activate. Geo-fence events will be triggered whenever the vehicle strays from the region defined by the active item.

**NOTE:** There is a 30-second grace period before a geo-fence event is triggered. That is, the vehicle must be outside of the geo-fence for at least 30 uninterrupted seconds for the event to be triggered, and be back in the geo-fence area for 30 uninterrupted seconds in order for the geo-fence event to end. This grace period exists in order to ensure that GPS position-skew and minor mismatches between the maps and the terrain do not cause false alarms.

To activate a fence, route, or itinerary:

1. In the Remote Route Selection utility, in the upper left of the window, click Query files on unit. A dialog box opens and displays a list of the files, their types (“R” for route, “F” for fence, and “I” for itinerary), and the number of GPS points they contain. In addition, if one of the files is active, it appears under current.
2. Click OK. The dialog box closes.

3. In the Files dropdown list, select the item you want to activate.

   ![List of geo-fence files on the Video Gateway](image)

   **Figure 157: List of geo-fence files on the Video Gateway**

4. Select Set active file. The selected geo-fence boundary is activated, and a confirmation message appears.

   ![List of geo-fencing files displayed](image)

   **Figure 158: List of geo-fencing files displayed**

   **Note:** In the list, the names of the fences and routes are followed by their type (either “fence” or “route”) and the number of points there are in the polygons that describe them. The names of the itineraries are followed by their type (“itinerary”) and the number of polygons they contain.

   **Note:** This list is not updated automatically when you upload files to the Video Gateway or erase files from it. It is only updated when **Query files on unit** is selected.

   4. Select Set active file. The selected geo-fence boundary is activated, and a confirmation message appears.
Figure 159: Activation confirmation message

Note: Geo-fence events will only be triggered if the Video Gateway’s geo-fence sensor is enabled and configured (see Configuring the Geo-Fence Sensor Settings, page 140).

Defining a Perimeter Limit

Instead of defining the geo-fence boundaries by defining polygons using a GPX file, you can define geo-fencing boundaries by specifying a radius from the current location of the vehicle. For example, if a delivery truck makes deliveries within 50 km. of the parking yard, you could define the geo-fence boundaries as 50 km. from the yard in any direction. Note that the center of the geo-fence perimeter is set based on where the Video Gateway is the moment you click the Set Perimeter button. Make sure the vehicle is in the correct location when you click this button.

NOTE: If you have already set a geo-fence region using a GPX file, when you select the Set Perimeter button, the perimeter settings replace the previously defined region settings. That is, the two options are mutually exclusive; the geo-fence boundaries can be set either by creating the region using a GPX file or by setting a perimeter, but both options cannot be active at the same time. Whichever option was selected last is the one that is implemented.

To define the geo-fence boundaries by setting a perimeter:

1. In the Remote Route Selection utility, in the text field beside the Set Perimeter button, enter the radius of the perimeter, in meters. That is, if the vehicle is supposed to go no further than 50 km., in any direction, from its current location, enter “50,000.”

2. Click Set Perimeter. The perimeter is activated, and a confirmation message appears.

Figure 160: Perimeter confirmation message

Note: Geo-fence events will only be triggered if the Video Gateway’s geo-fence sensor is enabled and configured (see Configuring the Geo-Fence Sensor Settings, page 140).

Configuring the Geo-Fence Sensor Settings

In order to make effective use of the geo-fence feature, you must configure the sensor and the Video Gateway to respond to geo-fence events. This includes two types of settings:

- **Off-route tolerance**: How far the vehicle must go outside the geo-fence region before an event is triggered
- **Handling of events**: Notification settings
NOTE: You can configure these settings before you activate the geo-fence boundaries. If no boundaries are active, no events will be generated, but the settings will be saved in the system and applied when you use the Remote Route Selection utility to activate boundaries.

To configure the geo-fence sensor settings:

1. In the configuration utility, in the Main Menu, under Sensors, click Geo Fence. The GeoFence configuration screen opens. If a geo-fence file is activated, its name appears under Fence File Used.

2. Select the Enabled checkbox. The fields required to configure the settings are added to the screen.

3. Under Off-Route Tolerance, enter how far outside the geo-fence boundaries the vehicle can go without triggering an event. If the vehicle goes beyond this limit, the sensor will trigger a geo-fence event.

4. Under Attach Cameras, select the cameras to which the Geo Fence sensor should be linked. For additional information about attaching cameras to a sensor, see Attach Cameras, page 124.

5. In the Notifications section, select the actions you want the Video Gateway to perform when a geo fence event is triggered. For additional information about configuring the notification settings, see Configuring Sensors and Activators, page 120.

6. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

Viewing the Current Geo-Fence Mode and Geo-Fence Events

Once you have configured geo-fencing as explained above, you can see its current status in either SVMultiClient or SVControlCenter. In addition, you can see if any sensor events were generated.

The current status of the geo-fence sensor has two parts:

- Sensor mode: Disabled, fence enabled, or perimeter enabled
- Sensor state: On (the vehicle is outside of the region defined by the current geo-fence) or off (the vehicle is within the region defined by the current geo-fence)

The mode of the sensor is indicated by color-coding:
• **Black:** The geo-fence sensor is disabled.
• **Blue:** Fence mode is active.
• **Red:** Perimeter mode is active.

The state of the sensor is indicated by the icon of the GF/Perim sensor, as explained below.

### Mode and State Indicators in SVMultiClient

In SVMultiClient, the current mode and state are indicated as follows:

- In the left panel, the icon of the GPS sensor is indicates the current mode: ✅ indicates that Fence mode is active, 🔴 indicates that Perimeter mode is active, and ❌ indicates that geo-fencing is disabled.
- In the left panel, the icon of the GF/Perim sensor indicates the current state: 🔴 indicates the sensor is on (i.e., the vehicle is outside the fence area) and ⬅️ indicates the sensor is off (i.e., the vehicle is within the fence area).

![Figure 162: Blue GPS icon indicating Fence mode is active](image)

- In the GPS map, the icon marking the current location of the vehicle is also color-coded to indicate the current mode (📍, 🚪, or 🔴).
Mode and State Indicators in SVControlCenter

In SVControlCenter, the current mode and state are indicated as follows:

- In the left panel, the icon of the GPS sensor is indicates the current mode: • indicates that Fence mode is active, • indicates that Perimeter mode is active, and • indicates that geo-fencing is disabled.

In addition, if the left panel is open with the GPS tab selected, the name of the Video Gateway is also color coded, and the mode appears in parentheses beside the name.

---

**Figure 163: Blue location icon indicating Fence mode is active**

**Figure 164: Blue GPS icon indicating Fence mode is active**
In the left panel, the icon of the GF/Perim sensor indicates the current state: 
indicates the sensor is on (i.e., the vehicle is outside the fence area) and 
indicates the sensor is off (i.e., the vehicle is within the fence area).

In the GPS map, the icon marking the current location of the vehicle is also color-coded to indicate the current mode ( , , or ).

Figure 165: Blue location icon indicating Fence mode is active

Switching Between Geo-Fence Modes

Once you have configured geo-fencing as explained above, you can quickly turn it on or off, or switch from Fence mode to Perimeter mode, without opening the Remote Route Selection utility. You can do this in either SVMultiClient or SVControlCenter.

When you activate Fence mode in this way, the boundaries of the region are set to the current active file. To find out which file is active, you can either open the Remote Route Selection utility or the Geo Fence configuration screen in the unit's configuration utility (see Configuring the Geo-Fence Sensor Settings, page 140).

When you activate Perimeter mode in this way, the limit is set to the last perimeter value that was implemented in the Remote Route Selection utility (see Defining a Perimeter Limit, page 140). If no perimeter value was ever set, a default value of 500 meters is used.

Changing the mode of the geo-fencing is treated as a GPS event. Therefore, every mode change appears under the GPS sensor when the sensor is expanded.

Figure 166: Geo-fence mode-change events listed under the GPS sensor

To switch the geo-fence mode:

- In either SVMultiClient or SVControlCenter, in the left panel, right-click the GPS sensor, and then select the mode, as follows:
• **Switch Off All Advanced Features**: Disable geo-fencing
• **Switch to Geo Fence Mode**: Activate Fence mode with the boundaries defined in the active fence file
• **Switch to Perimeter Mode**: Activate perimeter mode with the radius that was last defined in the **Remote Route Selection** utility

---

**Figure 167**: Selecting a geo-fencing mode in SVMultiClient

**Figure 168**: Selecting a geo-fencing mode in SVControlCenter

---

### Modifying Geo-Fence Settings

If you want to change the active fence file or the perimeter limit, you can do so in the **Remote Route Selection** utility.

**To modify geo-fence settings:**

1. In either SVMultiClient or SVControlCenter, open the **Remote Route Selection** utility.
2. Select **Cancel GEOF/PERRIM**. The geo-fence sensor is disabled, and a confirmation message appears.

3. Click **OK**. The message closes.

4. Modify the settings as required.
   
   **Note:** Follow the instructions above to upload new polygon files (see p. 134), create a new itinerary (see p. 137), activate a different geo-fence (see p. 138), or define a new perimeter limit (see p. 140).

5. When you have finished, click **Exit** to close the **Remote Route Selection** utility.

### Erasing Geo-Fences from the Unit

If you no longer need to use route, area, or itinerary files that are stored on the Video Gateway, you can erase them. You can erase individual files one at a time or all of the files at one time.

#### To erase an individual route, area, or itinerary file from the Video Gateway:

1. In the **Remote Route Selection** utility, in the upper left of the window, click **Query files on unit**. The list of geo-fencing files is refreshed.

2. Click the **Files** field. The list of geo-fencing files is displayed (see figure 158).

3. Select the item you want to erase, and then select **Erase**. The item is erased, and a confirmation message appears.

   ![Figure 169: Erasure confirmation message](image)

#### To erase all the route, area, and itinerary files from the Video Gateway:

1. In the **Remote Route Selection** utility, in the upper left of the window, click **Query files on unit**. The list of geo-fencing files is refreshed.

2. Select **Erase all files**. The items are erased, and a confirmation message appears.

   ![Figure 170: Erasure confirmation message](image)

### Configuring a Speed-Limit Sensor

The Speed-Limit sensor triggers an event if the speed of the vehicle exceeds the rate you specify.

#### To configure the Speed-Limit sensor:

1. In the **Main Menu**, under **Sensors**, click **Speed Limit**. The **Speed Limit Alert** configuration screen opens.
2. Select the Enabled checkbox. The fields required to configure the settings are added to the screen.

![Figure 171: Speed Limit Alert screen](image)

3. Under Maximum Speed, select the highest speed the vehicle can go without triggering an event. If the vehicle goes faster than this speed, the sensor will trigger a speeding event.

4. Under Attach Cameras, select the cameras to which the Speed-Limit sensor should be linked. For additional information about attaching cameras to a sensor, see Attach Cameras, page 124.

5. In the Notifications section, select the actions you want the Video Gateway to perform when a speeding event is triggered. For additional information about configuring the notification settings, see Configuring Sensors and Activators, page 120.

6. Click Update, and then save the settings. They will be implemented after the unit is restarted (see Saving Configuration Changes, page 157).

Configuring an Idle Monitor

The Idle Monitor sensor triggers an event if the vehicle remains in one location for longer than a given period of time. You can define both the length of time and a how close to the initial location the vehicle must be in order to be considered to have remained in the initial location. Thus, for example, if the trucks in your system are not expected to remain in any one location for longer than 15 minutes, you could configure the sensor to trigger an event if the truck remains within 500 meters of the same location for more than 15 minutes.

To configure the Speed-Limit sensor:

1. In the Main Menu, under Sensors, click Idle Monitor. The Idle Monitoring configuration screen opens.

2. Select the Enabled checkbox. The fields required to configure the settings are added to the screen.
Configuring Sensor and Activator Settings

Figure 172: Idle Monitoring screen

3. Under **Maximum Idle Time**, enter the longest amount of time the vehicle can remain in one place without triggering an event, in minutes. If the vehicle remains in any location longer than this amount of time, the sensor will trigger an event.

4. Under **Idle Distance Radius**, enter the maximum distance from any initial location that the vehicle can move and still be considered to be in one location. If the vehicle moves more than this distance from any location, the idle monitor resets and begins calculating the idle time from the next time the vehicle stops.

5. Under **Attach Cameras**, select the cameras to which the Idle Monitor should be linked. For additional information about attaching cameras to a sensor, see *Attach Cameras*, page 124.

6. In the **Notifications** section, select the actions you want the Video Gateway to perform when an idle-monitor event is triggered. For additional information about configuring the notification settings, see *Configuring Sensors and Activators*, page 120.

7. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see *Saving Configuration Changes*, page 157).

---

**Configuring a G-Force Sensor**

G-Force sensors are optional devices that can be built into MVGor CVG-M units upon customer request. These sensors detect extreme or sudden motion. They can be configured to be more or less sensitive, as required. At their highest sensitivity, they can even detect driver behavior that is somewhat erratic. However, at that level of sensitivity, they may be triggered more frequently than is ideal, because simple bumps in the road and sharp turns may set them off. At lower sensitivity settings, they only report more significant events, such as crashes or near-crashes when the driver slams on the brakes.

In addition to the sensitivity, you can also configure the debounce; this defines the minimum interval between distinct events. For example, if the debounce is one 30 seconds, two bumps would be treated as the same event if
they were detected less than 30-seCONDS apart, and 30 seconds without an event would have to pass in order for a new event to be identified.

To configure a G-Force sensor:

1. In the **Main Menu**, under **Sensors**, click **G Sensor 35**. The **G Sensor** configuration screen opens.

2. Select the **Enabled** checkbox. The fields required to configure the settings are added to the screen.

![G Sensor Configuration Screen](image)

3. Under **Sensitivity**, select how sensitive you want the sensor to be (lowest, lower, medium, higher, or highest). The higher the sensitivity level, the less movement will be required for the sensor to trigger an event. You may have to experiment with different settings to see which is ideal for the particular vehicle the Video Gateway is installed in.

4. Under **Debounce**, enter the minimum time that must pass between triggers in order for them to be treated as distinct events.

5. Under **Attach Cameras**, select the cameras to which the G-Force sensor should be linked. For additional information about attaching cameras to a sensor, see **Attach Cameras**, page 124.

6. In the **Notifications** section, select the actions you want the Video Gateway to perform when a G-Force sensor event is triggered. For additional information about configuring the notification settings, see **Configuring Sensors and Activators**, page 120.

7. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).
Defining Alternate Outlines

Outlines define alternate sets of recording and event-handling settings. For example, for the MVG, you could define one set of settings for times when the vehicle is in operation and another set for when it is parked; when the vehicle is in operation, the motion and sensor notifications would be turned off, but when it is parked, they would be turned on.

Outline configuration is an optional feature of the Video Gateway. If you do not define any outlines, all the event-handling settings are automatically stored in the Default outline. You do not have to configure the outline settings at all in this case. If you choose to use the Outline feature, you can define up to five additional outlines.

When multiple outlines have been defined, the running outline – the outline whose settings are currently being used by the system – can be switched in one of three ways:

- **Manually:** By selecting the desired outline in the configuration utility, as described below
- **Sensor:** In response to sensor events on Sensor 1 (toggling of a switch connected to In1)
- **Schedule:** According to a predefined schedule

The outline-switching alternatives are mutually exclusive; only one of the three switching methods can be active at any given time. The active outline-switching method is selected in the General Systems Settings screen (see page 23). For information about using Sensor 1 to trigger outline switching, see Configuring Sensor and Activator Settings, page 120. For information about setting up a schedule for outline switching, see Schedules, page 77.

**NOTE:** On CVG and CVG-M models, sensor-triggered outline switching should not be used if the sensor connector (In1) is used to control the display on a connected CCTV monitor. For additional information, see Configuring Sensor and Activator Settings, page 120; Configuring a Sensor to Control CCTV Display, page 127, and refer to the unit’s installation guide.

The name of the outline that is currently running is displayed at the top of the screen.

Creating an Outline

In addition to the default outline, you can create up to five additional outlines.

**To create a new outline:**

1. In the **Main Menu**, click **Outlines**. The **Show Outlines** screen opens.
Defining Alternate Outlines

2. Click Show Outlines. The Outlines screen opens:

![Figure 176: Outlines screen]

Note: The Load Outline on System Start checkbox and the Activate button do not appear if sensor-triggered or scheduled outline switching is activated. The active outline-switching method is selected in the General Systems Settings screen (see page 23).

3. In the Outlines screen, or in the Main Menu, click one of the Outline links (e.g., Outline 1) The outline’s summary screen opens:
4. Select **Enabled**. The outline’s initial recording and event-handling settings are displayed:
Figure 178: Outline #1 summary screen – enabled

Note: The initial settings of each outline are based on the Default outline.

5. Under **Outline Name**, modify the name of the outline as required, and then click **Update**. The name is updated. The change is fully implemented when the configuration changes are saved and the unit is restarted. (You can save and restart now, and then continue configuring the outline, or wait until you have configured more settings before saving the changes and restarting.)

Note: If the outline has already been configured, and you want to reset the settings to their defaults (namely, the settings of the Default outline) before you begin reconfiguring them, click **Restore Default Outline**, and then click **Update**.

6. In the **Main Menu**, under the selected outline, click the first device. For example, under **Outline 1**, click **Camera 1**.
### Defining Alternate Outlines

#### Figure 179: Opening Outline 1, Camera 1 settings in the Main Menu

The configuration screen for the device opens.

![Configuration Screen](image)

#### Figure 180: Outline 1, Camera 1 configuration screen
**Note:** If a device is not enabled in the Default outline, it cannot be enabled in any other outline. In this case, the configuration screen of the device in the outline section will say the device is disabled (see figure 181). For information about activating a device in the Default outline, see page 121.

![Screenshot of configuration screen](image)

**Figure 181: Device that is not enabled in the Default outline**

7. Select the desired settings for the device in the current outline.

   **Note:** For information about the settings, please refer to the section of this manual that relates to each type of setting, as follows:

   - **Video Motion Detection (VMD),** page 97
     
     **Note:** If VMD is enabled for a camera in the default outline, it cannot be disabled in any other outline. Similarly, VMD regions can only be defined and modified in the default outline; they are applied in all outlines in accordance with their definitions in the default outline.

   - **Configuring Video Lost,** page 103
   - **Video Recording Settings,** page 105
   - **Configuring Sensor and Activator Settings,** page 120
     
     **Note:** In the **Camera** screens, when recording is by event, the sensors and activators can only be selected as triggers if they are already enabled in the current outline. Thus, for example, if you want to select Sensor 1 as a trigger for the Camera 1 recorder, you must first enable Sensor 1 in its configuration screen, and then select it in the Camera 1 configuration screen.

8. Click **Update**.

9. Repeat steps 6–8 for each of the cameras, sensors, and activators connected to the **Video Gateway**.

10. Save the changes. The settings will be implemented after the unit is restarted (see **Saving Configuration Changes,** page 157).

**Activating Outlines Manually**

If more than one outline is defined, and outline switching is not performed automatically by the system (by means of Sensor 1 or through a schedule), you can manually select the outline you want to run at any time. In addition, you can specify that the selected outline be loaded automatically when the unit first starts up. In this case, the selected outline replaces the **Default** outline as the system default.
To manually switch the running outline:

- In the Outlines screen, in the line in which the outline is listed, or in the relevant outline configuration screen, click Activate. The selected outline runs immediately. If the Outlines screen was not already opened, it opens and displays an updated summary of the outline settings.

Note: The Activate button does not appear if sensor-triggered or scheduled outline switching is activated (see General System Settings, page 17).

To select the start-up outline:

1. In the Outlines screen, in the line in which the outline is listed, or in the relevant outline configuration screen, select Load Outline on System Start.

Note: The Load Outline on System Start checkbox does not appear if sensor-triggered or scheduled outline switching is activated (see General System Settings, page 17).

2. Click Activate (to the right of the checkbox). The selected outline runs immediately, and is selected as the start-up outline that will be loaded automatically whenever the system starts. If the Outlines screen was not already opened, it opens and displays an updated summary of the outline settings.
Saving Configuration Changes

As you make changes in each screen, you click the Update button to save the changes. However, in order to complete the save operation and update the Video Gateway, you need to carry out the steps described below. Most configuration changes only take effect after you carry out all of these steps.

**NOTE:** Changes in the WiFi and Network Priorities, changes in the Modem screen of the MVG and UVG400, and modifications to camera brightness, contrast, and saturation settings are implemented immediately when you click the Update button. To save them permanently, the changes must be saved, but restarting the unit is not necessary. All other configuration changes are implemented only after they are saved and the system is restarted.

**To save all changes:**

1. Do one of the following:
   - In the orange Update Confirmation (ATTENTION) message below the Main Menu, click “Click here to go to Save Settings page.”
   - In the Main Menu, under System, click Save Settings.

   The Save Settings screen opens:

   ![Save Settings screen](image)

   **Figure 182: Save Settings screen**

2. In the Save Settings screen, click Save Changes to System. The unit stores the changes permanently, and the System Restart Page screen opens:
Figure 183: System Restart page (HVG400, CVG, CVG-M)

Figure 184: System Restart Page screen (MVG, UVG)

Note: The System Restart page of MVG and UVG400 units, which have built-in SerVision routers, contains a Restart Router button. For information about this button, see Resetting the Unit, page 198.

3. Click Restart System. The unit restarts, and the changes are implemented. You are automatically logged out of the configuration utility, and a confirmation message appears.
Figure 185: Restart confirmation message

Note: To continue configuring the unit, wait at least 30 seconds, and then click the link and log into the configuration utility again.

Note: If you do not restart the unit at this time, most changes are not implemented on the unit, but they are saved on it. The next time the unit is reset, the changes are implemented.

Discarding Changes

Once you have saved a change to the unit's settings in the configuration utility, the change is stored on the unit. When the unit is next restarted, the change is implemented. If the unit has not yet been restarted, you can choose to cancel all configuration changes that were not yet implemented. If you choose this option, changes that have not yet been implemented are erased from the unit, and are not implemented when the unit restarts.

To discard all configuration changes that were saved but were not yet implemented:

1. In the Main Menu, under System, click Save Settings. The Save Settings screen opens.

2. In the Save Settings screen, click Discard Changes. The changes are canceled, and the Changes Discarded screen opens:
3. Continue configuring the unit as required.

Restoring Default Settings

If the unit does not function as expected, and you believe this is the result of recent configuration changes, you can choose to restore all of the original factory settings to the unit. You can then configure the unit manually once again, from scratch, as you would if the system was just installed.

**NOTE:** If recent configuration changes have made it impossible to access the unit at all, even through the local network, the factory settings can be restored as described under Restoring Factory Settings, page 199.

**To restore the default settings:**

1. In the **Main Menu**, under **System**, click **Save Settings**. The **Save Settings** screen opens.

2. In the **Save Settings** screen, click **Restore Default Settings**. The **Confirm Restore** screen opens.
3. Select **Are you sure you want to restore factory defaults?**.
   
   **Note:** If you do not select this option, the unit's settings will not be restored, even if you click **Confirm**.

4. If you want to save all the recorded video that is stored on the unit, select **Attempt To Save Recordings?**. Before restoring the factory settings, the system will attempt to save the recorded video on the storage media. If it succeeds, the video will be available on the unit after the factory settings are restored. The names of the unit and of the cameras recording the video will be lost; however, the cameras will be identified as Camera 1, Camera 2, etc.
   
   **Note:** Normally, the video can be saved if two conditions are met: (1) The recordings were all in SIF or CIF resolution. (2) The disk space allotted to each camera for storing video recordings matched the default allotment (see **Advanced Recorder Settings**, page 107).

5. Click **Confirm**. The default factory settings of the unit are restored, and the **System Restart Page** screen opens.
   
   **Note:** At the bottom of the **System Restart Page**, the **System Summary** screen appears and displays the settings that the unit will have when it restarts (i.e., the unit’s default settings). Make a note of the LAN settings and system name; having this information available will make it easier for you to finding the unit on the network after it restarts.
6. Click **Restart System**. The unit restarts, and the factory default settings are implemented. You are automatically logged out of the configuration utility, and a confirmation message appears.

![Figure 188: System Restart Page after default settings are restored](image)

**Note:** To begin reconfiguring the unit, do one of the following:
If the primary IP used by the unit before you restored the default settings was the default, factory-configured IP, click the link in the confirmation message to log into the configuration utility and reconfigure it.

If the primary IP used by the unit before you restored the default settings was different from the default, factory-configured IP, use SVMultiClient to search for the unit on the network, and open the unit's configuration utility from SVMultiClient (see Opening the Configuration Utility, page 8).
Connecting to the Video Gateway

When the system is up and running, you can connect to it in order to access video and other data in a number of ways:

- **Client applications**: For full client features, such as video streaming, event monitoring, and PTZ camera control, you must use one of the SerVision client applications. Applications that run on PCs and on certain cellular telephone and PDA models are available. For additional information, see About Client Software, page 6, and refer to the SerVision website (www.servision.net).

- **Configuration utility**: The configuration utility can connect to the Video Gateway as a client in order to display live images from cameras, retrieve event information from the system, and download recorded video to a designated FTP server.

Once the system is installed and configured, you should test it by connecting to it from a PC that is on its local network using the SVMultiClient client application, as explained in the next section. If this is successful, you can try other methods of connecting: connecting from a remote network using any of the SerVision client applications (please refer to the relevant manual for additional information), or connecting via the configuration utility (see page 166).

Connecting Through SVMultiClient

This section explains how to connect to the Video Gateway using SVMultiClient from a PC that is either on the same LAN as the Video Gateway or connected to the unit by an Ethernet cross cable. It is recommended that you do this as soon as you have finished installing and configuring the system. If this is successful, you can then install the SVMultiClient on a remote computer and connect to the Video Gateway via the internet. For complete information about connecting to SVMultiClient, locally or remotely, and using SVMultiClient to view video, monitor events, and control devices, see the SVMultiClient User Guide.

**NOTE:** If SVMultiClient is not installed on the PC, see Installing SVMultiClient, page 7.

**To connect to the Video Gateway:**

1. Open the SVMultiClient.
2. In the SVMultiClient, at the bottom of the **Connection Panel**, click the **Search** button.

![Search button](image)

**Figure 190: Search button**

The **Find Gateway** dialog box opens, and displays a list of all the SerVision systems connected to the network.

**Note:** If a Microsoft Windows Security Alert dialog box is displayed, click **Unblock**.
3. Select the Video Gateway and then click Connect. SVMultiClient connects to the Video Gateway, and the Video Gateway appears in the Connection Panel.

4. In the Connection Panel, expand the system to display all the devices connected to it.

5. Drag a camera from the Connection Panel to one of the camera panes in the Viewing area. Live video from the camera is displayed in the camera pane.
Connecting through the Configuration Utility

The configuration utility can connect to the Video Gateway as a client in order to retrieve information about the events that are recorded on the unit and display live snapshots from the cameras.

If you log into the configuration utility using a username for which configuration permissions are selected (see Authentication, page 60), you will have access to all of these client features as well as all of the other configuration screens. If you log into the configuration utility using a username for which only client access is permitted, you will only be able to access the client features (the Client section of the Main Menu). In this case, the screen you see when you log in will be the Events screen.

NOTE: The number of video streams (live and/or recorded) that the Video Gateway can supply simultaneously is limited. This limit is based on the system configuration and is due to memory constraints.
Viewing Events

You can view lists of recorded events that are stored on the Video Gateway.

To view lists of events:

1. In the Main Menu, click Client. The Events screen opens:

2. Under Sensors, select the sensors for which you would like to see lists of recorded events.

3. Under Requested Day, select the day from which you want to see events.

   Note: The dropdown list shows the earliest date from which events are recorded, and every date from that date until the present, regardless of whether recorded events are available from those dates.

4. Click Show Events. The events are listed in the lower part of the screen. A separate list is displayed for each sensor.
Figure 196: Lists of events
Viewing Snapshots

You can view live images from the cameras connected to the Video Gateway in the configuration utility, in the **Snapshot Viewer**. This means you can see what is happening on-site wherever you are, as long as you have access to a computer that is connected to the internet – even if you do not have a client device with a SerVision client application available. Video is not supported by this feature, but snapshots can be updated at frequent intervals so that you can receive a continuous flow of images that allows you to clearly see on-site developments as they occur.

Snapshots are transmitted from the Video Gateway to the browser as JPG image files. You can specify the desired image quality during the Snapshot session.

Opening the Snapshot Viewer

In order to open the **Snapshot Viewer** and view snapshots from the cameras, you must log in with a user account that has client permissions. (User accounts are defined in the **Authentication** screen; see *Authentication*, page 60.)

**To open the Snapshot Viewer:**

1. In the **Main Menu**, under **Client**, click **Snapshots**. The login page opens on the right side of the screen.
2. Under Authentication, enter a user name and password that have client permissions associated with them (in the Authentication screen; see Authentication, page 60).

3. Under Image Information, modify the fields as necessary. (You can change the values of these fields after you log into the Snapshot Viewer as often as required.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality</td>
<td>Snapshot image quality (range: 1-100). Note: The higher the quality, the larger the JPEG image file that is created, and the longer it takes to transfer it to the web browser. A quality setting of 60 is recommended; this setting is equivalent to the quality of the images you receive when viewing a video stream at 10 FPS / 128 kbs (the default high-quality setting).</td>
</tr>
<tr>
<td>Camera</td>
<td>The camera from which you want to see the snapshots. By default, camera #1 is selected.</td>
</tr>
</tbody>
</table>

4. Click Login. The Snapshot Viewer opens and displays the latest image it received from the Video Gateway from the selected camera.

Modifying the Snapshot Settings

When the Snapshot Viewer is open, you can change its settings as required. For example, you can select a different camera or specify the refresh rate.

To change the Snapshot Viewer settings:

1. In the Snapshot Viewer, change the settings as necessary by modifying the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality</td>
<td>Modify the snapshot image quality, to any value from 1 through 100.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Camera</td>
<td>Select a different camera from which to view snapshots, if more than one camera is</td>
</tr>
<tr>
<td></td>
<td>connected to the unit.</td>
</tr>
<tr>
<td>Refresh Rate</td>
<td>If you want the snapshot to be updated automatically, specify how often you want the</td>
</tr>
<tr>
<td></td>
<td>updates to occur, in seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A refresh rate of &quot;0&quot; means the snapshot is not updated automatically.</td>
</tr>
</tbody>
</table>

2. Click **Change Settings**. The new settings are implemented.

**Refreshing the Snapshot**

You can refresh the snapshot manually whenever you wish.

👉 **To manually refresh the snapshot:**

- Click **Refresh Image**.
System Diagnostics

The configuration utility contains various tools that can be used to monitor system functioning, help solve connection and other system problems, and to schedule routine system maintenance.

The **System Diagnostics** screen displays the current system statistics and contains tools that you can use to test the current connection and e-mail notification settings. Some of these tools, as well as additional system information, can also be accessed from the **Diagnostics** submenu.

**NOTE:** The use of these tools is only recommended for people with some understanding of computers and networking.

The following system information and diagnostic tools are available:

- **System Statistics:** Provides information about the unit’s hardware, firmware, and time settings (see page 173)
- **Ping:** Tests remote connections from the Video Gateway to another device (see page 174)
- **Traceroute:** Traces the path used to connect remotely from the Video Gateway to another device (see page 177)
- **Notifications:** Sends an e-mail message to all of the recipients of e-mail notifications. This option is also available in the **System Summary** screen. For additional information about notifications, see **SMS and E-mail Notifications**, page 61. For information about testing e-mail notifications, see **Testing Notification Settings**, page 67.
  
  **Note:** If no recipients are defined for one of the types of notifications, the test button for that type of notification does not appear.
- **Power Log:** Lists every time the Video Gateway resets, and indicates what caused the reset and what type of reset it was; lists the system temperature when the temperature approaches a level that can cause damage to the unit
- **Error Log:** Lists recording errors reported by the Video Gateway. This information may help SerVision technical support staff diagnose problems you are having with your system
- **User Log:** Provides a history of user logins and logouts, including the date, time, and IP address of the device from which the user connected to the Video Gateway.
- **Connections:** Lists various network connections that are in place. This information may help SerVision technical support staff diagnose problems you are having with your system.
- **Maintenance:** Enables you to schedule the system’s self-maintenance procedure and, on certain models, to configure the network connection delay (see page 182)
To open the System Diagnostics screen:

- In the Main Menu, click Diagnostics.

### System Statistics

The System Diagnostics screen includes a list of system statistics:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Temperature</td>
<td>The current temperature of the Video Gateway's CPU. If the temperature is too high, it is displayed in red.</td>
</tr>
</tbody>
</table>
| System Clock | The status of the system clock; can be one of the following:  
  - OK: Indicates the clock is set and functioning properly. The current date and time appear after the "OK" status.  
  - ERROR: Indicates the clock is either not set or not functioning properly. Try resetting the clock manually (see Setting the Unit Time, page 33). If that does not solve the problem, contact technical support. |
| Memory      | The size of the unit's RAM                       |
| DSP         | The speed of the unit's digital signal processor |
SerVision
Embedded Video Gateway System Guide

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD Size</td>
<td>The capacity of the unit's storage medium</td>
</tr>
<tr>
<td>HD Model</td>
<td>The model number of the unit's storage medium</td>
</tr>
<tr>
<td>Chipset</td>
<td>The unit's chipset identifier. (This information may be requested by technical support staff if the unit malfunctions.)</td>
</tr>
<tr>
<td>AES Key</td>
<td>The name and size (number of bits) of the AES key that will be used if a client requests that data be encrypted before it is transmitted by the Video Gateway to that client. If you have not modified the default AES, the default key is used, and <em>DEFAULT</em> appears. For additional information, see Modifying the AES Key, page 193.</td>
</tr>
</tbody>
</table>

## Testing Remote Connections

Ping and Traceroute are tools that send simple messages to an IP address to test the connection between the device sending the message and the device with the given IP.

- **Ping** sends the message and waits for a reply. If a reply is received, you know the device with the given IP is running and can receive and transmit data. Using Ping, you can check whether your Video Gateway unit is running and can be accessed remotely.

- **Traceroute** sends the message and follows the route it takes from machine to machine in the network to reach its destination. This may help you identify routing problems or firewalls that are interfering with remote connections to your Video Gateway.

**NOTE:** Some devices are configured not to respond to Ping requests. Therefore, the fact that a device does not respond to a Ping request does not prove unequivocally that the device cannot be accessed remotely. Similarly, since Traceroute makes use of Ping, the information returned by Traceroute may be incomplete.

Both Ping and Traceroute are available from any Windows Command Window. You can use them from Windows to test connections from the PC to other devices, such as the Video Gateway. This is useful as an initial diagnostic tool in a situation in which you can connect to the Video Gateway unit for configuration and client access through a PC that is on the same LAN as the unit, but you cannot connect to the unit remotely.

You can also run Ping and Traceroute from the Video Gateway configuration utility to test connections from the Video Gateway to other devices, such as SMS / SMTP servers and NTP servers.

### Ping

Ping is a tool that sends a simple message to an IP address and waits for a reply. If a reply is received, you know the device with the given IP is running and can receive and transmit data. Ping is available from any Windows Command Window. Using Ping from a remote PC, you can check whether your Video Gateway unit is running and can be accessed remotely. You can also test remote connections from the Video Gateway unit to other devices by running Ping from the configuration utility.

**NOTE:** Some devices are configured not to respond to Ping requests. Therefore, the fact that a device does not respond to a Ping request does not prove unequivocally that the device cannot be accessed remotely.

**To test connections to the Video Gateway unit using Ping from the PC:**

1. On the PC, open a Command Window as follows:
   - Open the **Start** menu and click **Run**. A **Run** window opens.
In the Run window, in the Open field, type cmd, and then click OK. A Command Window opens.

In the Command Window, type ping <IP>, where <IP> is the IP address of the Video Gateway. For example, type

```
ping 192.168.3.60
```

3. Press Enter. The PC attempts to ping the Video Gateway by sending four test messages to it. The Ping command returns responses from the Video Gateway for each message that was successfully sent, as in figure 204. If a target device does not respond to a message, the Ping command returns a "Request timed out" message, as in figure 205.
To test a remote connection from the Video Gateway unit to a host device using Ping:

1. In the System Diagnostics screen, under Ping, in the Ping IP/Host field, fill in the URL or public IP address of the host device to which the Video Gateway should connect.

![Ping request](image)

Figure 206: Ping request

Note: You can also access Ping from the Diagnostics submenu. The functionality is the same regardless of how you access it.
2. Click **Start**. The response screen opens. If the target device responds, the response, which includes the IP address of the device and a few other statistics, is displayed:

![Ping Response](image)

**Figure 207: Diagnostics submenu**

If the target device does not respond, an error code is displayed:

![Ping Error](image)

**Figure 208: Ping with response from remote device**

If the target device does not respond, an error code is displayed:

![Ping Error](image)

**Figure 209: Ping to which the remote device did not respond**

**Traceroute**

Traceroute is a tool that sends a simple message to an IP address and follows the route it takes from machine to machine in the network to reach its destination. This may help you identify routing problems or firewalls that are interfering with remote connections to your Video Gateway. Traceroute is available from any Windows Command Window. Using Traceroute from a remote PC, you can check the route from the PC to your Video Gateway unit. You can also check the routes of remote connections from the Video Gateway unit to other devices by running Traceroute from the configuration utility.
NOTE: Some sites block Ping requests. Since Traceroute makes use of Ping, the information returned by Traceroute may be incomplete.

To check the route from a PC to the Video Gateway unit using Traceroute:

1. On the PC, open a Command Window as follows:

   - Open the Start menu and click Run. A Run window opens.
   - In the Run window, in the Open field, type cmd, and then click OK. A Command Window opens.

   ![Figure 210: Run window](image)

   ![Figure 211: Command Window](image)

2. In the Command Window, type tracert <IP>, where <IP> is the IP address of the Video Gateway. For example, type

   ```
   tracert 216.10.144.11
   ```

3. Press Enter. Traceroute sends three packets, and follows their route for up to 30 steps from the sender to the target. For each step in the route, the time it took for each packet to arrive from the previous machine, and the IP of the current machine, are displayed.
Figure 212: Results of successful Traceroute

If the target device is not reached after 30 steps, Traceroute times out.

Figure 213: Traceroute timed out after 30 steps
To trace the route from the Video Gateway unit to a host device using Traceroute:

1. In the System Diagnostics screen, under Traceroute, in the Trace IP/Host field, fill in the URL or public IP address of the host device to which the Video Gateway should connect.

```
TRACE ROUTE
TRACE IP/HOST www.google.com START
```

**Figure 214: Traceroute request**

**Note:** You can also access Traceroute from the Diagnostics submenu. The functionality is the same regardless of how you access it.

```
HW_003  2.2.26a78/884

SUMMARY
CAMERAS
SENSORS
OUTLINES
SYSTEM
DIAGNOSTICS
PING
TRACEROUTE
POWER LOG
ERROR LOG
USER LOG
CONNECTIONS
UPGRADE SOFTWARE
UPGRADE ROUTER
MAINTENANCE
CLIENT

Traceroute in Diagnostics submenu
```

**Figure 215: Diagnostics submenu**

2. Click Start. The response screen opens. Traceroute sends three packets, and follows their route for up to 30 steps from the sender to the target. For each step in the route, the time it took for each packet to arrive from the previous machine, and the IP of the current machine, are displayed.
Figure 216: Traceroute results

If the target device is not reached after 30 steps, Traceroute times out.
Figure 217: Traceroute timed out after 30 steps

**Maintenance**

The maintenance screen is used to configure automatic system maintenance. In addition, on some Video Gateway models the screen can be used to set up a network connection delay.
The unit can be configured to periodically perform a routine maintenance procedure. The procedure helps ensure the unit will function optimally over long periods of time. During the maintenance procedure, the system is temporarily unavailable. The procedure takes up to three minutes.

In addition, the unit can be configured to wait a specified period of time after startup before attempting to connect to the local network. This option is useful in network configurations in which it is desirable to allow time for the local network to get up and running after a power outage or other interruption in network communication before the Video Gateway attempts to connect to the network.

**To configure the maintenance options:**

1. In the **System Diagnostics** screen, click **Maintenance**. The **Maintenance** screen opens.

   ![Maintenance screen](HVG400, CVG, CVG-M)

   **Figure 218: Maintenance screen (HVG400, CVG, CVG-M)**

2. Under **Scheduled maintenance at**, select the time at which you want the maintenance procedure to run.

3. In the text field between **Every** and **Days**, fill in how often you want the maintenance procedure to take place, in days. If you do not want the maintenance procedure to run at all, type “0.”

4. Under **Network Startup Delay**, specify in the number of seconds the unit should wait after it boots up before it attempts to connect to the network.

5. Click **Update**, and then save the settings. They will be implemented after the unit is restarted (see **Saving Configuration Changes**, page 157).
Upgrading the Firmware

From time to time, SerVision releases new firmware versions for the Video Gateway. This section explains how to obtain and install new Video Gateway firmware. New firmware can be installed on-site or remotely. It is recommended to install it on-site whenever possible. If your distributor has a TVG Upload Server to which you can connect, you can upgrade the firmware using the configuration utility. Otherwise, you must download the firmware from the SerVision website and use the TVG Download Utility to download it to the Video Gateway.

**NOTE:** Upgrading the firmware does not change any of the unit’s settings.

**CAUTION:** If the download process is interrupted in any way before it is completed, or if an incompatible firmware version is loaded, it may be impossible to connect to the unit in the normal way again. Make sure that you know in advance that you are loading the right firmware, and DO NOT INTERRUPT THE DOWNLOAD PROCESS once it is started. If it nevertheless becomes impossible to connect to the unit after an attempt to upgrade the firmware, the *Catch Boot operation* can be used to reconnect to the unit and download the firmware to it again. See *Catch Boot Operation*, page 188.

SerVision routers have their own firmware, and this firmware may require upgrading from time to time. These routers are built into MVG and UVG400 units. For information about upgrading the router firmware of these models, see *Upgrading Router Firmware*, page 192.

**Upgrading Firmware via a TVG Upload Server**

If your distributor has a TVG Upload Server to which you can connect, you can upgrade the firmware using the configuration utility. Before you begin, ask your distributor for the IP address or hostname of the server and its port.

**To upgrade the Video Gateway firmware from a TVG Upload Server:**

1. In the **Main Menu**, click **Diagnostics**, and then click **Upgrade Software**. The **System Upgrade** screen opens:
2. Fill in the fields as follows:
   - **IP/Host**: The IP address or hostname of the **TVG Upload Server**
   - **Port**: The port of the **TVG Upload Server**

3. Click **Update**. The unit connects to the server, and receives a list of available firmware versions from it. It displays the list in the screen.

   **Figure 220: Available firmware versions**
4. Select the required version from the list, and then click **Update**. The update process begins. A progress log is displayed.

**SYSTEM UPGRADE**

_UPDATE STARTED. PLEASE WAIT UNTIL THE SYSTEM RESTARTS ITSELF AT THE END OF THE UPGRADE PROCESS_
_CLOSED: 0 CLOSED: 0 CLOSED: 0 CLOSED: 1 CLOSED: 0 CLOSED: 1 CLOSED: 2 CLOSED: 0 CLOSED: 2 CLOSED: 0

**Figure 221: Log of the upgrade process**

When the process is complete, you are logged out of the configuration utility. Log in again to continue configuring the unit.

**Upgrading Firmware via the TVG Download Utility**

If your distributor does not offer direct downloading of firmware updates via a TVG Upload Server, you must download the required files and install them as explained in this section. In addition, the Catch Boot operation can only be implemented using the method described below.

**Required Files**

To upgrade the firmware, you need the following files:

- **The Download Utility**: TVG_download.exe
- A DLL file required by the Download Utility: PCOMM.dll
- The firmware file to install on the Video Gateway unit; the file has a TVX file extension (for example, tvg_2_2_10a3.tvx)

You can download the latest versions of these files from the SerVision website (http://www.servision.net). Be sure to save the Download Utility and the DLL file in the same folder. The firmware file can be saved in any location on your PC.

**Downloading the Firmware to the Unit**

The new firmware can be downloaded to the Video Gateway from a computer that is connected to the unit through a LAN, via a cross cable, or over the internet. However, because of potential communication problems when using the internet, it is recommended to download through the LAN or cross cable whenever possible.
To download the firmware to the unit:

1. Double-click the TVG_download.exe file. The Download Utility opens:

   ![Download Utility](image)

   **Figure 222: Download Utility**

   Note: The version number of the Download Utility appears in the title bar.

2. Select LAN.

3. In the IP and Port fields, enter the IP address and port of the unit in one of the following ways:
   - Manually enter the values.
   - If the Video Gateway unit is on the same local network as the PC, click Find units. The opens and lists all of the embedded Video Gateway units on the network. Select the relevant Video Gateway and then click Select. The IP and Port fields are filled in.

   ![List of embedded Video Gateways on the local network](image)

   **Figure 223: List of embedded Video Gateways on the local network**

   Note: If the unit has just started up, it may not appear until its boot process is completed. In this case, click Exit to close the Find gateways dialog box, wait a minute, and then open the Find gateways dialog box again.
4. In the upper-right corner of the **Download Utility**, make sure the **Login** checkbox is selected, and then enter the **Username** and **Password** you use to access the configuration utility of the unit.

5. Click the **File** button at the bottom of the dialog box. A file selection dialog box opens.

6. Browse to the TVX firmware file that you downloaded, and then click **OK**.

   The file name appears in the window.

   ![Figure 224: Download Utility with firmware file selected](image)

7. Click **Download**.

   Download progress is indicated in the progress bar in the lower portion of the **Download Utility**. The process begins with an integrity check that ensures the file is a valid firmware file. Then the file is downloaded to the unit. When the download is completed, the unit automatically resets, and the **Software download** message is displayed.

   ![Figure 225: Software download message](image)

8. After about a minute, the unit reset should be complete. Once this has occurred, the **Power** LED on the front of the unit should flash at frequent intervals. If the light is not flashing – it displays as a solid green or orange all the time – the reset was not successful. In this case, disconnect the unit from the power supply and then reconnect it. The unit resets again.

   **Note:** If the unit is disconnected from the power supply before the **Download Utility** informs you that it has finished, the firmware may become corrupted and it may then be impossible to connect to the unit. (In this case, it may be necessary to perform a Catch Boot operation. For additional information, please refer to your system guide or consult your vendor.)

**Catch Boot Operation**

**CAUTION:** This function is for technicians only.

In some cases, a download fails and it is not possible to access the unit afterwards in the usual way. This can occur, for example, if the download was interrupted before it was completed or if an incompatible firmware version was downloaded to the unit.
When this happens, you can usually reinstall the firmware using the *Catch Boot operation*. This option uses the unit’s built-in boot loader for downloading, and does not need the firmware in order to function.

**NOTE:** The Catch Boot operation uses an RS232 cable for download, and is much slower than LAN download.

To see whether it is possible — or necessary — to reinstall firmware using Catch Boot:

- Unplug the unit and then plug it back in. The Power LED indicates whether Catch Boot is necessary and possible, as follows:

<table>
<thead>
<tr>
<th>LED Behavior</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flashes orange once when power is restored and then remains a solid green</td>
<td>Catch Boot can and should be performed.</td>
</tr>
<tr>
<td>Flashes orange/green every second</td>
<td>Catch Boot is not necessary, because the unit has a valid software version.</td>
</tr>
<tr>
<td>Remains solid green and does not flash orange</td>
<td>Catch Boot cannot be performed.</td>
</tr>
<tr>
<td>Alternates between flashing quickly for a half second and remaining solid for a half second</td>
<td>There is a major error in the system. Contact technical support or your vendor. Do not perform Catch Boot.</td>
</tr>
</tbody>
</table>

To reinstall firmware using the Catch Boot operation:

1. Connect the Video Gateway to your computer with an RS232 connection cable.
   
   **Note:** If you do not have an RS232 cable, please consult your vendor.
   
   **Note:** If a PTZ controller is connected to the RS232 port, disconnect it first.
   
   **Note:** You must have an RS232 connector on your PC in order to perform the Catch Boot operation. If one does not exist, it is possible to purchase a USB-to-serial adaptor, and connect the RS232 cable through it. Such adaptors are available in most computer stores.

2. Run the **TVG_download.exe** utility with the `-t` parameter.
   
   To add the `-t` parameter, create a shortcut to **TVG_download.exe**, open its **Properties** and in the **Target** field add `-t` after the file name.
Upgrading the Firmware

1. The Download Utility opens, with the Catch Boot option available.

2. Select RS232, and then enter the COM port number.

3. Select Catch boot. A message containing instructions for using the Catch Boot feature appears:
5. Click **OK**. The message closes.

   **Note:** The Catch Boot operation does not perform a login; it is not necessary to fill in the **Username** and **Password** fields.

6. Click **File**. A file selection dialog box opens.

7. Browse to the TVX firmware file that you want to download to the unit, and then click **OK**. The file name appears in the window.

![Figure 228: Catch Boot option with firmware file selected](image)

   **Note:** The **Limit MTU** option has no affect on the Catch Boot operation.

8. Click **Download**.

9. Disconnect the unit from the power supply and then reconnect it. The download process starts automatically, and the new firmware is downloaded to the unit.
Upgrading Router Firmware

This section explains how to upgrade the router firmware of MVG and UVG400 units.

You can upgrade the router firmware directly from a website such as the SerVision website. Before you begin, ask your distributor for the correct address (URL).

**NOTE:** Do not upgrade the router firmware unless you are told to do so by technical support staff.

**NOTE:** It is recommended that you save all configuration changes and restart the unit to implement them before you upgrade the router firmware.

To upgrade the router firmware:

1. In the **Main Menu**, click **Diagnostics**, and then click **Upgrade Router**. The **Router Upgrade** screen opens:

   ![Router Upgrade screen](image)

   **Figure 229: Router Upgrade screen**

2. Under **Upgrade URL**, fill in the location of the new firmware file. For example, [http://www.ru.com/ru.tgz](http://www.ru.com/ru.tgz). (Note: This is not the actual URL to use; consult your distributor for information about the correct URL.)

3. Click **Update**. The new firmware is uploaded to the unit and then the router firmware is updated.

   The upgrade process itself – once the file upload is completed – takes approximately three minutes. A timer indicates when the upgrade is completed. When it is completed, the **System Summary** screen is displayed. If this screen is not displayed within about six minutes of the end of the file upload, and you cannot connect to the unit via a client application or through the configuration utility, restart the unit by disconnecting it from the power supply and then reconnecting it. Bear in mind that interrupting the upgrade process before it is completed may cause the router to become completely inoperable, so do not restart the unit before the six minutes have passed. Note that if you are using a WiFi or cellular connection to upgrade the router firmware, it may take longer for the unit to reestablish the connection to the network.
Modifying the AES Key

You can prevent unauthorized access to data that is transmitted from the Video Gateway to client devices by encrypting the data before it is transmitted. SerVision's embedded Video Gateways support AES encryption. By default, they use a default encryption key. If you want to use this default key for your Video Gateways, no extra configuration is required on the Video Gateways. All you have to do is ensure that all client devices are configured to use encryption.

**NOTE:** You can configure the Video Gateway to refuse connections from clients that do not request encryption. For additional information, see *Allow Only Encrypted*, page 20.

You can increase the security further by using a custom AES encryption key instead of the default key. To do this, you must set the custom key manually in all of your client devices as well as on the Video Gateway; the keys on both ends of every encrypted connection must match.

In addition, you can only set one custom encryption key for a client device at any given time. Thus, all Video Gateways to which a given client will connect using an AES-encrypted connection must use the same key.

In order to set up a custom AES encryption key for your system, you must begin by defining the key in SVMultiClient. The key must be in ASCII hex, and can either contain 128, 192 or 256 bits. Each character uses 4 bits. Thus, for example, a 128-bit key would contain 32 characters. (For additional information about defining a custom encryption key in SVMultiClient, please refer to the SVMultiClient User Guide.)

When you create a custom key in SVMultiClient, it is a good idea to assign a name to it, so that you can identify it easily. Be sure to make a note of the key when you define it in SVMultiClient, because it is hidden after it is created. Then, copy the key to your clipboard, so that you can paste it in the appropriate field in the TVG Download Utility, as explained below.

**To set a custom AES encryption key on the Video Gateway:**

1. Run the TVG_download.exe utility with the **-key** parameter.

To add the **-key** parameter, create a shortcut to TVG_download.exe, open its **Properties** and in the **Target** field add **-key** after the file name.
Modifying the AES Key

1. Right-click the shortcut on your desktop.
2. Select Properties.
3. In the Target field of the shortcut properties, add the key.

Figure 230: -key in the Target field of the shortcut properties

The Download Utility opens, with the Key option available.

Figure 231: Download Utility with Key option

2. Select LAN.
3. In the IP and Port fields, enter the IP address and port of the unit in one of the following ways:
   - Manually enter the values.
   - If the Video Gateway unit is on the same local network as the PC, click Find units. The opens and lists all of the embedded Video Gateway units on the network. Select the relevant Video Gateway and then click Select. The IP and Port fields are filled in.
Modifying the AES Key

4. In the upper-right corner of the Download Utility, make sure the **Login** checkbox is selected, and then enter the **Username** and **Password** you use to access the configuration utility of the unit.

5. Click **Key**. The **AES Key** dialog box opens.

6. Click **Create a Key**. The **Create a key** dialog box opens.

---

**Figure 232: List of embedded Video Gateways on the local network**

*Note:* If the unit has just started up, it may not appear until its boot process is completed. In this case, click **Exit** to close the **Find gateways** dialog box, wait a minute, and then open the **Find gateways** dialog box again.

<table>
<thead>
<tr>
<th>Server</th>
<th>Name</th>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TVG-556</td>
<td>TVG-556</td>
<td>192.168.2.4</td>
<td>9988</td>
</tr>
<tr>
<td>TVG-557</td>
<td>TVG-557</td>
<td>192.168.2.5</td>
<td>9988</td>
</tr>
<tr>
<td>TVG-558</td>
<td>TVG-558</td>
<td>192.168.2.6</td>
<td>9988</td>
</tr>
</tbody>
</table>

**Figure 233: AES Key dialog box**

**Figure 234: Create a key dialog box**
7. Under **Original key**, paste the key you entered in SVMultiClient.

8. Click **Create**. The key is encoded. The encoded version appears under **Encoded key**.

   ![Create a key](image)

   **Figure 235: Encoded key**

9. Copy the encoded key.

10. Click **Done**.

11. In the **AES Key** dialog, paste the encoded key.

12. Fill in the bit-length of the key, add a name, and click **Send to unit**.

   ![AES Key](image)

   **Figure 236: Encoded key**

   The key is set on the Video Gateway, and a confirmation message is displayed:

   ![Confirmation message](image)

   **Figure 237: Confirmation message**

13. In the **Download Utility**, click **Done**. The **Download Utility** closes.

14. In the Video Gateway configuration utility, in the **Main Menu**, under **System**, click **Restart**. The **System Restart Page** opens.

15. Click **Restart System**. The Video Gateway restarts. After the unit restarts, the name and bit-length of the custom encryption key appear in the **System Summary** screen. When SVMultiClient is connected to the Video Gateway, they also appear in SVMultiClient, in the statistics window of the Video Gateway.
Modifying the AES Key

Figure 238: Custom AES key name and size in the System Summary

Figure 239: Custom AES key name and size in the Video Gateway statistics in SVMultiClient
Resetting the Unit

You can reset the unit at any time. Resetting the unit may help if video streaming is unreliable or frequently interrupted. In addition, most configuration changes you make are only fully implemented after the unit is reset. If changes were made to the configuration of the unit, and the changes were saved on the unit, but the unit was not reset afterwards, the changes are implemented when the unit is reset. Resetting does not cause any settings to be lost or restored to their default values.

The unit can be reset in one of the following ways:

- Through the configuration utility
- By unplugging the unit from the power

On MVG and UVG400 units, resetting the unit also resets the router. If you wish, you can reset the router without resetting the unit. While the router is restarting, you will not be able to connect to unit, but it will continue to record video and event information.

**To reset the unit using the configuration utility:**

1. Log into the configuration utility (see Opening the Configuration Utility, page 8).
2. In the **Main Menu**, under **System**, click **Restart**. The **System Restart Page** opens.
3. Click **Restart System**. The unit restarts.

**To perform a power reset:**

- Unplug the unit from the power and then plug it in again.

**To reset a SerVision router:**

1. Log into the configuration utility (see Opening the Configuration Utility, page 8).
2. In the **Main Menu**, under **System**, click **Restart**. The **System Restart Page** opens.
3. Click **Restart Router**. The router restarts.
Restoring Factory Settings

If you need to restore the factory settings of the unit, you can do this in one of two ways.

- **Software**: If you can connect to the unit’s configuration utility through the local network, you can restore the default settings in the **Save Settings** page (see *Restoring Default Settings*, page 160).

- **Hardware**: If you cannot connect to the unit, you can reset the settings as described below. This may be necessary when certain configuration settings are set incorrectly or you forget their values. For example, if you forget all username and password pairs that have permissions for configuring the unit, you will not be able to access the configuration utility.

When you use either method to restore the factory settings, the following changes are implemented on the unit:

- The unit's IP and port are reset to the IP and port that appear on the sticker on the underside of the unit (usually, the IP is 192.168.1.210 and the port is 9988).

- The two default usernames are set to their default values and all other usernames are deleted (the username and password required for access to the configuration utility are reset to *svuser* and *servconf* respectively).

- All other settings are reset to their original values.

- All recorded video on the Video Gateway unit is erased.

After you have restored the factory settings, you can access the unit as described under *Opening the Configuration Utility*, on page 8.

Hardware-based restoration of factory settings is accomplished by shorting two of the pins of the **RS232/485** connector together. To perform this procedure, it is best to use a jumper. Jumpers are available at any electronics supply store.

![Jumper](image)

**Figure 241: Jumper**

**To reset the configuration settings to their factory values:**

1. Disconnect the unit’s power.

2. If anything is plugged into the **RS232/485** connector (e.g., a PTZ camera controller or the supplied RS232/485 adaptor), disconnect it from the port.

3. Place the jumper on pins 2 and 3 of the **RS232/485** connector.
Figure 242: Pins to short in order to restore the factory setting (MVG)

Figure 243: Pins to short in order to restore the factory settings (CVG)
4. Reconnect the power to the unit. When the startup process is completed (the Power LED on the front of the unit flashes at frequent intervals), the default factory settings are restored.

5. Disconnect the power from the unit again.

6. Remove the jumper from the RS232/485 connector.

7. If you disconnected a PTZ controller before performing this procedure, reconnect the controller.

8. Reconnect the power to the unit.
Troubleshooting

This section contains a list of common problems and suggestions for finding solutions. If you cannot solve a problem you are having with the unit, please contact technical support.

NOTE: The technical support representative may ask you for the serial number of your unit. The serial number appears on the sticker on the underside of the unit, and is labeled S/N.

1. Problem:
   After modifying configuration settings and restarting the Video Gateway, the unit cannot be accessed.

   Solution:
   Disconnect the power supply from the unit and then reconnect it.

   Additional information: Resetting the Unit, page 198

2. Problem:
   The firmware update process did not complete properly, and the Video Gateway unit cannot be accessed.

   Solution:
   Disconnect the power supply from the unit and then reconnect it. If the LED on the front of the unit flashes orange once when it starts up and then displays as a solid green (and is not flashing), reinstall the firmware using the Catch Boot operation. If the LED displays as a solid orange, or does not flash orange once before it becomes a solid green, contact your distributor.

   Additional information: Catch Boot Operation, page 188

3. Problem:
   The unit can be accessed by PCs that are connected to the LAN, but not by remote client devices.

   Solutions:
   - Check that the relevant network settings are correct.
     Additional information: LAN Settings, page 38; Modem, page 40; WiFi, page 47
   - Check the firewall settings of the network gateway (router); ensure that the required port is open for incoming connections and that the port is forwarded correctly.
     Additional information: Ports, page 17

4. Problem:
   A connection to a cellular network cannot be established.

   Solutions:
   - Ensure that all of the connection parameters are defined correctly in the Modem Configuration screen.
   - If you are using a GSM modem, check if the SIM card is PIN-protected. If it is, ensure that the correct PIN is entered in the Modem Configuration screen.
   - Contact your cellular provider to ensure that the modem settings are correct and the line is active.
• If LCP is enabled, try disabling it.
  Additional information: Modem, page 40.

5. Problem:
A username and/or password that can be used to access the unit’s configuration utility are not known.

Solution:
Restore the factory settings to the unit and then reconfigure it.

Additional information: Restoring Factory Settings, page 199

6. Problem:
Only the Client option appears in the Main Menu.

Solution:
You have logged in using a username for which only client permissions are selected. Login using a username for which configuration permission is selected.

Additional information: Authentication, page 60; Connecting through the Configuration Utility, page 166

7. Problem:
When client applications attempt to connect to the unit, an "Authentication failed" error is displayed in the client.

Solution:
Ensure that the client application is configured with a username for which client permissions are selected.

Additional information: Authentication, page 60

8. Problem:
TV-Out does not appear in the Main Menu.

Solution:
• Contact your vendor for support.

9. Problems:
• Video does not display properly in the client application:
  • You cannot see any video.
  • The video image is distorted.
  • The frames flow upwards constantly.
  • A horizontal black stripe appears near the bottom of the client video display.

Solution:
The system is not configured for the proper video format. Ensure that video format used by the camera (PAL or NTSC) is selected in the General System Settings screen.

Additional information: Configuring General System Settings, page 21 (in particular, on the Video Mode field, see page 22)
10. Problems:

- Video of events that was supposed to be uploaded to an AVV server automatically (by means of the AVV feature) does not appear there.

- A link to video that was uploaded to an AVV server appears in an e-mail notification, but when you click the link, the browser cannot find the file. The browser returns an error message – for example, “http error 404,” “The webpage cannot be found,” or “Not Found.”

Solutions:

- Ensure that the port forwarding and firewalls of the external networks and of the FTP server’s network are configured to permit communication on the specified port.

- Ensure that the AVV configuration settings are correct.

- Wait a few minutes. Video of an event is only uploaded after the event ends. Processing and uploading also take some time. When the event is successfully uploaded, you will receive an additional e-mail telling you that the upload ended and including the same link. Click the link in this e-mail and the file should be available on the AVV server.

- If the camera is set to record by event, ensure that the sensor (VMD, sensor, activator) triggering the AVV is defined as a trigger for recording in the camera’s configuration.

Additional information: Automatically Uploading Video to an AVV Server, page 67; Configuring Video Recording, page 106

11. Problem:

The standard video quality settings do not work well with a client application.

Solutions:

- In the video recording settings, select **Enable Advanced Settings**, and customize the bitrate and framerate. The customized settings will now be available in client applications for live as well as recorded video.

  Additional information: Video Recording Settings, page 105

- Contact technical support for information about customizing stream properties.

12. Problem:

The unit does not record video even though it is configured to do so, or video that was recorded by the unit cannot be accessed by any of the client applications.

Solutions:

- Ensure that the unit time and the time zone are correct.

  Additional information: Setting the Unit Time, page 33

- In the **System Diagnostics** screen, check the **System Clock** status. If the status is “Error,” try resetting the clock manually. If that does not solve the problem, contact technical support.

  Additional information: System Statistics, page 173; Setting the Unit Time, page 33

- If you have configured the unit for event-triggered recording, ensure that at least one sensor is selected as a trigger, that the selected sensors are functioning properly, and that one or more of the sensors detected events during the time period from which you attempted to view recorded video.

  Additional information: Configuring Video Recording, page 106
In the **System Diagnostics** screen (or the **System** screen), check the **HD Size** and **HD Model**. If the size is 0 or the model is incorrect, there may be a problem with the storage media. Contact your vendor.

Additional information: *System Statistics*, page 173

### 13. Problem:
The unit is connected to a LAN but cannot be accessed through the LAN.

**Solutions:**
- Ensure that the Ethernet (network) cable is fully inserted into the **Ethernet Out** connector on the rear panel of the Video Gateway unit.
  
  Additional information: Please refer to the unit’s installation guide for information about connecting the unit to a network.
- Check whether the LEDs on the rear panel of the unit are blinking. If they are not, replace the Ethernet cable that connects the unit to the LAN.
- On MVG and UVG400 units, make sure the router is enabled.
  
  Additional information: *LAN Settings*, page 38
- On MVG and UVG400 units, ensure that the short Ethernet cable connecting the Video Gateway component of the Video Gateway to the unit’s router is properly inserted into both connectors (the top-most Ethernet connector on the right and the Ethernet connector immediately below it).
- On MVG and UVG400 units, if both Ethernet cables are functional and properly inserted into their connectors but the LEDs on the rear panel of the unit are not blinking, contact technical support.
- Replace the Ethernet cable that connects the unit to the LAN.
- Contact technical support.

### 14. Problem:
The Power LED on the front panel of the unit lights up, but the unit cannot be accessed by any external devices.

**Solutions:**
- Ensure that you are using the power supply cable that came with the unit. (If you use certain types of incompatible power supply cables, the power LED will light up, but the unit will not have sufficient power to perform any other functions. For example, be sure not to use the cable from an HVG400 200 unit with an HVG400 400, a UVG400 400, or a CVG.)
- Restart the unit and observe the Power LED on the front panel. The normal power-up sequence includes a number of flashes: The LED starts out green, flashes orange, turns green again, flashes five times, and, finally, when the start-up process is completed and the unit is operating normally, blinks every second.
- If the unit completes part of the start-up sequence and then restarts without completing the process, try reinstalling the firmware using *Catch Boot*.
  
  Additional information: *Catch Boot Operation*, page 188
- If the unit completes the entire start-up sequence and then restarts, try restoring the factory settings.
  
  Additional information: *Restoring Factory Settings*, page 199
- If the LED displays as a solid green at power-up, or displays as a solid green and then a solid orange but does not flash, the unit is unusable. Contact your vendor for additional assistance.
15. Problem:
The unit does not turn on – the Power LED on the front panel does not light up and the unit cannot be accessed by any external devices.

Solutions:
- Check the power connections and cables.
- Contact your vendor for assistance.

Note: Do not open the Video Gateway. It contains no user-serviceable parts.

16. Problem:
The unit disconnects from and reconnects to SVMultiClient every few minutes.

Solutions:
- Check that the external LAN connection is connected to the Ethernet Out connector on the rear of the unit.
- Contact your vendor for assistance.

17. Problem:
The internal speaker on the HVG400 is enabled but sound that is transmitted from a client device is not audible.

Solution:
Ensure that the Mute button on the rear of the unit is turned off.

Additional information: Configuring General System Settings, page 21 (in particular, see the note about the Speaker field on page 87)

18. Problem:
WiFi is enabled in the WiFi screen, but the Video Gateway does not connect to any of the access points; all the configured access points are “Not in Range.”

Solutions:
- Ensure that the access points are running and are in range of the Video Gateway unit.
- Ensure that the WiFi antenna is securely attached to the WiFi connector on the rear panel of the unit.
- Ensure that the Video Gateway is not configured to function as a WiFi access point; if it is configured to function as an access point, it cannot also connect to other access points.

Additional information: WiFi, page 47
- If the Video Gateway is installed in an insulated container, make sure the container is made of plastic, not metal. Metal interferes with the WiFi signal.

  Additional information: The Video Gateway's installation guide.
Appendix A: Viewing Video on a CCTV Monitor (TV-Out)

This appendix explains how you can view video on a CCTV monitor if one is connected to your Video Gateway. These instructions assume that a supported CCTV monitor is connected to your Video Gateway and TV-Out is activated in the unit’s configuration (see Configuring a CCTV Monitor (TV-Out), page 25). For information about acquiring and connecting a CCTV monitor to your Video Gateway, please refer to the installation guide.

If a CCTV monitor is connected to your Video Gateway, you can view video on it. The default display is defined in the unit’s configuration (see Configuring a CCTV Monitor (TV-Out), page 25). The following options are available:

- Full-screen display of live video from one of the cameras
- Full-screen display of live video that loops from one camera to the next at specified intervals
- Split-screen display of live video from all of the cameras

Figure 245: Split-screen displays video from all cameras simultaneously
When the Video Gateway unit starts up, the monitor displays a startup screen containing the name of the unit, its private IP in the local network, the firmware version, and a video pane displaying live video from one of the cameras connected to the unit. If mouse/touch is activated, a Done button also appears. After a few seconds, this display is replaced by the default video display.

NOTE: If the unit is configured to connect to an external LAN using DHCP (see LAN Settings, page 38), [DHCP] appears after the IP address. If the IP address was not yet assigned when the startup screen was displayed, 0.0.0.0 appears instead of the IP address. If mouse/touch controls are available (see below), you can see the correct IP in the Sys Info screen (see Viewing System Information on the Monitor, page 234) after it is assigned.

The default display can be changed on the fly using one or both of the following methods:
- **Mouse/Touch:** HVG400 and UVG400 models are supplied with a mouse. If the mouse is connected to the Video Gateway, you can use it to perform a variety of operations on the monitor: changing the sizes of the camera panes, selecting cameras, activating PTZ camera controls, and playing recorded video. The same operations can be performed on MVG, CVG, and CVG-M units if they are connected to supported touchscreen monitors. In this case, touching the screen activates the same features that would be activated on the other models by clicking the left mouse button.

- **Push-button switch:** If a switch is connected to the relevant sensor connector on the rear panel of the unit, you can use the switch to cycle through the various available display types. However, you can only view live video, and PTZ controls are not available.

**NOTE:** Mouse/touch controls only work if they are enabled in the configuration, and a push-button switch can only be used if the relevant sensor connector is configured properly and the option is enabled. For additional information, see Configuring a CCTV Monitor (TV-Out), page 25; Configuring a Sensor to Control CCTV Display, page 127.

The rest of this appendix explains how to use the mouse/touch controls to perform various operations. For information about connecting the supplied mouse or a supported touchscreen monitor, please refer to the Video Gateway unit’s installation guide.

**NOTE:** If you are using a touchscreen, it is recommended that you calibrate it before you use it for the first time. For information about how to do this, please consult the manufacturer’s documentation or your vendor. In addition, for optimal precision and sensitivity, it is recommended to use a pen, a pencil, or a stylus to tap the screen. Do not press hard or stab the display — the screen is quite delicate!

### Using Mouse/Touch Controls

If mouse/touch controls are set up and enabled on your Video Gateway (see page 210), you can perform the following actions:

- Switch from split-screen to full-screen display
- View recorded video
- Edit and download recorded video
- Configure picture and display properties
- View system settings
- Control PTZ cameras

These actions are performed through a menu that can be displayed on the monitor’s screen.

**To open the monitor’s main menu:**

- Click/tap anywhere on the screen. The menu is displayed on the left side of the screen. A single quarter-screen camera pane is displayed in the upper-right corner of the screen.
NOTE: If the display at the time you opened the menu consisted of a full-screen camera pane, the camera pane is reduced in size from full-screen to quarter-screen. If the display previously contained multiple quarter-screen camera panes, only the top-right pane is displayed.

The menu contains the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Selects the type of video display and activates or deactivates looping from camera to camera</td>
</tr>
<tr>
<td>Playback</td>
<td>Plays recorded video</td>
</tr>
<tr>
<td>Edition</td>
<td>Enables you to select a number of excerpts from recorded video for viewing or downloading to an FTP server</td>
</tr>
<tr>
<td>Config</td>
<td>Configures various display options</td>
</tr>
<tr>
<td>Sys info</td>
<td>Displays the name and network settings of the Video Gateway</td>
</tr>
</tbody>
</table>
| PTZ | Enables you to activate the controls of PTZ cameras  
**Note:** This option only appears in the menu if the PTZ controls of at least one camera are activated in the unit's configuration. |
| Fix cursor | In some cases, the image of the cursor can become slightly distorted, such that it is difficult to identify the exact location at which it points. If this occurs, select this option to return the cursor to its normal arrow form (↑).  
**Note:** If the cursor is not distorted, selecting this option may cause it to become distorted. Furthermore, selecting this option repeatedly may cause the unit to crash, such that it must be restarted manually. |
| Done | Closes the menu |
Setting the Video Display Layout

You can switch the video display from full-screen to split-screen, or vice-versa, and choose to loop the full-screen display from camera to camera.

To select a video display layout:

1. In the main monitor menu, select Display. The Display menu opens, with the current video display setting highlighted:

   ![Display menu]

   Figure 249: Display menu

2. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUAD</td>
<td>Set the display to a split screen, in which the display is divided into four video panes, and video from up to four cameras is displayed simultaneously.</td>
</tr>
<tr>
<td>VGA [1] [2] [3] [4]</td>
<td>Select the number of a camera for full-screen display. For example, select 1 to display live video from Camera #1. <strong>Note:</strong> Cameras that are not enabled do not appear in the list.</td>
</tr>
<tr>
<td>SWITCH</td>
<td>Display full-screen video, and loop from one camera to the next. <strong>Note:</strong> The default interval is set in the unit’s configuration. You can modify it on the monitor, if you wish (see Adjusting Loop Interval and Screen Saver Settings, page 229).</td>
</tr>
<tr>
<td>NONE</td>
<td>Do not display any video.</td>
</tr>
<tr>
<td>Done</td>
<td>Close the menu without making any selections.</td>
</tr>
</tbody>
</table>

The display option you selected is implemented, and the menu is closed.
Playing Back Recorded Video

If the Video Gateway is configured to record video, either continuously or in response to events (see Video Recording Settings, page 105), you can view the recorded video on the monitor. You can select the recorded video to view by start time or by event (VMD or sensor).

To play recorded video:

1. In the main monitor menu, select Playback. The Playback menu opens, with the default settings highlighted.

![Playback menu](image)

**Figure 250: Playback menu**

2. Under Select By, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>To select the video for playback by selecting start and end times</td>
</tr>
<tr>
<td>Sensor</td>
<td>To select the video for playback by selecting a sensor event</td>
</tr>
</tbody>
</table>

The selected option is highlighted.

3. Under Camera, select the number of the camera from which you want to see the recorded video. For example, select 1 to display recorded video from Camera #1. The selected option is highlighted.

4. Under Display, select the desired playback size:
   - SIF: Quarter-screen
   - VGA: Full-screen

The selected option is highlighted.

5. Select Next. The relevant playback selection screen opens. If you selected playback by time, the Time Selection screen is displayed; if you selected playback by sensor, the Sensor Selection screen is displayed. You can use these screens to select the video you want to see and start playback in the Playback screen. Follow the instructions in the next sections (see Playback by Time, page 214, and Playback by Sensor, page 214) to select the recorded video you want to see.
Playback by Time

If you selected playback by time in the Playback menu, the Time Selection screen opens.

![Time Selection screen](image)

*Figure 251: Time Selection screen*

**To play back recorded video by time:**

1. Under From, select the date and time at which you want to begin playback, and under To, select the date and time at which you want to end playback, as follows:
   - Select the value you want to modify (e.g., in the figure above, under From, select “12” if you want to change the minute value of the start time), or select the right and left arrows ( ) to scroll through all of the values. A box appears around the selected value.
   - Select the up and down arrows ( ) as necessary to modify the selected value.
   The duration of the selected time period appears under Duration.
   **Note:** To close the screen and return to live video display, select Done.

2. Select Play. The Playback screen opens, and the video is played, beginning with the specified start date and time, in the size you specified in the Playback menu. Playback controls appear in the upper left of the screen. See *The Playback Screen, page 216*, for information about the Playback screen.

Playback by Sensor

If you selected playback by sensor in the Playback menu, the Sensor Selection screen opens. The screen contains a list of the sensors connected to the selected camera (including the camera’s VMD, if it is activated).
To play back video of an event that was detected by a sensor:

1. In the Sensor Selection screen, select the sensor that triggered the event. The Date Selection screen opens and displays a list of all the dates for which there is recorded video of events that were triggered by the selected sensor:

2. Select the desired date. The Event-Time Selection screen opens and displays a list of the start times and durations of the events recorded on that date. (The durations appear in parentheses after the time, in seconds)
3. Select the down or up arrows of the scroll bar to display additional event times, if necessary.

   Note: Selecting the scroll bar itself does not scroll the list; only the arrows at the top and bottom of the scroll bar can be used to scroll.

   Note: To close the screen and return to live video display, select Done or select the button above the menu.

4. Select a time. The Playback screen opens, and the video is played, beginning with the specified start date and time, in the size you specified in the Playback menu. Playback controls appear in the upper left of the screen. See The Playback Screen below for information about the Playback screen.

The Playback Screen

The Playback screen contains a camera pane in which the selected video is played, as well as playback and navigation controls. If the display options call for a timestamp and/or the camera name, they are superimposed on the camera pane. For information about setting these options, see Configuring a CCTV Monitor (TV-Out), page 25; Adjusting On-Screen Information Display, page 231.
NOTE: If you chose VGA playback size in the Playback menu, playback is full-screen, and the controls overlap the picture. If you chose SIF, playback is in a camera pane at the upper right of the screen.

Playback continues for about 24 hours unless you use one of the playback controls or navigation buttons to stop it.

To use the playback controls:

- Select the buttons as follows:

<table>
<thead>
<tr>
<th>Playback Control</th>
<th>Description</th>
</tr>
</thead>
</table>
| Stop             | Stop playback.  
|                  | To resume playback, select Play. Playback resumes from the original start time. |
| Pause            | Pause playback.  
|                  | To resume playback, select Play. Playback resumes from the pause time. |
| Play             | Resume playback after playback has been paused or stopped. |
| Increase speed   | Increase playback speed. Each click/tap increases speed by 2X (2X, 4X, 8X, 16X). (The current playback speed is indicated to the right of this button.) |
| Decrease speed   | Reduce playback speed. Each click/tap reduces speed by 2X (16X, 8X, 4X, 2X). (The current playback speed is indicated to the left of this button.) |

The navigation buttons allow you to end the playback session before it is closed automatically.

To use the navigation buttons:

- Select the buttons as follows:
Editing and Downloading Video Excerpts

You can store a list of excerpts from recorded video that are of particular interest to you. You create the list by means of the CCTV monitor interface, and it is stored on the Video Gateway unit. You can add new items to the list at any time, or clear the list and start creating a new one from scratch. As long as the video excerpts in the list are stored on the Video Gateway unit, you can play them on the monitor and download them to your FTP server.

The current list of excerpts is called the edition, and each video excerpt it contains is called an item. You can play the items in the current edition on your CCTV monitor whenever you wish. When you do so, the items play one after the other in the order in which they appear in the list. In addition, you can download the entire contents of the edition to your FTP server. The items are incorporated into a single video file for downloading.

The edition feature can be used to help you locate and keep track of important recorded video. For example, if an intruder is recorded by camera 1 when he enters a building, camera 2 when he enters a particular office, and camera 3 when he leaves the building, you can select the footage from each camera in which the intruder appears and create a single video recording containing the three excerpts. You can then play the three recordings on the monitor in succession in order to study them more carefully or show them to a supervisor or other security staff; you will not have to search for the relevant parts each time you want to see them. In addition, you can download a file containing all three recordings to an FTP server in order to save it for later use and distribute it to other viewers.

You can manage the edition in the Edition menu. The menu provides access to the feature’s controls and, at the top of the screen, shows the current name of the edition (if it has a name) and the number of items it contains.

To open the Edition menu:

- In the main monitor menu, select Edition.

![Edition menu](figure.png)
Naming the Download File

If you want to download the edition, you should assign a name to it. When you download an edition to the FTP server, this name becomes the name of the file. The current name of the edition appears at the top of the Edition menu.

To name the edition:

1. In the Edition menu, select Name. The Name screen opens. The field at the top of the screen displays the current name, if the edition has one. Below the field is a virtual keyboard you can use to modify the existing name or type one.

2. Select the “keys” of the virtual keyboard to type a name for the edition. The characters you select appear in the text field at the top of the screen.

3. When you have finished typing the name, select Done to save the name. The Name screen closes, and the Edition menu is displayed. The name you specified appears at the top of the menu.
Adding Items to the Edition

You can add one or more items to the edition. You can select an item to add either by selecting a time range or by selecting an event.

To add an item to the edition:

1. In the Edition menu, select Add. The Add menu opens.

2. Under Select By, select one of the following:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>To select the item by selecting start and end times</td>
</tr>
<tr>
<td>Sensor</td>
<td>To select the item by selecting a sensor event</td>
</tr>
</tbody>
</table>

3. Under **Camera**, select the number of the camera from which the video was recorded. For example, select 1 to select recorded video from Camera #1.

4. Under **Display**, select the desired video frame size:
   - **SIF**: Quarter-screen
   - **VGA**: Full-screen

5. Select **Next**. The relevant recording-selection screen opens. If you chose to select the video by time, the **Time Selection** screen is displayed; if you chose to select the video by sensor, the **Sensor Selection** screen is displayed. Follow the relevant instructions below to select the video excerpt to add to the edition.

   **Note**: To close the screen and return to the **Edition** menu without adding any new items to the edition, select **Done**.

![Time Selection screen](image)

*Figure 260: Time Selection screen*
To select the video excerpt by time:

1. In the Time-Selection screen (figure 260), under From, select the date and time of the beginning of the excerpt, and under To, select the date and time of the end of the excerpt, as follows:
   - Select the value you want to modify (e.g., in the figure above, under From, select “12” if you want to change the minute value of the start time), or select the right and left arrows to scroll through all of the values. A box appears around the selected value.
   - Select the up and down arrows as necessary to modify the selected value.
   
   The duration of the selected time period appears under Duration.

   Note: To close the screen and return to the Edition menu without adding any new items to the edition, select Done.

2. Select Add. The excerpt is added to the edition. The Time Selection screen closes, and the Edition menu appears. The item counter at the top of the Edition menu indicates that a new item has been added to the edition. For example, it this is the second item that was added, (2 items) appears at the top of the menu.
Appendix A: Viewing Video on a CCTV Monitor (TV-Out)

To select the video excerpt by event:

1. In the Sensor Selection screen (figure 261), select the sensor that triggered the event. The Date Selection screen opens and displays a list of all the dates for which there is recorded video of events that were triggered by the selected sensor.

2. Select the desired date. The Event-Time Selection screen opens and displays a list of the start times and durations of the events recorded on that date. (The durations appear in parentheses after the time, in seconds)
Figure 264: Event-Time Selection screen

3. Select the down or up arrows of the scroll bar to display additional event times, if necessary.

   **Note:** Selecting the scroll bar itself does not scroll the list; only the arrows at the top and bottom of the scroll bar can be used to scroll.

   **Note:** To close the screen and return to the **Edition** menu without adding any new items to the edition, select **Done** or select the \[X\] button above the menu.

4. Select a time. The event is added to the edition. The **Event Time Selection** screen closes, and the **Edition** menu appears. The item counter at the top of the **Edition** menu indicates that a new item has been added to the edition. For example, if this is the second item that was added, (2 items) appears at the top of the menu (see figure 262).

**Viewing the List of Items in the Edition**

You can see a list of the items that are included in the edition.

![Image](image-url)

*To view the list of items in the current edition:*

- In the **Edition** menu, select **View**. The View screen opens and displays a list of the video items in the current edition. For each item, the camera, date, start time, and duration appear.
Playing the Edition

If you want to see the current contents of the edition, you can play the items on the monitor.

![View screen](image)

*Figure 265: View screen*

**To play the items in the edition:**

- In the **Edition** menu, select **Play**. The items in the edition are played on the screen.

Downloading the Edition

Once you have finished adding items to the edition, you can download the edition to your FTP server. The items in the edition are all inserted into a single file, in *srv* format (SerVision’s proprietary video format, which can be played by any SerVision video player), with the name that is currently defined for the edition, and downloaded to the FTP server defined in the unit’s configuration in the **FTP** screen (see *FTP Server Settings*, page 75).

**To download the current contents of the edition:**

1. In the **Edition** menu, select **Download**. The **Download** screen opens.
2. If you want to stop all video recording during the download, select Disable recording.
   Note: Selecting this option will reduce the time required for downloading, but, obviously, with the risk that important events will not be recorded. For additional information, see Download Optimizations, page 18.

3. Select Start. The current contents of the edition are downloaded to the FTP server.

Clearing the Edition

You can remove all of the items from the edition. This is useful, for example, when you have finished downloading the current edition and want to begin creating a new one.

⚠️ To remove all of the items from the edition:
- In the Edition menu, select Clear. The list is cleared, and the Clear screen appears and displays the message, No items.
Configuring Display Options

The default display options are defined in the unit’s configuration utility. You can modify these settings using the Config menu, and you can save the new settings in the unit’s configuration.

The Config menu provides access to three screens:

- **Picture Params screen**: Sets the brightness and contrast of each camera
- **TV-Out Params screen**: Sets the loop interval for the full-screen display that switches from camera to camera, activates and deactivates the screen saver, and sets the timeout for the screen saver
- **OSD Params screen**: Configures the on-screen display (OSD) of the camera name and of the timestamp for recorded video

To open the Config menu:

- In the main monitor menu, select **Config**.
Adjusting Camera Brightness and Contrast

Initial camera brightness and contrast settings are set in the configuration utility (see Configuring Camera Settings, page 92). You can modify these settings on the monitor, and, if you wish, save the new settings to the unit’s configuration.

**NOTE:** Changing these parameters immediately affects all the video streams from the relevant camera, both live and recorded, as explained below (see step 5, page 229).

**To modify the brightness or contrast of a camera:**

1. In the **Config** menu, select **Picture Params**. The **Picture Params** screen opens:
Appendix A: Viewing Video on a CCTV Monitor (TV-Out)

Figure 269: Picture Params screen

2. Under Camera, select the number of the camera whose settings you want to modify. Video from this camera is displayed in the upper-right corner of the screen.

3. Under Brightness, select the arrows to the right or left of the slider bar to adjust the brightness, as follows:
   - Single arrows – and : Adjust the brightness in small increments.
   - Double arrows – and : Adjust the brightness in large increments.

4. The camera settings are changed, and the video displayed in the camera pane in the upper left of the screen changes accordingly.

5. Under Contrast, select the arrows to the right or left of the slider to adjust the contrast, as described in step 3 above.

6. The camera settings are changed, and the video displayed in the camera pane in the upper left of the screen changes accordingly.

5. When the brightness and contrast are set as you want them to be, exit the menu by selecting one of the following buttons:
   - Done: Return to live video display. The settings remain in effect until they are manually changed again or until the Video Gateway restarts. When the unit restarts, the previous settings are implemented again.
   - Save: Save the settings on the Video Gateway. The next time the unit restarts, the unit’s configuration is updated with the new settings. The settings remain in effect until they are manually changed again, either on the monitor or in the configuration utility.
   - Back: Return to the Config menu. The settings remain in effect until they are manually changed again or until the Video Gateway restarts. When the unit restarts, the previous settings are implemented again.

Adjusting Loop Interval and Screen Saver Settings

Initial loop-interval and screen-saver settings are set in the configuration utility (see Configuring a CCTV Monitor (TV-Out), page 25). You can modify these settings on the monitor, and, if you wish, save the new settings to the unit’s configuration.
To modify the loop interval and screen saver settings:

1. In the Config menu, select TV-Out Params. The TV-Out Params screen opens:

   ![TV-Out Params screen](image)

   **Figure 270: TV-Out Params screen**

2. Under Switch Delay, select the up arrow ▲ to the left of the field or the down arrow ▼ to the right of the field to modify the loop interval. This value only affects the full-screen rotating display. This value indicates how many seconds the display will remain on each camera before switching to the next camera when the rotating display is active.

3. If you want to activate the screen saver, under Screen Saver, select Enabled. The Timeout field is added to the screen, and displays the current timeout value in hours and minutes (HH:MM format):

   ![Screen Saver enabled](image)

   **Figure 271: Screen Saver enabled**
4. Under **Timeout**, select the up and down arrows (↑ and ↓) to specify the hours and minutes of the screen-saver timeout. The screen saver is activated when the mouse has not been moved for this amount of time.

5. When you are finished configuring the switch delay and screen saver settings, exit the menu by selecting one of the following buttons:
   - **Done**: Return to live video display. The settings remain in effect until they are manually changed again or until the Video Gateway restarts. When the unit restarts, the previous settings are implemented again.
   - **Save**: Save the settings on the Video Gateway. The next time the unit restarts, the unit’s configuration is updated with the new settings. The settings remain in effect until they are manually changed again, either on the monitor or in the configuration utility.
   - **Back**: Return to the **Config** menu. The settings remain in effect until they are manually changed again or until the Video Gateway restarts. When the unit restarts, the previous settings are implemented again.

**Adjusting On-Screen Information Display**

The On-Screen Display (OSD) options control how information is displayed in the video panes. Each pane can have one or two banners superimposed on the video:

- **Lower banner**: When displayed, this banner indicates the name of the camera whose video is displayed in the pane. The name can be displayed as it appears in the configuration utility – for example, “Back Door” – or it can simply be the camera number – for example, “Camera 1.”
- **Upper banner**: For camera panes in which recorded video is being played, this banner can provide a timestamp, indicating the date and time at which the recording was made.

**NOTE:** Banners require a lot of system resources. If your system appears overloaded, try removing them.

The color of the lettering of the banners can be configured to maximize its visibility.

---

**Figure 272: Camera pane with Timestamp and Camera Name banners displayed (full-screen camera pane)**

Initial OSD settings are defined in the configuration utility (see *Configuring a CCTV Monitor* (TV-Out), page 25). You can modify these settings on the monitor, and, if you wish, save the new settings to the unit’s configuration.
To modify the OSD settings:

1. In the **Config** menu, select **OSD Params**. The **OSD Params** screen opens, and lists the various banner display options. A checkbox beside each option indicates whether it is turned on or off (✓ indicates the option is on; □ indicates it is off).

![OSD Params screen](image)

*Figure 273: OSD Params screen*

2. Select the checkbox beside an option to turn it on or off, as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera Name (live)</td>
<td>Display the name of the camera in live video camera panes. The name of the camera, as it appears in the Video Gateway's configuration, is displayed unless <strong>Camera Number</strong> (see below) is also selected.</td>
</tr>
<tr>
<td>Camera Name (playback)</td>
<td>Display the name of the camera in recorded video camera panes. The name of the camera, as it appears in the Video Gateway's configuration, is displayed unless <strong>Camera Number</strong> (see below) is also selected.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Display the date and time of recorded video.</td>
</tr>
<tr>
<td>Camera Number</td>
<td>When camera names are displayed, display them as Camera #x, rather than the name of the camera as it appears in the configuration. This option is recommended if the configured name of the camera contains non-English characters, because these characters will not display properly on the monitor.</td>
</tr>
</tbody>
</table>

*Note: If the Camera Name display is not turned on, this option has no affect.*

3. If you want to select a different banner color, select **Colors**. The color selection menu opens.

---

**NOTE:** Only the five standard banner colors (yellow, orange, black, blue, and red) can be selected directly on the monitor. If you want to select a custom color, you must do so through the unit's configuration utility. For additional information, see *Configuring a CCTV Monitor (TV-Out)*, page 25.
4. Select the desired color. The banners are displayed in the selected color.

5. When you have selected the banner color you want, exit the color selection menu by selecting one of the following buttons:
   - **Done**: Return to live video display. The settings remain in effect until they are manually changed again or until the Video Gateway restarts. When the unit restarts, the previous settings are implemented again.
   - **Save**: Save the settings on the Video Gateway. The next time the unit restarts, the unit’s configuration is updated with the new settings. The settings remain in effect until they are manually changed again, either on the monitor or in the configuration utility.
   - **Back**: Return to the **Config** menu. The settings remain in effect until they are manually changed again or until the Video Gateway restarts. When the unit restarts, the previous settings are implemented again.
Viewing System Information on the Monitor

You can view the following system information on the monitor:

- Name of the unit
- Main private IP of the unit
- Secondary (zero-conf) private IP of the unit
- Net mask
- Firmware version

To view system information:

- In the main monitor menu, select Sys info. The System Information screen opens:

![Image of System Information screen]

Figure 276: System Information screen

Using PTZ Controls

If cameras with PTZ controllers are connected to the Video Gateway, and the controllers are connected to the unit and activated in the unit's configuration, you can perform the following tasks on the monitor:

- Move the cameras using all the supported features of the camera: pan, tilt, and zoom
- Select and save a preset location
- Move the camera to a preset location

To use PTZ controls:

1. In the main monitor menu, select PTZ. The PTZ menu opens.
Appendix A: Viewing Video on a CCTV Monitor (TV-Out)

2. Under **Camera**, select the number of the camera whose PTZ controls you want to use. For example, select 1 to control Camera #1. **Note:** The list of cameras only includes cameras with PTZ capabilities that are configured to appear in the TV-Out display (see *Configuring a CCTV Monitor (TV-Out)*, page 25).

3. To move the selected camera, select the controls as follows:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Tilt Up" /></td>
<td>Tilt the camera up</td>
</tr>
<tr>
<td><img src="image" alt="Zoom In" /></td>
<td>Zoom in</td>
</tr>
<tr>
<td><img src="image" alt="Zoom Out" /></td>
<td>Zoom out</td>
</tr>
<tr>
<td><img src="image" alt="Tilt Down" /></td>
<td>Tilt the camera down</td>
</tr>
<tr>
<td><img src="image" alt="Pan Right" /></td>
<td>Pan to the right</td>
</tr>
<tr>
<td><img src="image" alt="Pan Left" /></td>
<td>Pan to the left</td>
</tr>
<tr>
<td><img src="image" alt="Home" /></td>
<td>Move to the home position of the camera</td>
</tr>
</tbody>
</table>

4. To move to a preset location, under **Preset**, click/tap the **Up** and **Down** arrows (▲ and ▼) until the number of the desired preset is displayed, and then select **Go To**. The camera moves to the selected preset location (if it is already assigned on the camera).

5. To set a preset:
   - Use the navigation controls to direct the camera to the desired location, as described in step 3.
Appendix A: Viewing Video on a CCTV Monitor (TV-Out)

- Under **Preset**, click/tap the **Up** and **Down** arrows (&&! and $$) until the number you want to assign to the preset is displayed.
- Select **Set**.

The location is assigned to the preset number.

**Recording Status Display**

If the unit was configured to display the system’s recording status in the monitor (see **Display Recording Status**, page 29), the status is displayed in the lower-right corner of the screen. The status information indicates whether video recording is functioning properly and, if it is, displays the current recording status of each camera.

When recording is functioning properly, a status message based on the following template is displayed:

```
HD:OK REC 0[WP:]X0 1[WP:]X1 2[WP:]X2 3[WP:]X3
```

The template contains the following items:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD:OK</td>
<td>Hard drive is functioning properly (status: OK)</td>
</tr>
<tr>
<td>REC</td>
<td>Recording is functioning properly</td>
</tr>
<tr>
<td>0[WP:]X0</td>
<td>Camera 1 recording status</td>
</tr>
<tr>
<td>1[WP:]X1</td>
<td>Camera 2 recording status</td>
</tr>
<tr>
<td>2[WP:]X2</td>
<td>Camera 3 recording status</td>
</tr>
<tr>
<td>3[WP:]X3</td>
<td>Camera 4 recording status</td>
</tr>
</tbody>
</table>

The recording status displayed for each camera has two parts:

- **WP:** appears if write protection is enabled for the camera. Otherwise, it does not appear.
- **Xi:** is the current recording status of the camera. It can be one of the following values:

<table>
<thead>
<tr>
<th>Recording Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>No recording</td>
</tr>
<tr>
<td>C</td>
<td>Continuous recording</td>
</tr>
<tr>
<td>T</td>
<td>Event-triggered recording: recording is not currently underway</td>
</tr>
<tr>
<td>W</td>
<td>Event-triggered recording: recording of the pre-alarm part is underway</td>
</tr>
<tr>
<td>w</td>
<td>Event-triggered recording: recording of the Event, and/or of the post-alarm part, is underway</td>
</tr>
</tbody>
</table>

For example, **HD:OK REC 0C 1WP:C 2T 3N** means that four cameras are connected to the unit, all four are recording as configured, and their recording statuses are as follows:

- Camera 1: Continuous
- Camera 2: Continuous and write-protected
- Camera 3: Event-triggered (no recording is underway)
- Camera 4: No recording
NOTE: For information about configuring recording settings, see Video Recording Settings, page 105.

When recording is not taking place, either because the recorder is being initialized or because of an error, one of the following status messages is displayed:

<table>
<thead>
<tr>
<th>Status Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD:OK REC:start</td>
<td>Recording is being initialized</td>
</tr>
<tr>
<td>HD:ERR</td>
<td>Hard drive error: The hard drive could not be initialized.</td>
</tr>
<tr>
<td>HD:OK REC:ERR init</td>
<td>Recording initialization error: The hard drive was initialized, but recording could not be initialized. This error indicates that there were bad parameters, bad sectors, etc.</td>
</tr>
<tr>
<td>HD:OK REC:ERR buf</td>
<td>Error allocating buffers for recording</td>
</tr>
<tr>
<td>HD:OK REC:ERR time</td>
<td>Invalid system time: Recording is disabled, and will restart when the time is set, either via the network or via GPS (on MVG and CVG-M units)</td>
</tr>
</tbody>
</table>
Appendix B: LAN Settings

All Video Gateways can connect to a local network (LAN) via an Ethernet cable. When a Video Gateway unit is connected to a LAN, it can connect to other networks through the LAN. For example, if the LAN is connected to the internet, the Video Gateway can connect to the internet through the LAN. This connection enables Video Gateway to send video and other data to client devices over the internet. Some Video Gateway models can connect to cellular and Wi-Fi networks as well as LANs.

When a Video Gateway unit is connected to a network, it is assigned a local IP address within that network. Units that are connected to more than one network simultaneously can have more than one IP address at a time – one on each network to which they are connected. The IP of the unit on each network must conform to the requirements of that network.

In order to connect to a Video Gateway unit from a client application that is not on the same local network, you must use the public IP address of the unit – the address that is assigned to the network’s gateway (router) on the external network. In addition, port forwarding for the unit must be set up on the network gateway in order for a connection to be established.

About the Local IP Address of the Unit

The local IP address of the unit identifies it within the LAN. It can be static – a fixed address that is assigned manually in the unit’s configuration – or dynamic – assigned by a DHCP server on the LAN (see LAN Settings, page 38). If the primary local IP used by the Video Gateway is dynamic, this means that it may be assigned a different IP address each time it is turned on and connects to the local network. Whenever possible, it is recommended to assign a static IP to the Video Gateway.

Every unit has a factory-configured default static IP address, which appears on the sticker on the underside of the unit. Normally, this address is 192.168.1.210. You can assign a different static IP address to the unit during the configuration process, or opt to use a dynamic IP address.

If the unit has a static IP address, a second IP address is also assigned to it automatically by the system; this address serves as a backup address through which the unit can be accessed if problems arise with the first IP address. The address is assigned using the ZeroConf protocol, and begins with 169.254 (for example, 169.254.2.56); the last two values in the address vary depending on which ZeroConf addresses are available in the network.

About the Public IP Address of the Unit

The network gateway that connects the LAN to an external network such as the internet has two IP addresses: an internal IP address by which it is identified in the LAN, and an external IP address by which it is identified on the external network. If the external network is the internet, the IP is called a public IP. The public IP address of the network gateway is assigned to it by the internet service provider (ISP). To connect to the unit remotely – either using a client application or the configuration utility – you must connect using the gateway’s public IP address and the port that was defined for the purpose on the gateway (see Ports, page 17).

In some cases, it is problematic to connect remotely to a network gateway because it either does not have a public IP address at all or the public IP address is dynamic. To ascertain whether your network gateway has a public IP address, and whether it is static or dynamic, contact your ISP. If the ISP cannot allocate a public IP to the gateway, you must use a SerVision proxy service to connect to the unit remotely. If the ISP allocates a dynamic public IP address to the unit, you can use a dynamic DNS (DDNS) service to facilitate internet connections to the gateway. For additional information, see Proxy and DDNS Settings, page 57.
Appendix C: Networks Managed by SerVision Routers

MVG and UVG400 models have built-in SerVision routers. Each of these routers manages a small local network (LAN) that can include up to four devices – the Video Gateway itself and up to three other devices. For example, you could connect a PC and an IP-based cash box to the router, and they would all be part of the unit’s local network.

The SerVision router makes it possible to connect MVG and UVG400 units to multiple networks – cable-based, cellular, and WiFi – at one time.

Because the router is part of both the internal LAN and one or more external networks, it has two types of IP addresses:

- **Local IP**: An IP address on the internal LAN. This IP address identifies the router within the network that it manages. It is static (fixed) and is 172.20.233.1.
- **External IP**: An IP on each external network to which it is connected (cabled LAN, WiFi, and/or cellular). These IPs function as the public IP addresses of the Video Gateway units themselves, and are assigned by the system administrators of the relevant networks.

The router contains a DHCP server that can automatically assign IP addresses to devices that are plugged into its Ethernet ports. If you will not need to access a connected device remotely, you can configure the device to acquire its IP from this DHCP server. In this case, the device will be able to connect to the external network, but remote devices will not be able to access it. If you want to access the device remotely, you should manually configure its IP address and other network settings as described below (for information about how to configure the network settings of the device, consult the device’s documentation), and set up port forwarding for the device as described under Port Forwarding, page 55.

**NOTE:** The Video Gateway component of the Video Gateway automatically connects to the router component when the unit starts up. The router's DHCP server assigns an IP address to the Video Gateway component and port forwarding is automatically configured.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Assign a static IP address to the device. The IP must be in the range 172.20.233.2 through 172.20.233.99.</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.20.233.1</td>
</tr>
<tr>
<td>DNS</td>
<td>172.20.233.1</td>
</tr>
</tbody>
</table>