



VMS2000 Server

User's Guide

D017-0001-200-05

Note: Please read this manual thoroughly before operating this unit and retain it for future reference.

1 Table of Contents

- 2 Terminology..... 3
- 3 Read Me First..... 5
- 4 Overview - VMS Server 6
- 5 VMS2000 Server 7
 - 5.1 Main Window 7
 - 5.2 Updated: Menu 10
 - 5.3 Server Setup 11
 - 5.3.1 Reset Login Password 13
 - 5.3.2 Load Camera Config..... 14
 - 5.3.3 Save Camera Config..... 14
 - 5.3.4 IP Camera Setup..... 15
 - 5.3.5 DNP Setup..... 22
 - 5.3.6 Snapshot Setup 23
 - 5.3.7 Edit Remote Servers 24
 - 5.3.8 Thermal Data Setup 25
 - 5.3.9 Storage Options 25
 - 5.3.10 PTZ Camera Setup 26
 - 5.3.11 Edit Signal Loss Alarm..... 27
 - 5.3.12 HTTP API Settings 28
 - 5.3.13 OS / Hardware Options 30
 - 5.3.14 IEC61850 Setup 31
 - 5.3.15 Reserved..... 32
 - 5.3.16 Advanced setup..... 32
 - 5.4 Alarm Setup 33
 - 5.5 Stop Capture..... 36

2 Terminology

These are terms and abbreviations used in this document:

Alarm	<ul style="list-style-type: none"> - The detection of a state change is recording a new entry in the log. E.g. Digital Input wired to door contact is changing state from closed to open; the video analytics captures (trigger) a Motion Detection; the average temperature is above threshold value. - Defaults: System Information, DVS Trouble, Video Signal Lost.
Event	<ul style="list-style-type: none"> - Repetitive action based on a time schedule. E.g. snapshots every 15 minutes. - A one-time action triggered by an Alarm. E.g. Turn on buzzer when Door opens; Zoom camera 1 when Motion Detection is captured on camera 2. (Digital Output operation, VMS Server restarted)
Digital Input/ Output (DI/O)	<ul style="list-style-type: none"> - A Digital Input (DI) monitors the state of a contact and the output is passed to the DVS as a binary signal 1 or 0. E.g. A door open is '0' and a door closed is binary '1'. - The Digital Output (DO) executes a binary command from the DVS by operating a relay. E.g. The relay output is closed to turn the lights on.
Video Analytics	<ul style="list-style-type: none"> - Software algorithm that analyzes video images based on preset rules and generates alarms.
PTZ Camera	<ul style="list-style-type: none"> - The Pan-Tilt-Zoom camera is capable of remote directional and zoom control.
PTZ Preset	<ul style="list-style-type: none"> - A set of coordinates for position and zoom.
DVS	<ul style="list-style-type: none"> - The Digital Video Server (<i>dedicated</i>) is a specialized hardware used for capturing, processing and recording video.
DNP3	<ul style="list-style-type: none"> - Distribute Network Protocol v3: Real-time communication protocol (Ethernet or Serial) used by the SCADA systems.
SCADA	<ul style="list-style-type: none"> - Supervisory Control and Data Acquisition: a control system for supervisory management of electric utilities and processing plants.
SQL database	<ul style="list-style-type: none"> - Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database management system.
Archive Server	<ul style="list-style-type: none"> - A dedicated computer and storage that manages the retrieval of data from each DVS for long-term storage.
VMS	<ul style="list-style-type: none"> - Video Management Software
VMS Client	<ul style="list-style-type: none"> - Interface for configuring and operating the Video Management System
VMS Server	<ul style="list-style-type: none"> - Software application running on DVS
Web Server	<ul style="list-style-type: none"> - Server software dedicated to serve contents to the World Wide Web.
Web browser	<ul style="list-style-type: none"> - A web browser is a software application for accessing information on the World Wide Web. Currently supported Internet Explorer Version: 8, 9, 10 and 11.
LAN	<ul style="list-style-type: none"> - Local Area Network
WAN	<ul style="list-style-type: none"> - Wide Area Network

IP Address	- An Internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network by IT Department
IP Port	- A number (1-65355) assigned by software developers to applications for communication. E.g. Web server port 80; SQL port 2301;
UDP, TCP, HTTP	- Communication protocols used for sending packets of data over the network.
fps	- Frames per second are expressing the number of pictures processed in a second.
Kbps	- Kilobits per second are expressing the bandwidth used to stream the compressed video.
Video stream bandwidth	- Amount of data that can be transmitted at a given time; for digital communication is expressed in bits per seconds. E.g. 290kbs = 290,000 bits per seconds
Video aspect ratios	- Aspect ratios are expressed in the form “width x height” and refers to the width of a picture in relation to its height. Most common: 4x3 also known as VGA; 16x9 for 720p/1080p

3 Read Me First

This chapter describes how the guide is organized and how to use it. The document is divided into sections ordered by chronology of use and frequency of use.

Section 4 - Overview

This section presents the architecture of the VMS and how it fits in the system distribution.

Section 6 – VMS2000 Server

The settings are listed in no specific order. You will have to configure only what is necessary for your installation.

Throughout this manual you will find two distinctive paragraphs:

Best practice – recommendations based on FAE experience and customer feedback.

Troubleshooting - tests and solutions for most common situations.

4 Overview - VMS Server

The **VMS** - Video Management Software is a complete monitoring solution that integrates these functions:

1. Live video viewing and remote camera control,
2. Video data archive management
3. Video analytics algorithms for intrusion detection
4. Real-time alarms in a SCADA system via the DNP3
5. Event notification through email
6. Remote access services.

The VMS is built on a Server - Client architecture. The Server application runs on a dedicated Substation Hardened DVS – Digital Video Server. The DVS is installed in the substation and is connected to PTZ Cameras, IP Cameras, Thermal Cameras, Card Reader and other peripherals through the built in Inputs/Outputs – see In Figure 4-1.

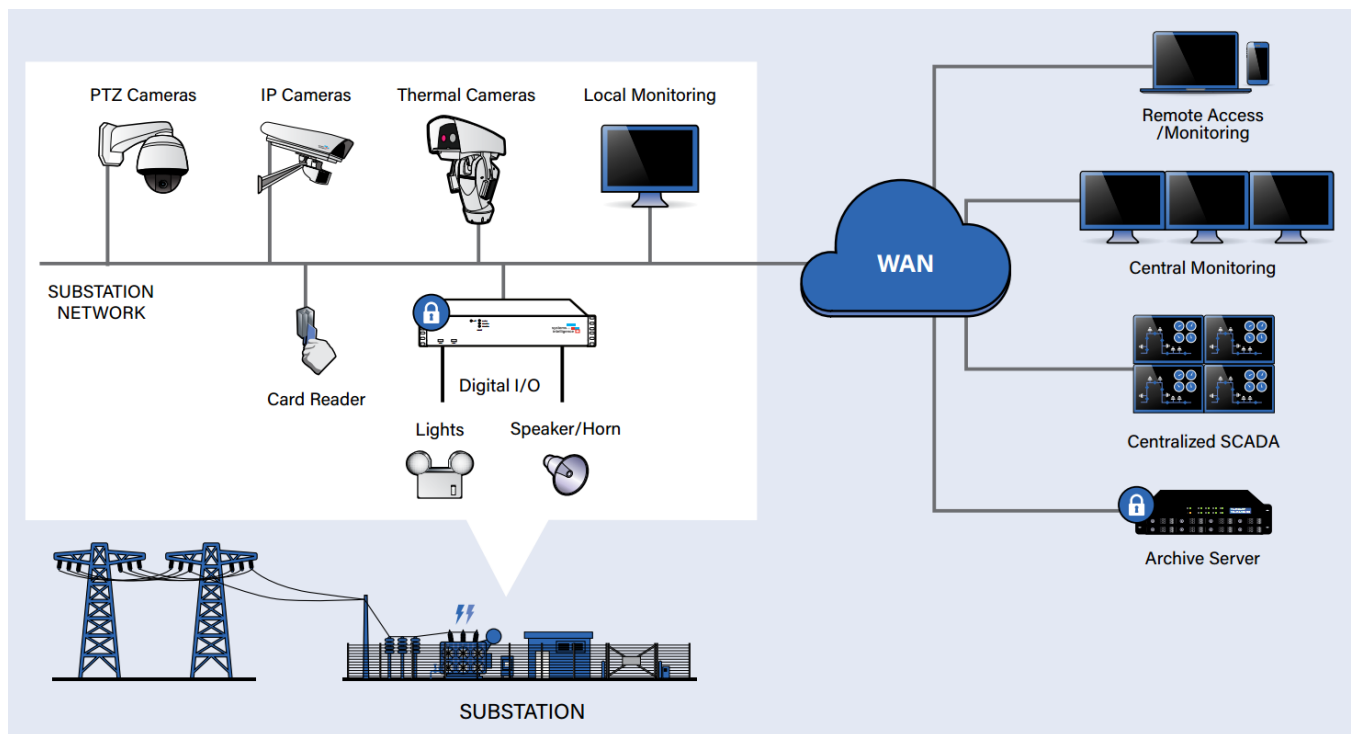


Figure 4-1 System Architecture

The Client acts as Central Control and can run on most Windows PC – see Figure 4-1. The Client application is used for configuration and everyday operations.

The Client stores the DVS connection information, view structure and users' preferences. It doesn't store any settings related to video. These settings are stored in the Server.

Best practice: Changes to the VMS Client configuration must be done by a single user with administrator credentials.

5 VMS2000 Server

The VMS Server is a software application that runs on specialized hardware, is factory installed and licensed. This chapter will describe all the buttons and configurations available to setup the DVS. You must physically have access to the DVS or use a Remote Desktop application. For remote connection you need the IP address of the DVS Server and the login information. You will have to configure only what is necessary for your installation.

5.1 Main Window

The VMS2000 Server application runs in full screen mode and the main user interface is shown in Figure 5-1. There are three areas highlighted:

- The “Title” bar of the window presents the system information: software version, hardware information and the IP address.
- The “Menu” on the left presents two buttons “Log in” and “Info”. After you are logged in you have access to all options – see section 5.2.
- The “Log” displays the local DVS system status messages. This information may help with solving warnings and troubleshooting issues.
- The “VMS License information” is displayed at the top of the Log window. This information lists the features of the VMS2000.

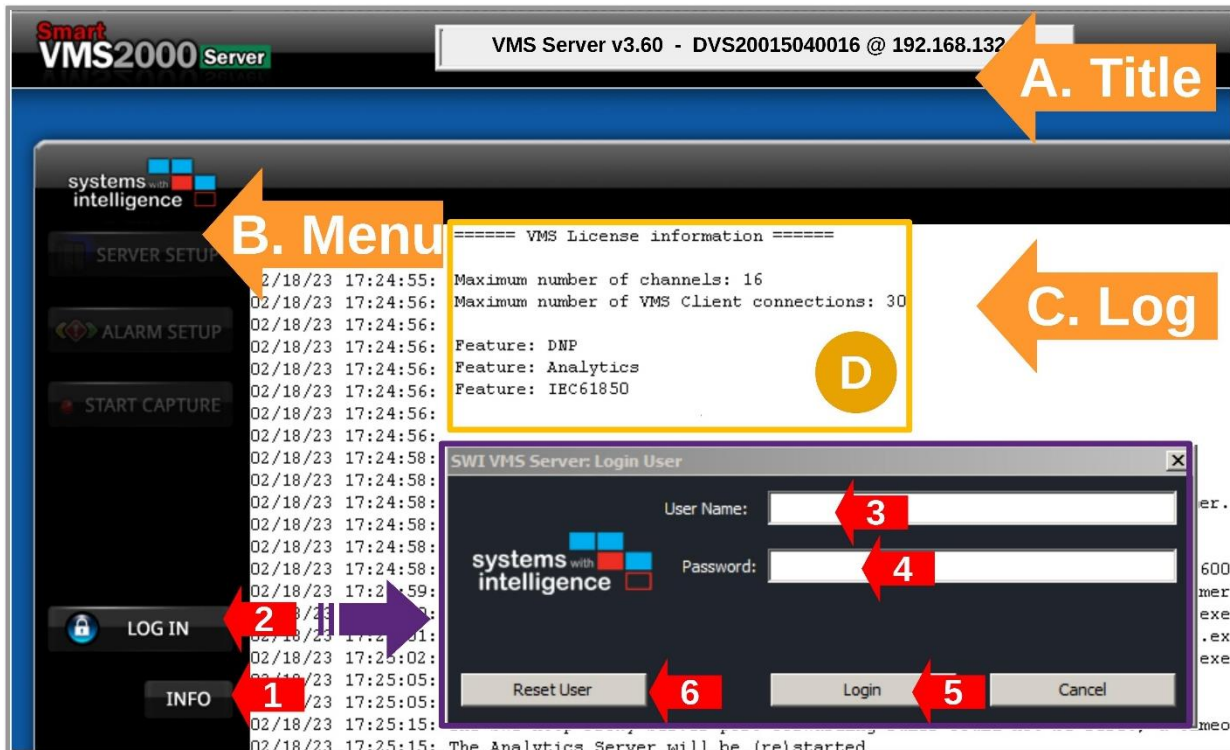


Figure 5-1 Main Interface

The Menu presents only the two buttons before logged in:

- Info – press this button and the dialog in Figure 5-2 is displayed. It displays the version of the application and the license information.



Figure 5-2 Information

2. Log in – press this button and the dialog requesting credentials is displayed.
3. User Name - when the unit first boots, only the Login button will be accessible and when pressed it will ask you to set username and password. Subsequent access to the user interface will require this username and password. Please retain this information. Only on the first start, if the VMS is not configured. By default, the ones sent to customer are already set.
4. Password – type the password in this field.
5. Log in – press this button to complete the process. The buttons in the menu are enabled as in Figure 5-4.
6. Reset User – press this button in case you lost the username/password or want to change the log in information. After you pressed this button the dialog box shown Figure 5-3 is displayed.

Follow this procedure to reset the user credentials – see Figure 5-3.

- A. Use this section in case you lost the log in credentials.
 1. Copy the “Passcode” and e-mail it to SWI Support Team and you will receive a Key.
 2. Enter the “Key” you received from SWI and proceed to step 5.
- B. Use this section to change the user log in information.
 3. Current User – enter the current information.
 4. Current Password – enter the current information and proceed to step 5.
- C. Use this section to enter the new user credentials.
 5. New User Name – type in the new name.
 6. New Password – type in the new password.
 7. Confirm Password – retype the password and proceed to step 8.
 8. Change – press this button to preserve the changes.
 9. Cancel – press this button to discard the changes.

SWI VMS Server: Reset User

Authorization (Requires One Selection Below)

Enter the corresponding key to authorize the change.

Passcode: **1** **A**

Key: **2**

Enter user name and password to authorize the change.

Current User: **3** **B**

Current Password: **4**

New User Info

Leave user name blank if want to reset to startup conditions.

New User Name: **5** **C**

New Password: **6**

Confirm Password: **7**

8 **9**

Figure 5-3 Reset User

5.2 Updated: Menu

The Menu on the left of the frame (as shown in Figure 5-4) is available after you log in.

	<p>These configurations are available:</p> <ol style="list-style-type: none"> 1. Server Setup: configure DVS and VMS2000 Server software parameters - see section 5.3. 2. Alarm Setup: configure parameters associated with Alarm and Event manager, specifically email notification – see section 5.4. 3. Start/Stop Capture: start or stop local recording of video. Note that video recording will start on DVS boot-up depending on the parameters set in VMS2000 Server Setup section. 4. Log Out: press this button after you complete the setup process. 5. Info – press this button to see the application version as in Figure 5-2.
--	---

Figure 5-4 Menu

5.3 Server Setup

The VMS2000 Server Setup allows the user to configure various DVS and VMS2000 Server software parameters.

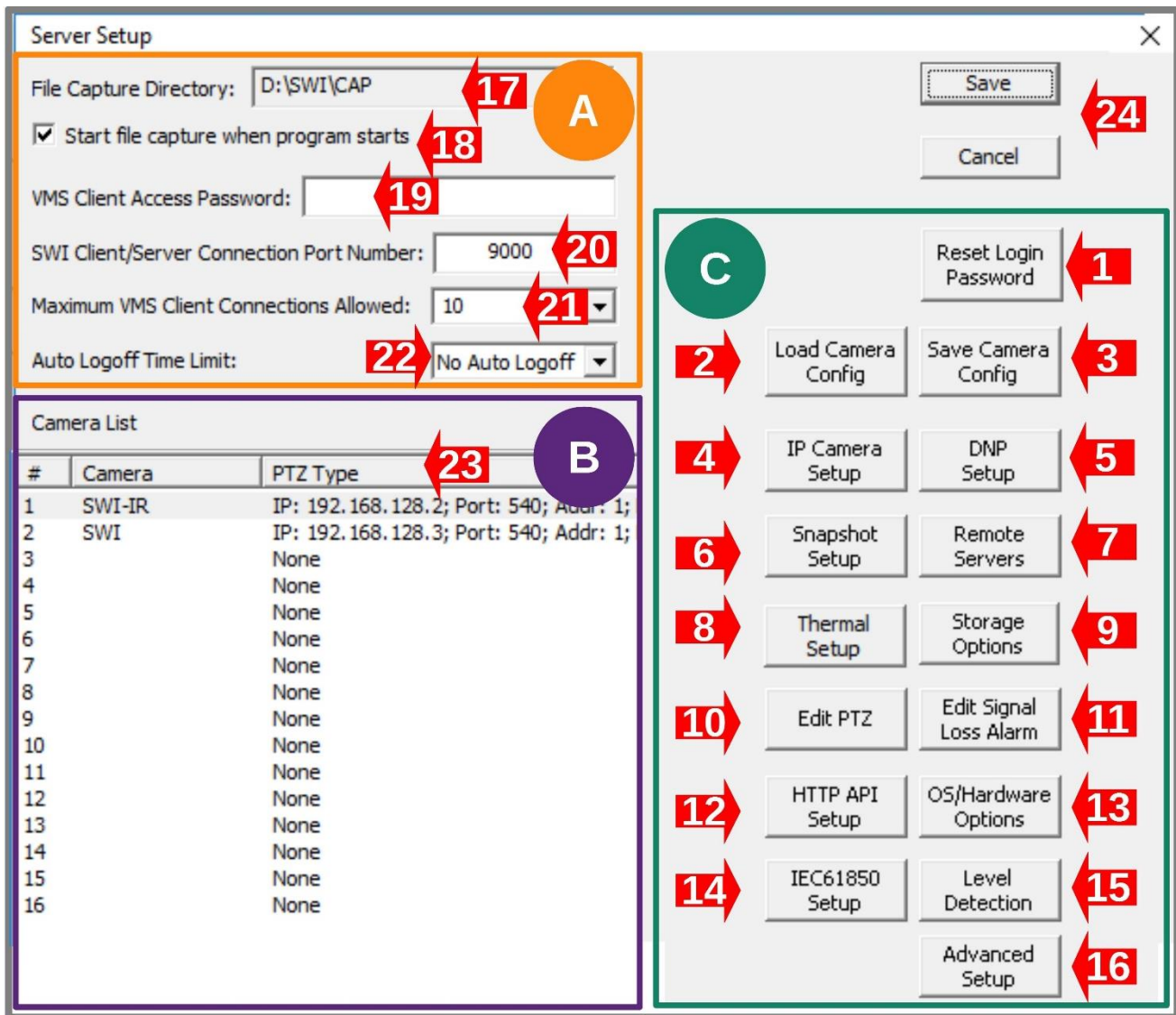


Figure 5-5 Server Setup

The VMS Server Setup dialog is shown in Figure 5-5 and three areas are marked:

- Section A: consult SWI Support Team before changing these parameters; detailed description below.
- Section B: marks the table showing the current configured cameras.
- Section C: contains the buttons that access specific configurations.

In area marked C these functions are available:

1. Reset Login Password – see section 5.3.1.
2. Load Camera Configuration – press this button to load the settings of the IP Cameras that were previously configured using the instructions in section 5.3.3 and 5.3.4.

3. Save Camera Configuration - press this button to save the settings of the IP Cameras configured using the instructions in section 5.3.2 and 5.3.4.
4. IP Camera Setup: configure the IP cameras connected to this DVS see section 5.3.4.
5. DNP Setup: This section is used to configure the DNP protocol for use in SCADA integration applications. This is for advanced users who are familiar with the DNP protocol. Information regarding setting up the DNP protocol can be found in SWI's Application Note: DVS DNP Protocol Implementation. Contact SWI support for more information on DNP setup.
6. Snapshot Setup: Allows the user to define a video snapshot schedule for specified cameras.
7. Remote Servers: define remote VMS servers to "inter-connect" alarms between different VMS servers. This is used when an action on one VMS server is to be tied to an event or alarm on another VMS sever – see section 5.3.7.
8. Thermal Data Setup: configuration of the thermal data retention - default 180 days, maximum 365 days.
9. Storage Options: specify when to start and stop deleting the oldest archived video.
10. Edit PTZ: communication and parameter settings for the selected camera – see section 5.3.10.
11. Edit Signal Loss Alarm: Selecting this button will bring up a screen allowing users to trigger alarms when video signals from selected cameras are lost - see section 5.3.11.
12. HTTP API Setup: This button will bring up a dialog box to configure the HTTP API – see section 5.3.12.
13. OS/Hardware Options: This button brings up a screen that allows the operator to disable or enable USB storage devices to be used with the DVS, restart the computer, and enable or disable options in the Windows control panel.
14. IEC61850 Setup: This button will bring up a dialog box to configure the IEC-61850 communication protocol – see section 5.3.14.
15. Reserved for future development.
16. Advance Setup: accessible by SWI Support personnel for troubleshooting purposes.
17. File Capture Directory: location of the video file capture directory on the DVS.
18. Start file capture when program starts: This parameter enables/disables video recording on start-up of the VMS2000 Server software (on boot-up of the DVS).
19. VMS Client Access Password: This adds another level of security for the connection between the VMS client and the server. The administrator of the VMS client must enter this password while configuring the connection to the corresponding server. This "Password" must match the "Password" in "d017-0001-401-00_VMS_Client_UG.pdf" – section "5.2 Client Configuration/ Connection", paragraph 5.2.1.
20. SWI Client/Server Connection Port Number: This port number is used for data communication between VMS2000 Server and VMS2000 Client – the default value is 9000. This "Port #" must match the "Port #" in "d017-0001-401-00_VMS_Client_UG.pdf" – section "5.2 Client Configuration/ Connection", paragraph 5.2.1. This port number must match between VMS2000 Server and VMS2000 Client. The
21. Maximum VMS Client Connections Allowed: This sets the maximum number of VMS2000 Clients that can connect simultaneously to the VMS2000 Server. You can reduce this number if your network bandwidth is limited.
22. Auto Logoff Time Limit: This is a security measure that automatically logs the user off the VMS2000 server after the preset limit is reached.
23. The Camera List table shows the existing configured Video and Thermal Cameras.
24. Press the "Save" button to preserve the current configuration or press the "Cancel" button to discard the changes.

5.3.1 Reset Login Password

The “Reset Login” allows you to change the existing log in credentials. This may be a requirement of your IT security policy; example - all passwords must be changed every 6 months. After you press the “Reset Login” button (arrow 1 in Figure 5-5) you are prompted to confirm the change. If you select “Yes” you must follow the steps illustrated in Figure 5-6 .

1. Press the “Yes” button and the configuration dialog box is displayed.

2. Type the new “User Name”

3. Type the new “Password”

4. Retype the new Password

5. Press “Add” to preserve the configuration. Press “Cancel” to discard the configuration.

6. Press “Yes” to confirm and return to previous dialog box.

Figure 5-6 Reset Login

Best practice: It is strongly recommended that you save the new Login information.

5.3.2 Load Camera Config

Best practice: It is strongly recommended that you save the IP Camera Configuration.

Press the “Load Profile” button, marked by arrow 2 in Figure 5-5, to load the previously saved settings – section 5.3.3. Use the standard browse dialog box shown in Figure 5-7 to select the file.

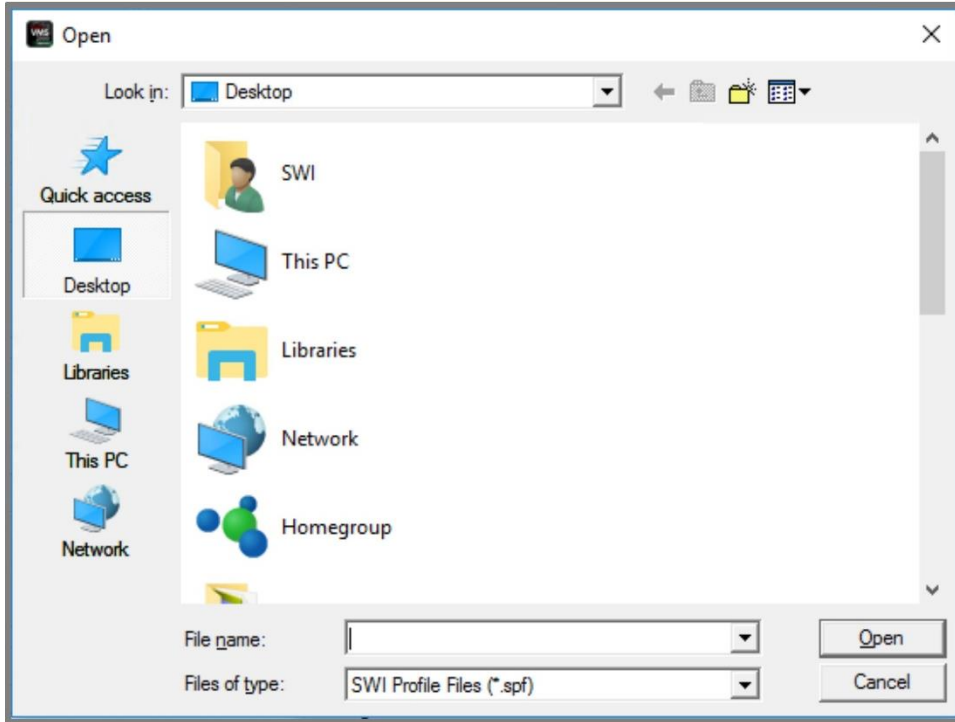


Figure 5-7 Save/Load Camera Config

5.3.3 Save Camera Config

Best practice: It is strongly recommended that you save the IP Camera Configuration.

Press the “Save Profile” button, marked by arrow 3 in Figure 5-5, to save the settings in the IP Camera Setup. Use the Windows standard browse dialog box shown in Figure 5-7 to name the file. This file is a backup of your current setup and can be used for recovery or for another VMS2000 deployment.

5.3.4 IP Camera Setup

You will use the “IP Camera Setup” to configure the parameters associated with the IP cameras connected to the DVS. For this configuration you must have access to the DVS locally or remotely (via Remote Desktop).

5.3.4.1 Access the IP Camera Setup

Shown in Figure 5-8 are the steps to reach the IP Camera Setup dialog box:

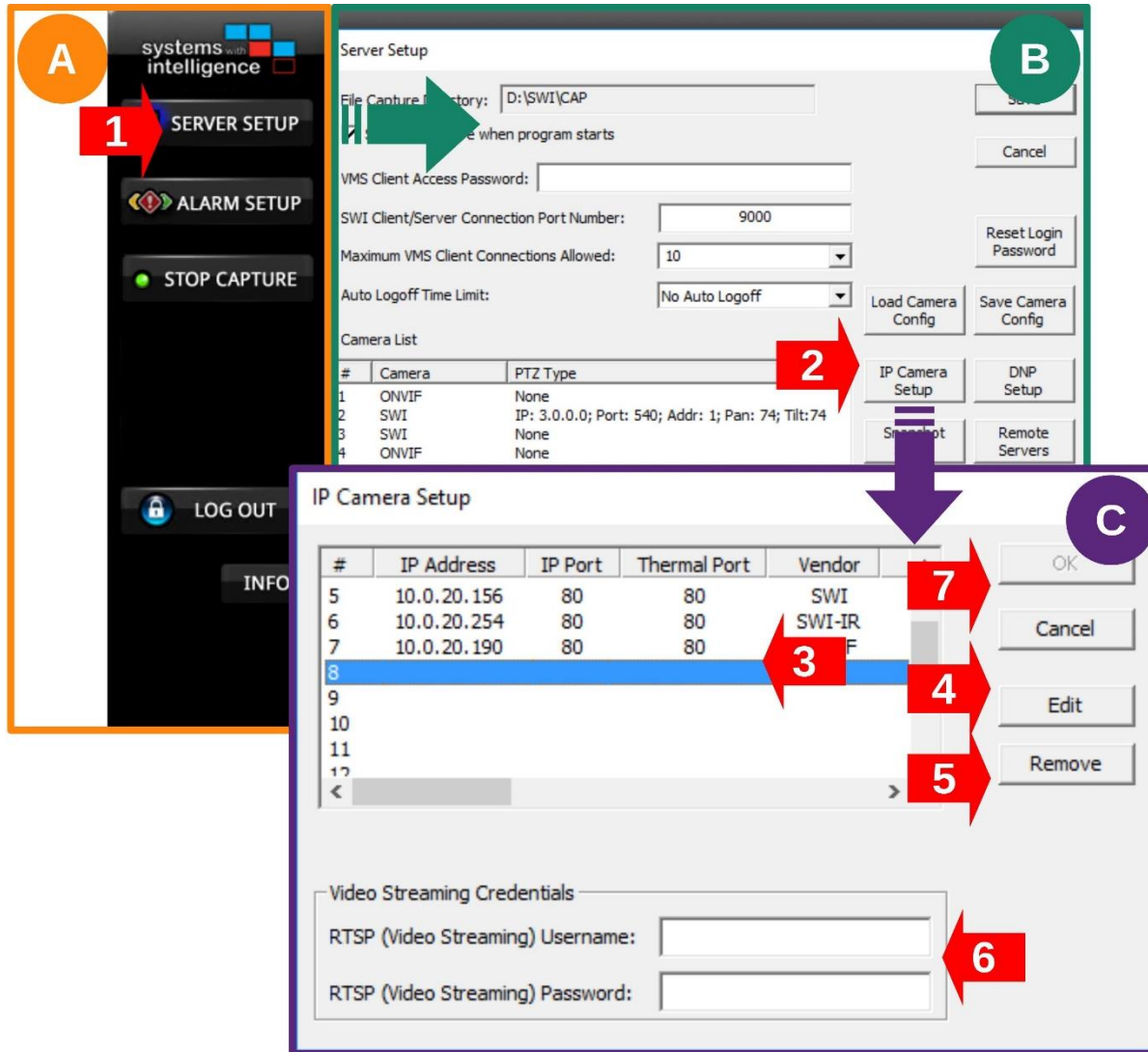


Figure 5-8 IP Camera Configuration

1. Click on the “Server Setup” button.
2. Press the “IP Camera Config” button and the “IP Camera Setup” dialog is displayed.
3. Add new camera - click on an empty slot in the list then press the “Edit” button; in this example #8 is the first empty slot. Follow the instructions in Figure 5-9.
4. Modify existing – click in the list # the camera that you want to modify then press the “Edit” button. Follow the instructions in Figure 5-9.
5. Remove existing – click camera in the list then press the “Remove” button.
6. RTSP Username/Password – enter log-in information for the stream If it is required by the camera. This is used if you share the camera feed to other VMSs through RTSP protocol and wish to set a password for that connection (that could be different from the camera's password).

7. Press the OK button to preserve the configuration or press the Cancel button to discard the changes; you will return to the previous screen.

Note: # - the index in the list represents the order of the channels displayed and it may not be identical to the order of the physical ports.

5.3.4.2 Add or Modify IP Camera

You must follow the instructions in section 5.3.4.1 to access the “IP Camera Setup” dialog box.

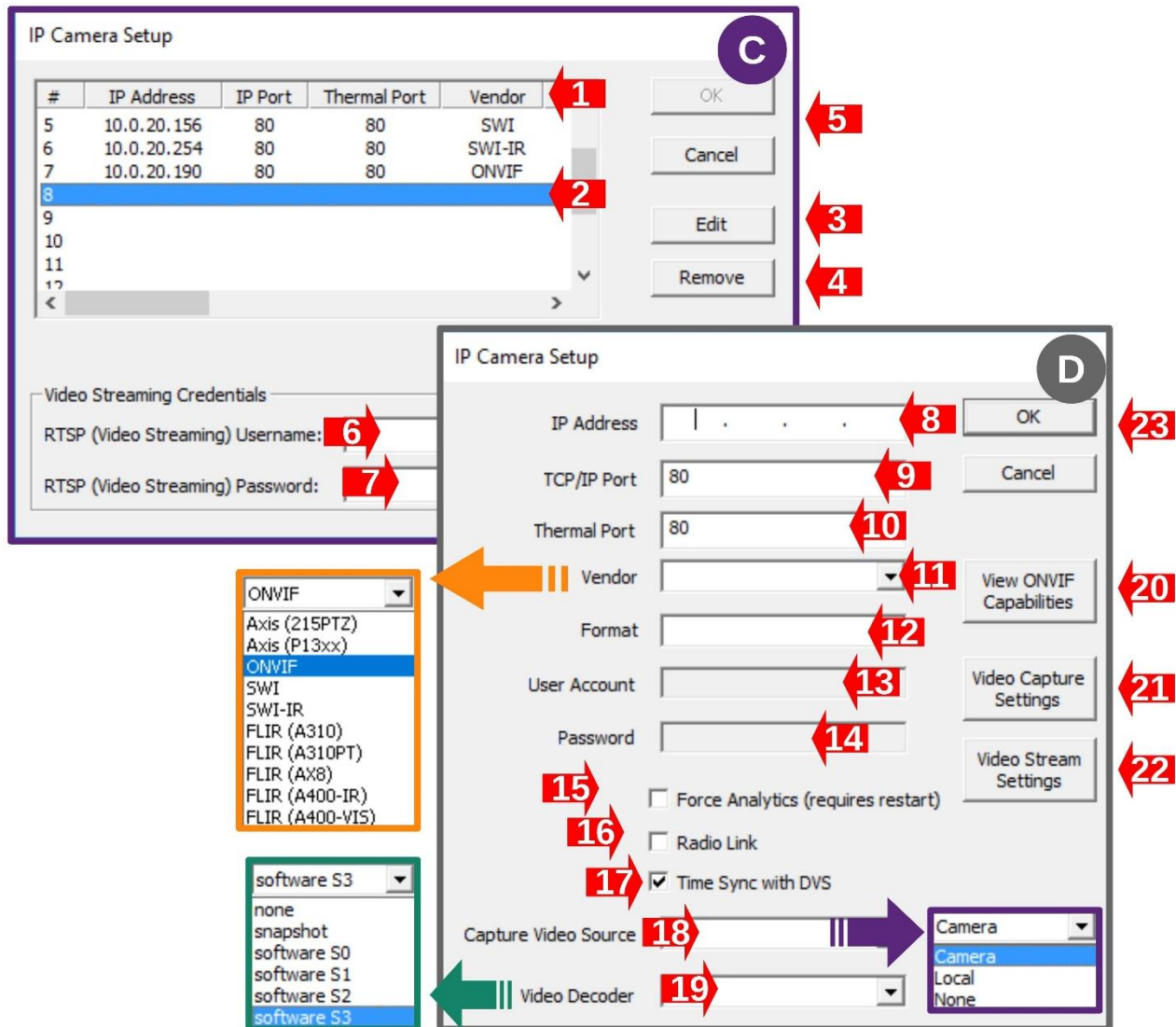


Figure 5-9 Edit IP Camera Configuration

Follow these steps to add or modify an IP camera – see Figure 5-9:

1. Information – in the header are the main parameters of the cameras in the list.
2. To add a new camera press to an empty slot in the list. To modify a camera in the list, click on the row that contains the camera of interest.
3. Add new camera: click on an empty slot in the list. To edit existing – press the # camera in the list. Click on the “Edit” button and the dialog box marked (D) is displayed, proceed to step 8.
4. Click on the “Remove” button and the selected camera (row) is deleted from the configuration.
5. After you complete the configuration press the “OK” button to preserve changes or press the “Cancel” button.

6. RTSP (Video Streaming) Username: leave this field empty unless instructed by SWI Support.
7. RTSP (Video Streaming) Password: leave this field empty unless instructed by SWI Support.
8. IP Address: The IP address of the IP camera, this is provided by SWI.
9. TCP/IP Port: The TCP/IP Port of the IP camera. Default: 80.
10. Thermal port – if this is a dual camera (visual and thermal). The TCP/IP Port number must match the configuration of the IP Camera. Default: 80.
11. Vendor: drop-box list to select the IP Camera Vendor. You must select the vendor of the connected IP Camera.
Note: Contact SWI for more information about supporting IP Cameras.
12. Format: The video stream format from the IP Camera. The video stream format is dependent on what is available from the specific IP camera manufacturer. Only the formats available from the IP camera manufacturer will be selectable.
13. Username – camera log-in. The username (account) needed to access the IP Camera streams directly.
14. Password – camera log-in. The password required to gain access to the IP Camera streams directly.
15. Force Analytics: This setting is checked in two scenarios. If the user would like to capture snapshots but has no analytic rules set for the camera or if the user wants to run analytics on a PTZ camera for only specific presets, the Force Analytics box should be checked. The server will have to be restarted in order for this change to take effect.
16. Radio Link: This setting is checked when a camera's network connection between itself and the DVS is low bandwidth. The setting changes the IP protocol from UDP to TCP.
17. Time Sync with DVS
18. Capture Video Source: There are three options for this setting. When "Camera" is selected, the capture stream from the camera is used to save video. When "Local" is selected the video being displayed on the VMS Client is also being used to record video. When "None" is selected then no video is captured.
19. Video Decoder: On the DVS where the camera is connected to a hardware encoder card the "Hardware" option should be selected. On the DVS the "Software S3" option should be selected where the analytics stream of the camera is providing a 5Hz MJPEG signal in CIF format. Other Software options are S1 which is the display stream directly from the camera, and S2 which is the capture stream of the camera. S0 is the restreamed display stream from the VMS software. The Snapshot option allows an alarm snapshot to be created but no analytics will be available. "None" is used when no analytics are desired.
20. View ONVIF settings – these are specific to ONVF camera.
21. Video Capture Settings: This button makes another window appear. "Capture Continuously" is the default option and it means video is continuously recorded from the camera. "Capture on Alarm/Event" has the VMS2000 software only saving video for 6 minutes before and 6 minutes after an event occurs.
22. Video Stream settings – these are specific to the camera model selected in the vendor list.
23. You must press the "OK" button in the dialog box marked (D) to preserve the settings. Press the Cancel button to discard the changes; you will return to the previous screen.

5.3.4.3 Add TS3700 Camera

This section will guide you to configure the VMS Server with the TS3700. This model is a dual stream camera, it supplies one video stream and one thermal stream. You must configure each stream and for model TS3700-PT you must configure the Pan-Tilt (PT) Module. Below are listed these steps:

- I. Add the TS3700 Visual Stream.
- II. Add the TS3700 IR Stream
- III. Optional - configure the PT Module for Visual Camera and IR Camera.
- IV. Reboot the DVS.
- V. Retrieve token for the API Key

I. Add the TS3700 Visual stream

To configure the TS3700 Visual stream follow the instructions in Figure 5-10:

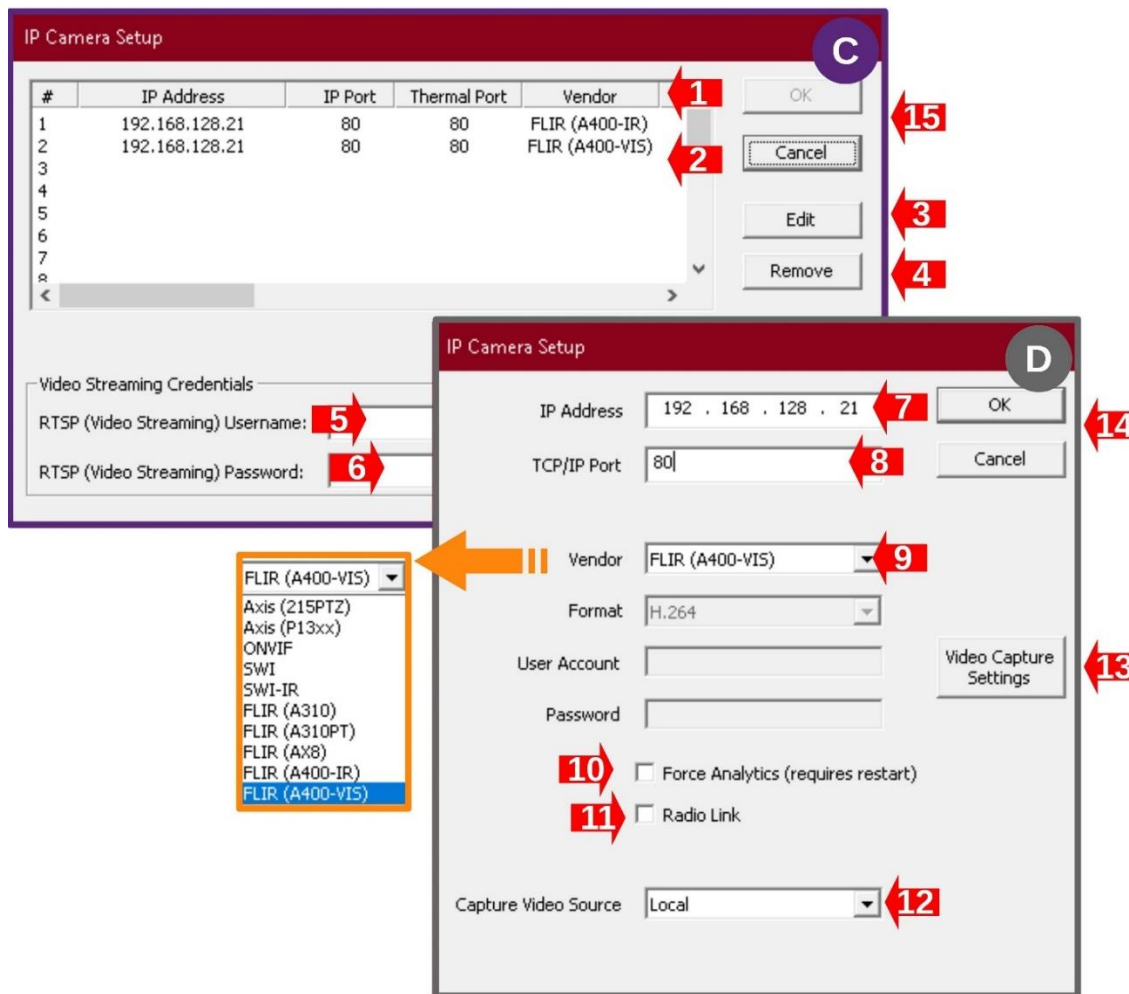


Figure 5-10 Setup the TS3700 Visual Stream

1. Information: this is the header of the list that shows the cameras configured.
2. To add a new camera press to an empty slot in the list. To modify a camera in the list click on the row that contains the camera of interest.
3. Click on the “Edit” button and the dialog box marked (D) is displayed, proceed to step 7.
4. Click on the “Remove” button and the selected camera (row) is deleted from the configuration.
5. RTSP (Video Streaming) Username: leave this field empty unless instructed by SWI Support.

6. RTSP (Video Streaming) Password: leave this field empty unless instructed by SWI Support.
7. Type the IP address of the camera; this information is provided by SWI.
8. The TCP/IP Port is set to 80 by default. Don't change this value unless directed by SWI Support.
9. Select "FLIR (A400-IR)" in the "Vendor" drop-down list.
10. Leave unchecked the "Force Analytics" box.
11. Leave unchecked the "Radio Link" box.
12. Select "Local" in the "Capture Video Source" drop-down list.
13. Don't change the default settings in the "Video Capture Settings".
14. Press the "OK" button to save the configuration. Press the "Cancel" button to discard the configuration and return to the previous dialog box.
15. Press the "Save" button to save the configuration. Press the "Cancel" button to discard the configuration and return to the previous dialog box. At this point the Visual stream is configured, proceed to step II.

II. Add the TS3700 IR stream

To configure the TS3700 IR stream follow the instructions in Figure 5-11.

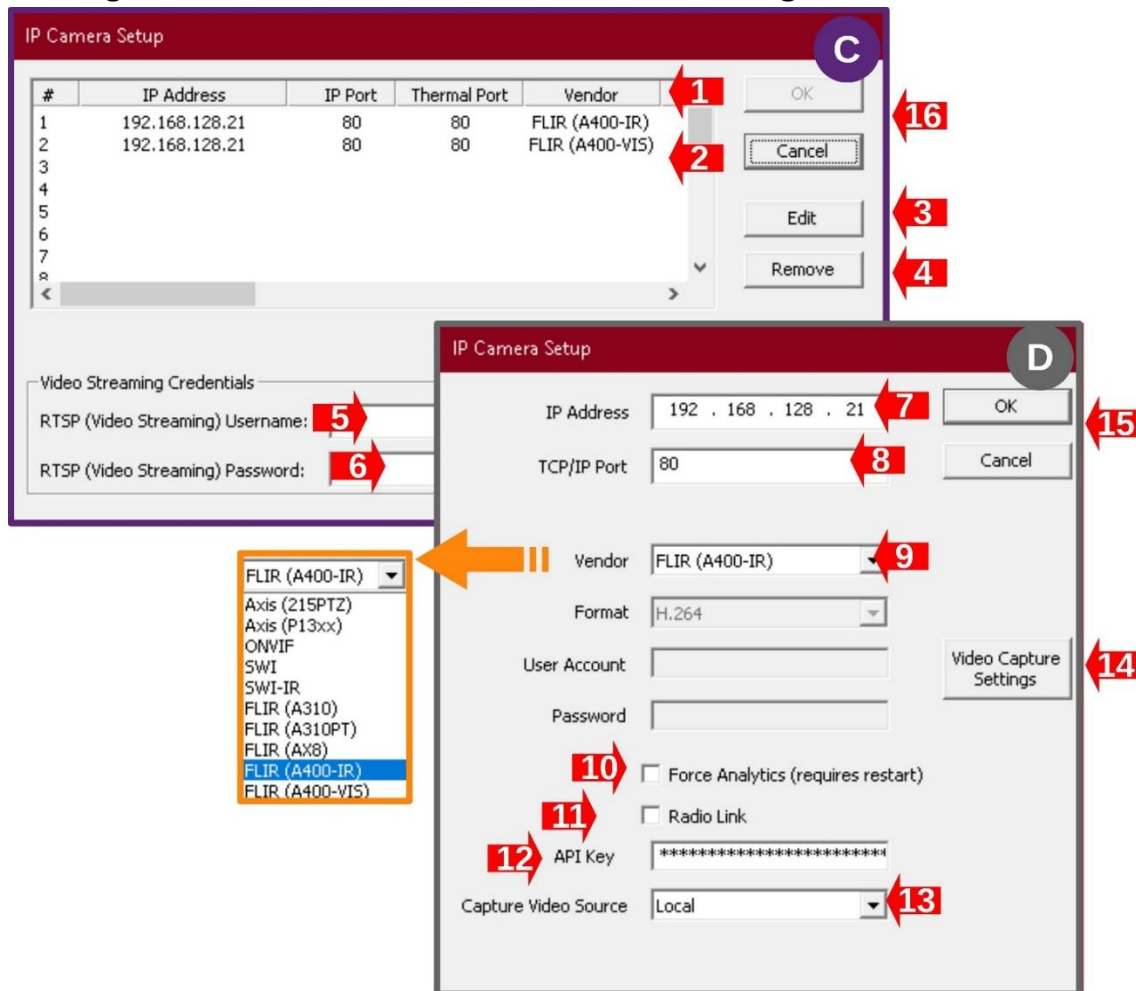


Figure 5-11 Setup the TS3700 IR Stream

1. Information: this is the header of the list that shows the configured cameras.
2. To add a new camera, press an empty slot in the list. To modify a camera in the list, click on the row that contains the camera of interest.
3. Click on the "Edit" button and the dialog box marked (D) is displayed, proceed to step 7.

4. Click on the “Remove” button and the selected camera (row) is deleted from the configuration.
5. RTSP (Video Streaming) Username: leave this field empty unless instructed by SWI Support.
6. RTSP (Video Streaming) Password: leave this field empty unless instructed by SWI Support.
7. Type the IP address of the camera; this information is provided by SWI.
8. The TCP/IP Port is set to 80 by default. Don't change this value unless directed by SWI Support.
9. Select “FLIR (A400-IR)” in the “Vendor” drop-down list.
10. Leave unchecked the “Force Analytics” box.
11. Leave unchecked the “Radio Link” box.
12. SWI will supply a 48-characters token, copy this information and paste it in the “API Key” field. Also, you can retrieve the token using the instructions in step V.
13. Select “Local” in the “Capture Video Source” drop-down list.
14. Don't change the default settings in the “Video Capture Settings”.
15. Press the “OK” button to save the configuration. Press the “Cancel” button to discard the configuration and return to the previous dialog box.
16. Press the “Save” button to save the configuration. Press the “Cancel” button to discard the configuration and return to the previous dialog box. At this point the IR stream is configured, proceed to the next step.

III. Optional: configure the PT Module

If you order the TS3700-PT model you must follow the instructions in this step to configure the PT Module.

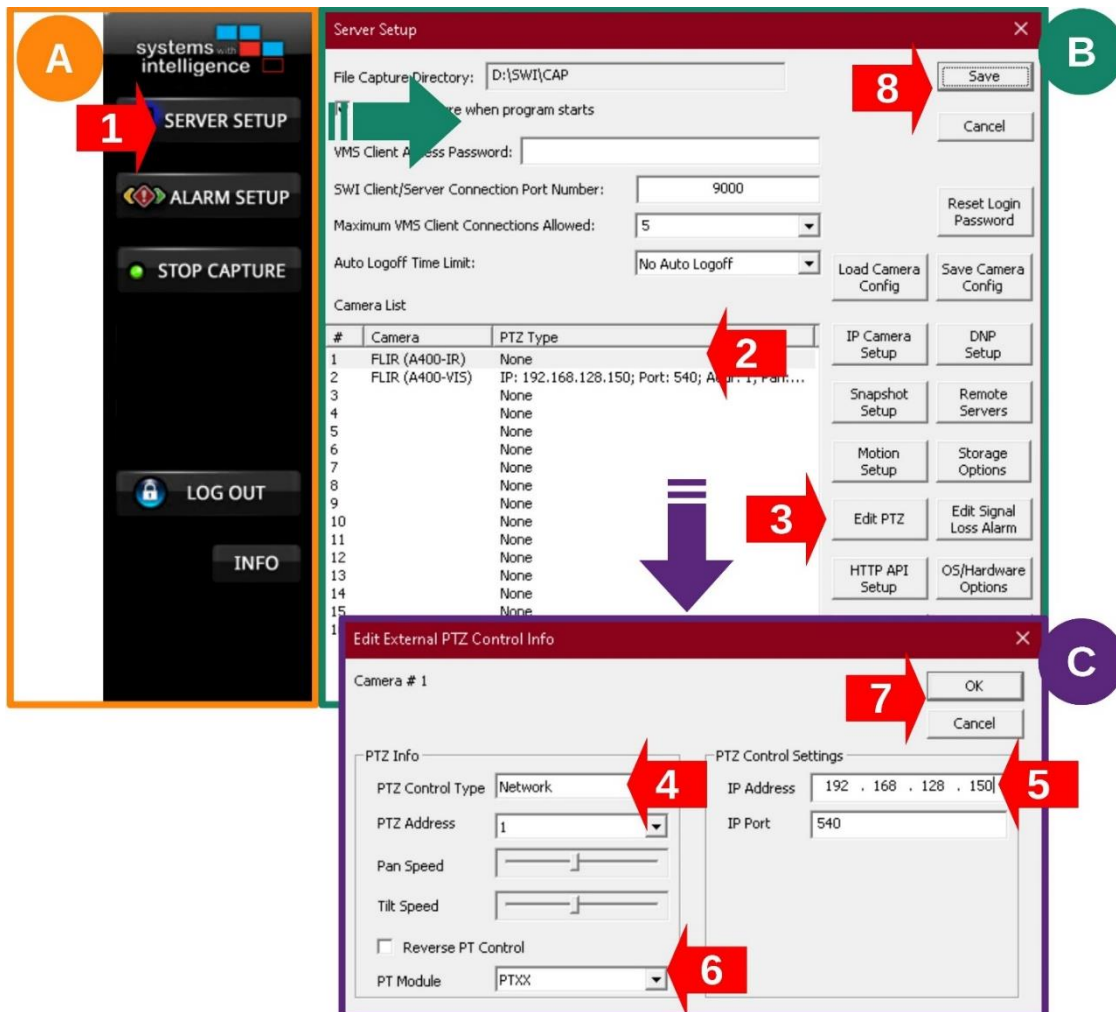


Figure 5-12 Setup the TS3700 PTZ Module

To configure the PT Module, follow the instructions in Figure 5-12:

1. Click the “Server Setup” button in the right menu, this will open the dialog box marked (B).
 2. Click on the camera you want to configure. Example: Camera #1, FLIR (A400-IR).
 3. Press the “Edit PTZ” button and the dialog box marked (C) will open.
 4. Select “Network” in the “PTZ Control Type” drop-down list.
 5. Type the “IP Address”, this information is provided by SWI. The “IP Port” is: 540, don't change.
 6. Select “PTXX” in the “PT Module” drop-down list.
 7. Press the “OK” button to save the configuration. Press the “Save” button to discard the configuration and return to previous dialog-box. Repeat the steps 2 to 7 for Camera #2, FLIR (A400-VIS).
 8. Press the “Save” button to preserve the configuration. Press the “Cancel” button to discard the changes.
- IV. You must reboot the DVS.**

At this moment the configuration is complete, and you must restart the DVS.

V. Retrieve the token for the API Key

This section contains instructions to retrieve the token for the API KEY.

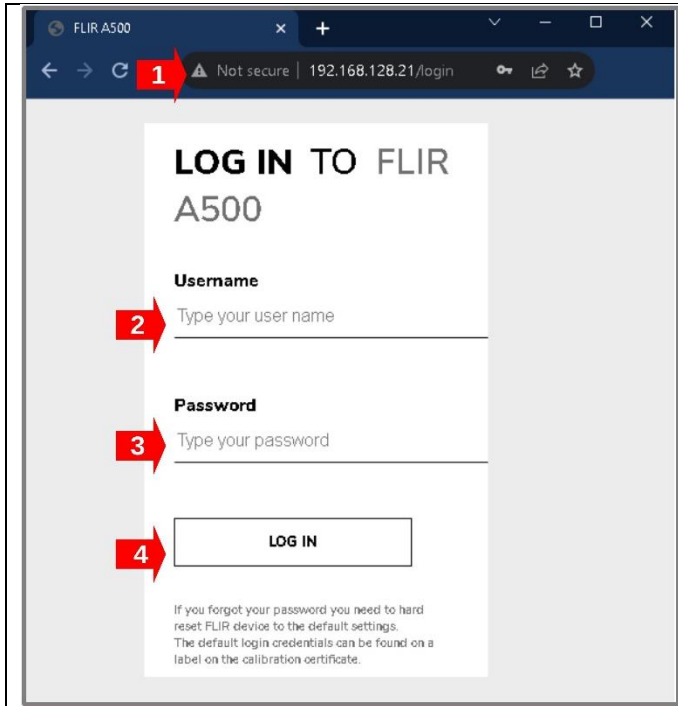


Figure 5-13 FLIR Log-in

Start the Web Browsers – Internet Explorer is provided.

1. In the address bar type the IP address of the camera.
2. Type the log-in name provided by SWI.
3. Type the password provided by SWI.
4. Press the “LOG IN” button.

Proceed to the next set of instructions.

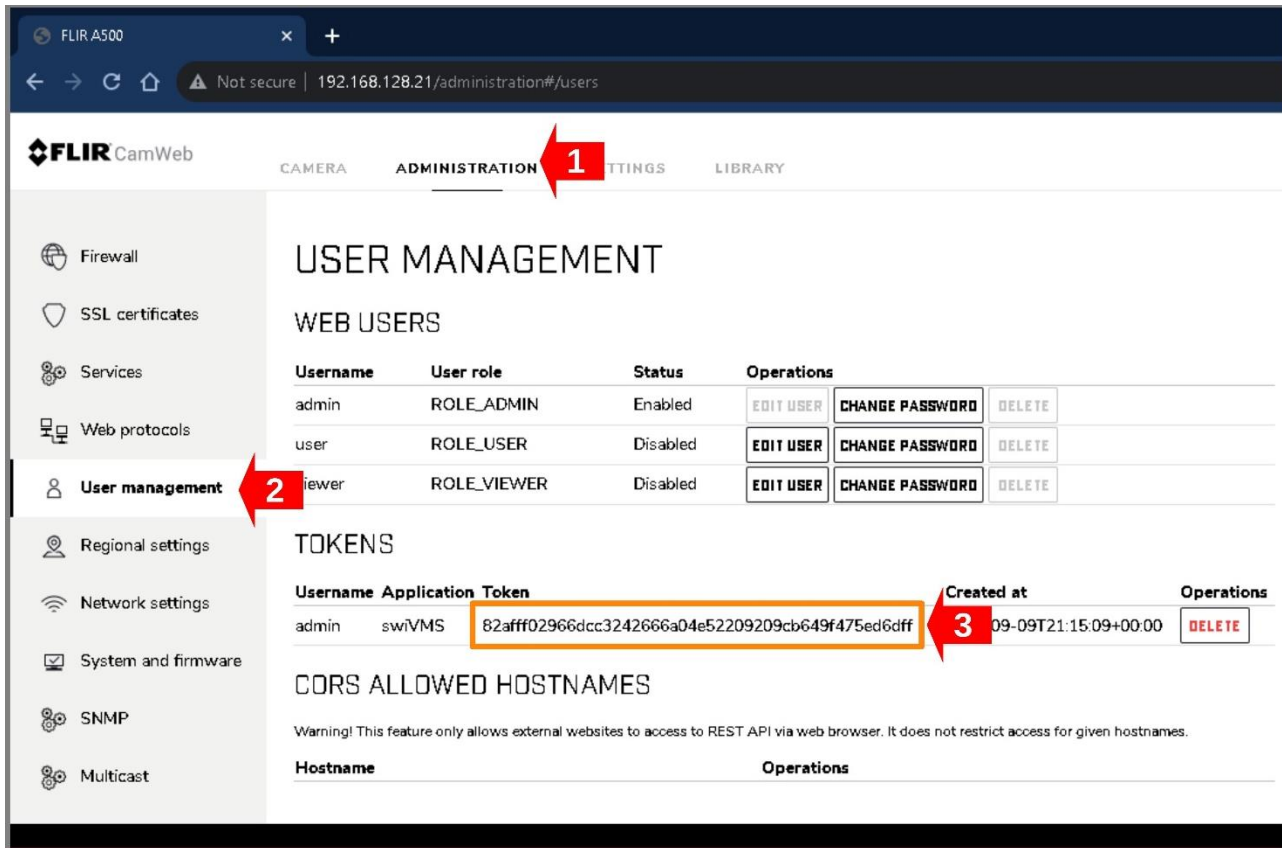


Figure 5-14 FLIR Retrieve Token

To retrieve the Token, follow the instructions in Figure 5-14:

1. Press the “ADMINISTRATION” tab located in the top menu.
2. Press the “User management” button located in the left-menu.
3. In the “TOKENS” section copy the token allocated to the “admin”.

Use this token to populate the field “API Key” of the IR Stream configuration required in Step II.

5.3.5 DNP Setup

The document: “D017-0028-201-01 DVS-DNP3_Comm_Manual_Print.pdf” has detailed instructions. Please contact SWI support team to obtain the manual or additional information.

5.3.6 Snapshot Setup

Best practice: It is strongly recommended that you use the VMS Client application to do this configuration – as per “d017-0001-401-00_VMS_Client_UG.pdf”.

Snapshots are easy to set and they establish a continuous timeline of the image. You use the “Snapshot Setup” feature to configure a camera to take a snapshot based on a predefined schedule. Each configured snapshot becomes a defined alarm and as such is saved in the Alarm and Event database for future retrieval. Also, it can be linked to an automated e-mail notification allowing you to receive the scheduled snapshot in their mailbox at the specific time interval.

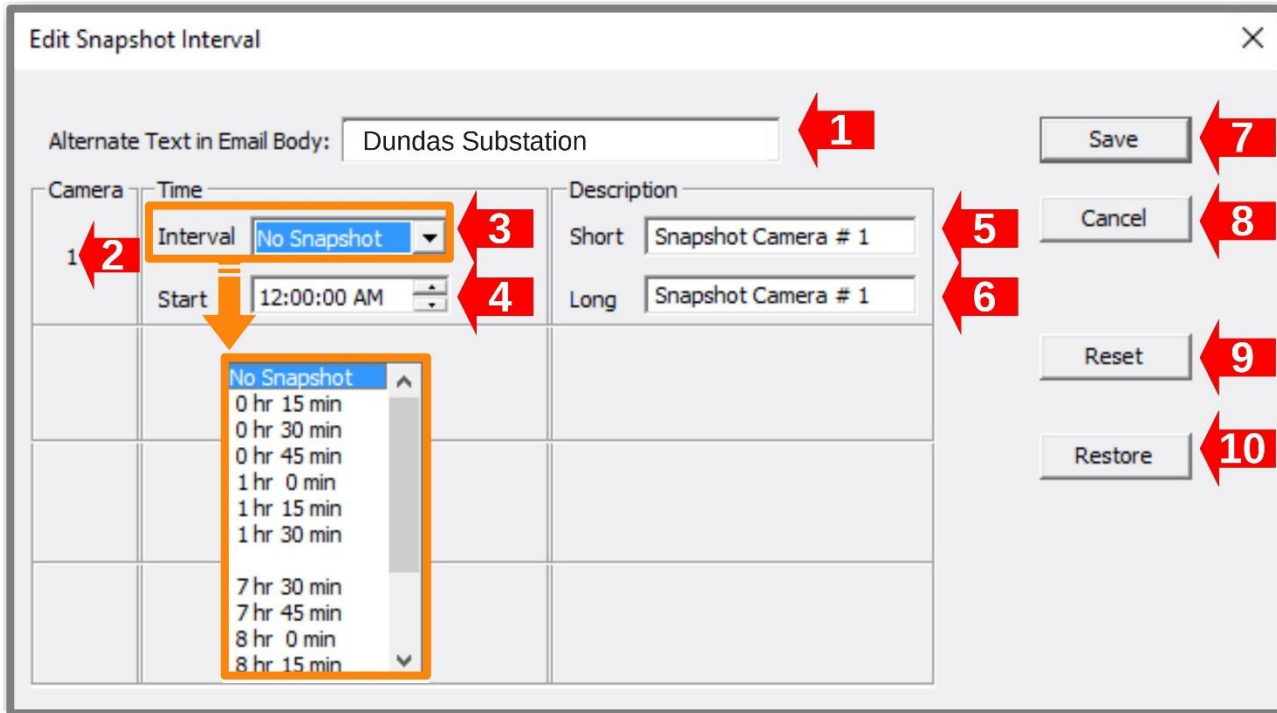


Figure 5-15 Snapshot Setup

You reach the “Snapshot Setup” widow by pressing the “Server Setup” button (top-left in the main window) and then press the “Snapshot Setup” button – marked 13 in Figure 5-5. Follow Figure 5-15.

1. Alternate Text in Email Body: If the snapshot is tied to an email notification, this field provides additional information.
2. Camera: The index of the camera connected to the DVS that the VMS2000 Server is running on.
3. Time – Interval: you select the interval between snapshots. Selections: every 15min.; starting at 15min. and 24 hours.
4. Time – Start: The time at which the camera snapshots will start.
5. Description – Short: Type a short description that helps you to identify the camera and the event.
6. Description – Long: Type a detailed description that helps you to identify the camera and the event.
7. Save: press the “Save” button to preserve the configuration and return to the previous dialog.
8. Cancel: press the “Cancel” button to discard the last configuration
9. Reset: press the “Reset” button to set all values to the system default.
10. Restore: press the “Restore” button to return to the last saved configuration.

Note: All configured snapshots become defined alarms. As such, each snapshot is saved in the Alarm and Event database for future retrieval, and it can be linked to an automated email notification allowing the user to receive the scheduled snapshot in their mailbox at the specific time interval. See section 5.4 for details on configuring email notifications.

5.3.7 Edit Remote Servers

Note: This configuration is available only on VMS Server.

This section defines the remote VMS servers that are needed in order to “inter-connect” alarms between different VMS servers. This is used when an action on one VMS server is to be tied to an event or alarm on another VMS sever.

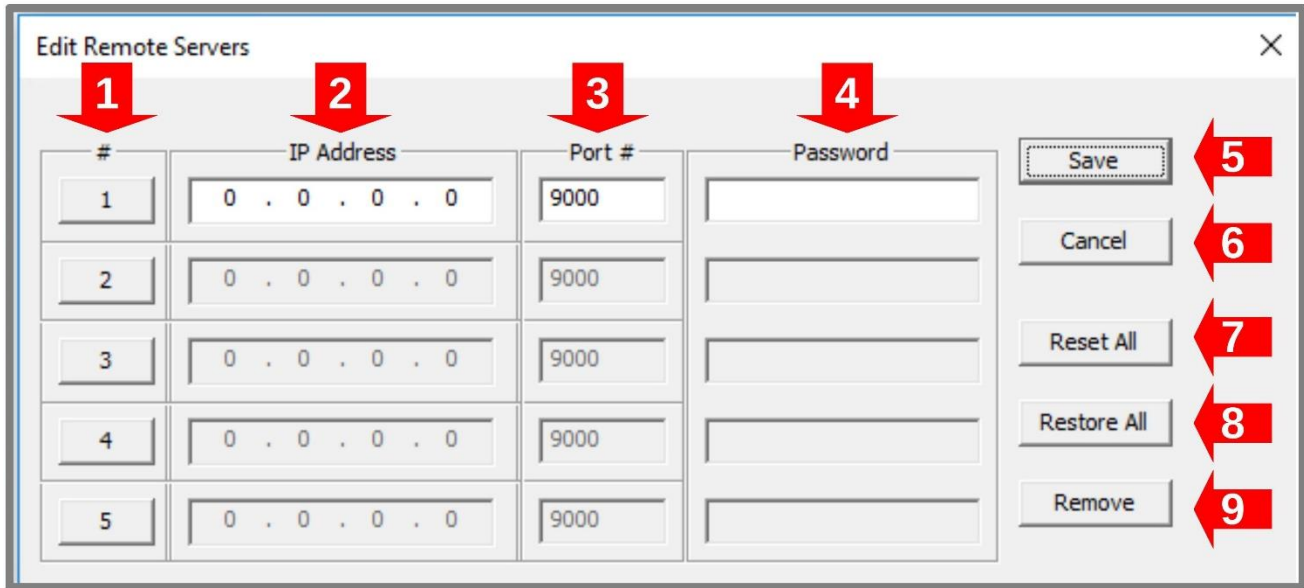


Figure 5-16 Edit Remote Servers

This are the elements:

1. # - index button: press this button to edit this entry in the table.
2. IP Address: enter in this field the IP Address of the DVS to interconnect.
3. Port #: The communication port number used by the DVS. Do not change – typical 9000.
4. Password – enter in this field the password for the DVS you want to connect to.
5. Save – press this button to save this configuration.
6. Cancel – press this button to discard the changes and return to previous dialog box.
7. Reset All – press this button to clear all entries.
8. Restore All – press this button to return to the last saved configuration.
9. Remove – press this button to delete this entry from the table.

5.3.8 Thermal Data Setup

The Thermal Data Retention period can be configured to a maximum of 365 days, with the default setting being 180 days. Press the “Thermal Setup” button, marked as 8 in Figure 5-5. The dialog shown in Figure 5-17 allows you to change this parameter – this is the period during which thermal measurements are stored.

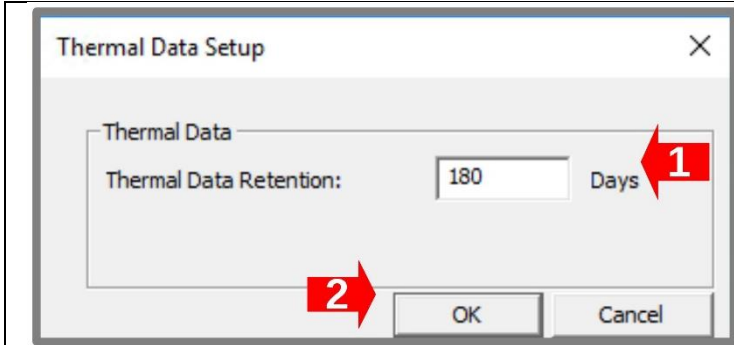


Figure 5-17 Thermal Data Setup

1. Thermal Data Retention – default is 180 days, maximum is 365 days.
2. Press “OK” to preserve the configuration or press “Cancel” to discard the changes and return to the main dialog.

5.3.9 Storage Options

The DVS has a dedicated storage drive (typical “D:”) and the “Storage Options” dialog box displays the thresholds that trigger delete of old data.

Best practice: It is strongly recommended that you use the default values as this configuration was thoroughly tested.

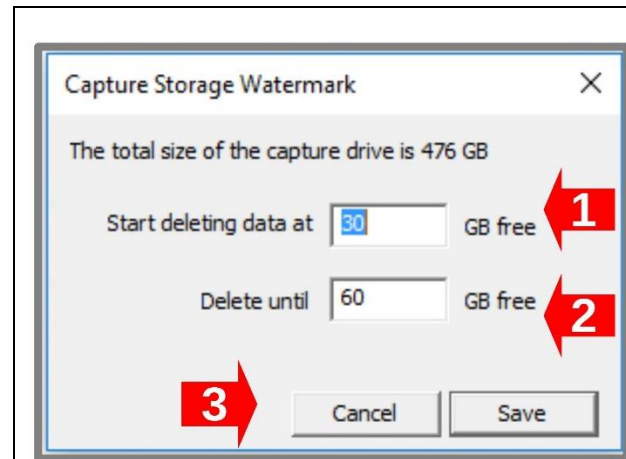


Figure 5-18 Storage Options

The “Storage Options” dialog is shown in Figure 5-18:

1. The value in “Start deleting data at” field sets the threshold that triggers automatic deletion of the oldest data.
2. The value in the “Delete until” field set the threshold of free storage that must be reached before the deletion process stops.
3. Press the “Save” button to preserve the configuration. Press the “Cancel” button to discard the changes and return to previous screen.

5.3.10 PTZ Camera Setup

This section describes how to configure network PTZ cameras, typical SWI models TCAM2000 and TCAM2500. The ONVIF and AXIS PTZ cameras do not need to be configured for PTZ controls. The VMS2000 Server is also compatible with any analog camera and positioning system that supports the industry standard PELCO-D protocol; these cameras must be configured manually. Specific instructions for configuring the TS3700-PT are listed in section 5.3.4.3.

The parameters required for this configuration are supplied by the camera manufacturer or SWI Support.

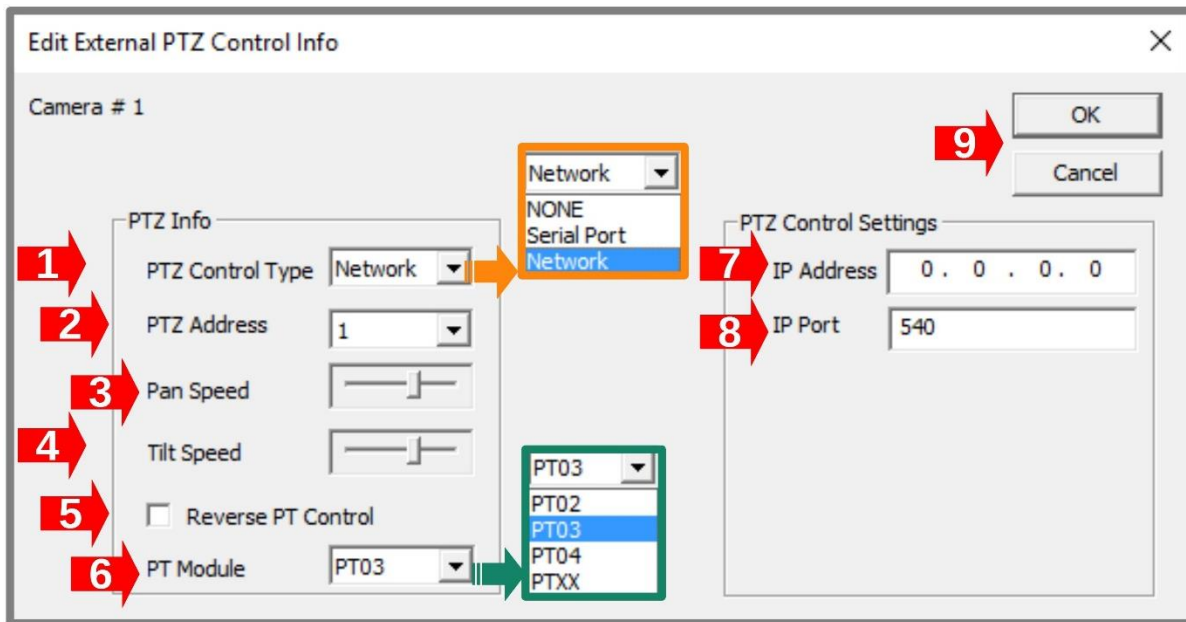


Figure 5-19 Edit PTZ

By selecting a channel in the box Camera List and pressing the Edit PTZ button on the Server Setup screen allows the user to select the type of PTZ control for that specific channel and edit the communication and parameter settings through the following dialog box:

1. PTZ Control Type: Select serial or network control based on camera specifications.
2. PTZ Address: Serial communication address for the analog camera or positioning system.
3. Pan Speed: Slider bar to configure the pan motion speed of the PTZ camera (refer to the PTZ camera manufacturer user guide for more information on this parameter). Thomas: There are no values on the actual screen so we should specify that moving the slider to the left it will result in slower moves and tot the right is faster for both pan and tilt.
4. Tilt Speed: Slider bar to configure the tilt motion speed of the PTZ camera (refer to the PTZ camera manufacturer user guide for more information on this parameter).
5. Save: Save all entered configuration and return to the previous dialog.
6. PT Module
7. IP Address
8. IP Port
9. OK press this button. Cancel: Return to previous Dialog box without changing any entered information.

Edit Serial Port: is available for backwards compatibility and old analog cameras. Here you configure specific communication serial parameters after the port is selected. You must have these serial communication parameters from the camera manufacturer: Baud Rate, Parity, Data Bits and Stop Bits.

5.3.11 Edit Signal Loss Alarm

The “Video Signal Alarm Setup” setting allows you to select which Video Channel will trigger an alarm that you can then configure to send you an e-mail notification.

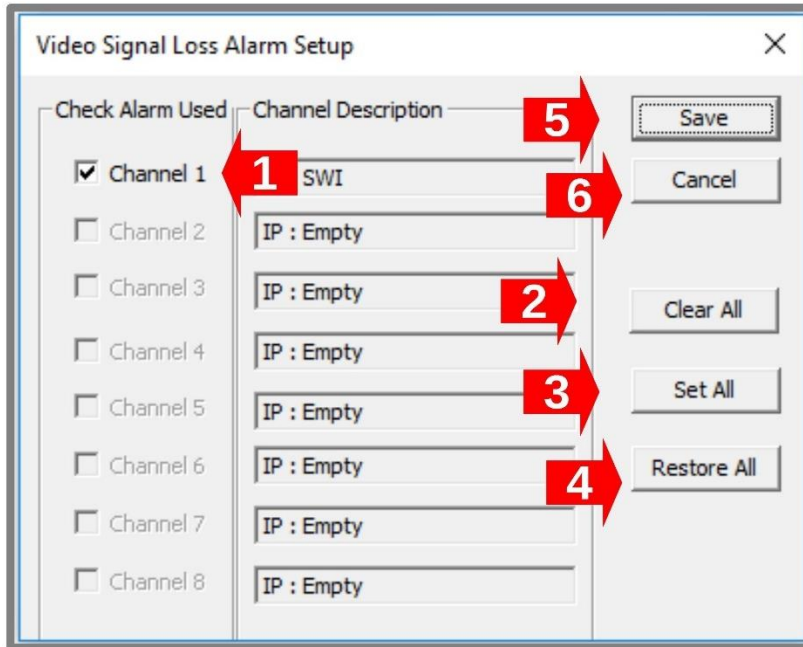


Figure 5-20 Video Signal Loss Alarm Setup

Follow Figure 5-20 to setup the alarms:

1. Click the checkbox to enable or disable the alarm for each channel.
2. Press the “Clear All” button to disable the alarms on all channels.
3. Press the “Set All” button to enable the alarms on all channels.
4. Press the “Restore All” button to return to the last saved state.
5. Press the “Save” button to store current selections.
6. Press the “Cancel” button to discard the changes and return to previous dialog.

5.3.12 HTTP API Settings

Note: This is an advance feature - please contact SWI Support Team and obtain the “D033-0054-000 VMS HTTP API” document for specific details. The paragraph below is just a brief description.

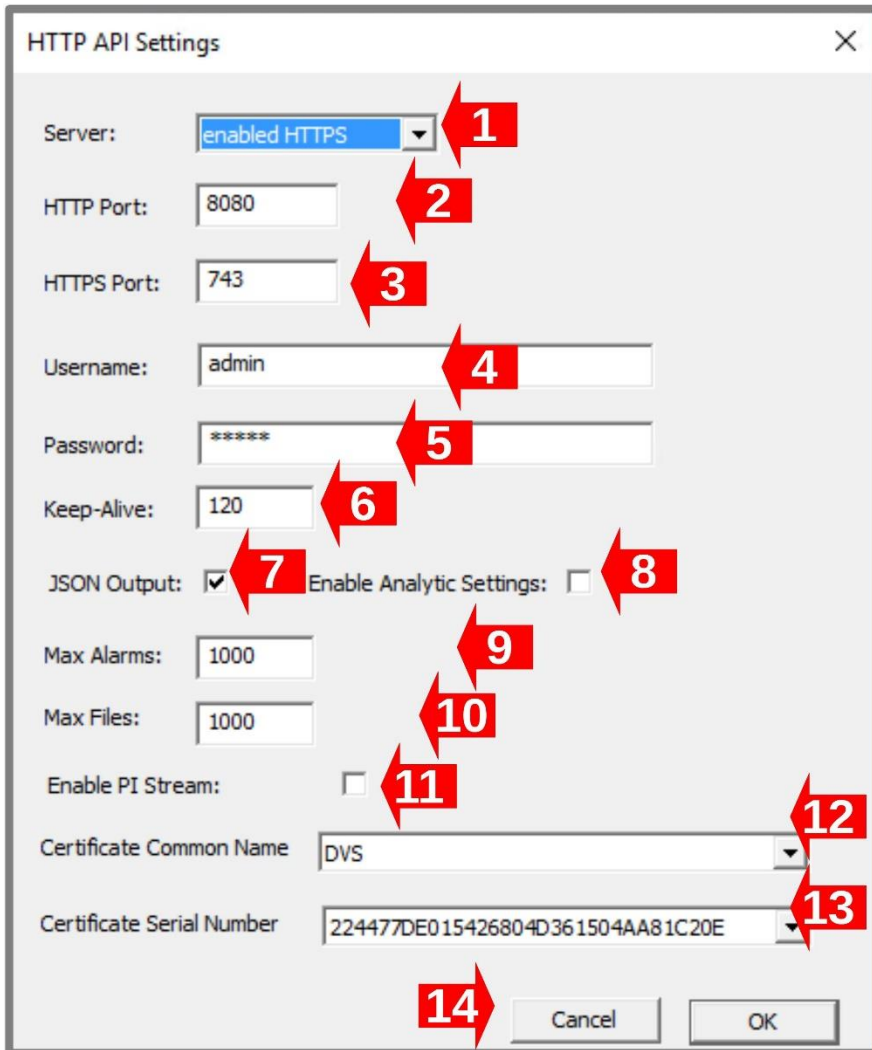


Figure 5-21 HTTPS API Settings

The dialog shown in Figure 5-21 is used to configure and enable the HTTP API settings on the DVS.

1. Server: Disabled, Enabled or Enabled HTTPS (shown in Figure 5-21)
2. The HTTP Port is configured through the TCP Port setting.
3. HTTPS Port.
4. Username and
5. Password fields may be configured by populating their respective fields. These optional fields enable Digest Access Authentication
6. Keep- Alive: Period of inactivity after which a keep-alive connection is closed – in seconds.
7. JSON (JavaScript Object Notation) Format is enabled by checking the box.
8. Enable Analytic Settings setting allows you to enable/disable analytics via HTTP API.
9. Max Alarms and
10. Max Files sets an upper limit on the number of alarms or files to be returned by the server.

11. Enable PI Stream: check this box only if you have PI video streaming integration (external platform) otherwise leave it unchecked (disabled).
12. Certificate Common Name, active selection only for the Enabled HTTPS.
13. Certificate Serial Number, active selection only for the Enabled HTTPS.
14. Press the “OK” button to store this configuration. Press the “Cancel” to discard changes.

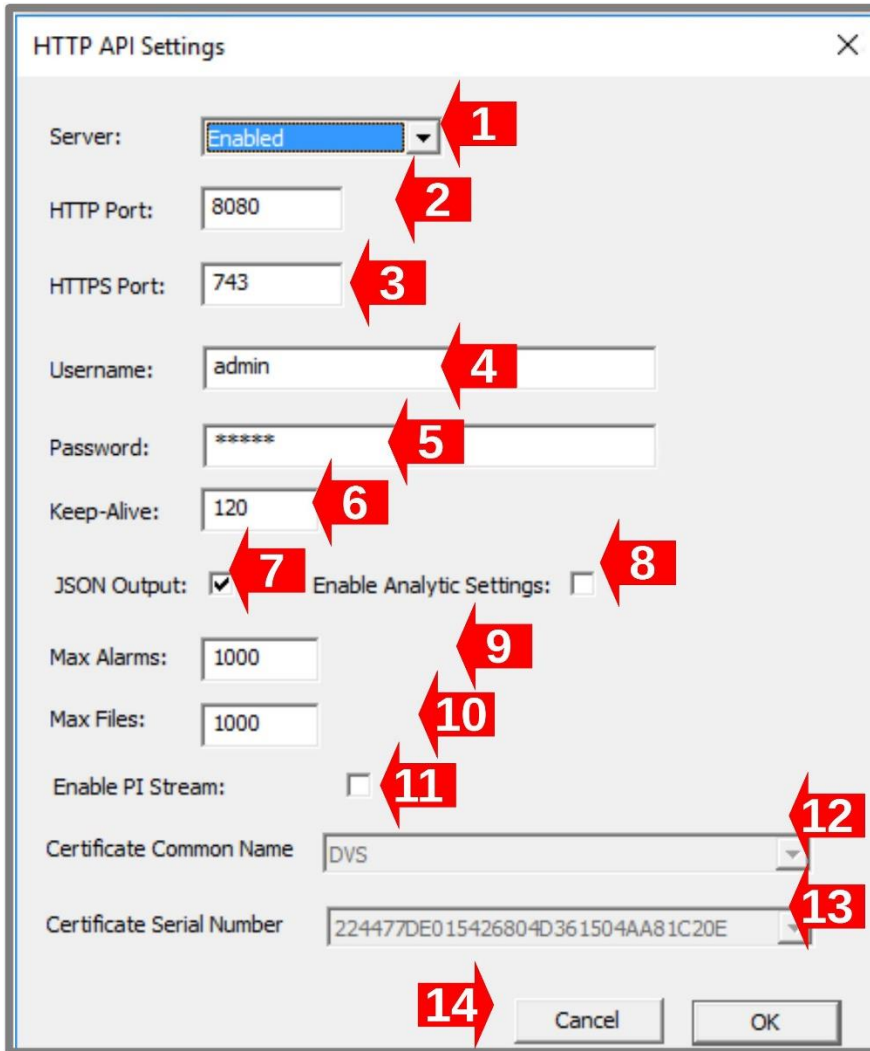


Figure 5-22 HTTP API Settings

5.3.13 OS / Hardware Options

Note: This is an advance feature - please contact SWI Support team for specific details. The paragraph below is just a brief description. The OS/Hardware dialog is shown in Figure 5-23.

	<p>These parameters can be setup here:</p> <ol style="list-style-type: none"> 1. Enable - USB ports access storage devices. 2. Enable - access to the Windows Control panel on the DVS. 3. Disable - USB ports access storage devices. 4. Disable - access to the Windows Control panel on the DVS. 5. Current Windows Password 6. New Password 7. Re-enter New Password 8. Exit 9. Restart 10. Change Logon
--	--

Figure 5-23 OS/Hardware Options

5.3.14 IEC61850 Setup

The document: “D017-0001-502-01 DVS-DNP3_VMS61850 Communication Manual.pdf” has detailed instructions. Please contact SWI support team to obtain the manual or additional information. The VMS61850 Server is installed and configured at the factory. The VMS61850 Server is launched automatically at start up using the “DVS2500A.cid” file. This is the default file place in “C:\SWI\VMS61850Server\Configuration”. It is recommended that you do not overwriting the existing file. Optionally you could rename the existing file.

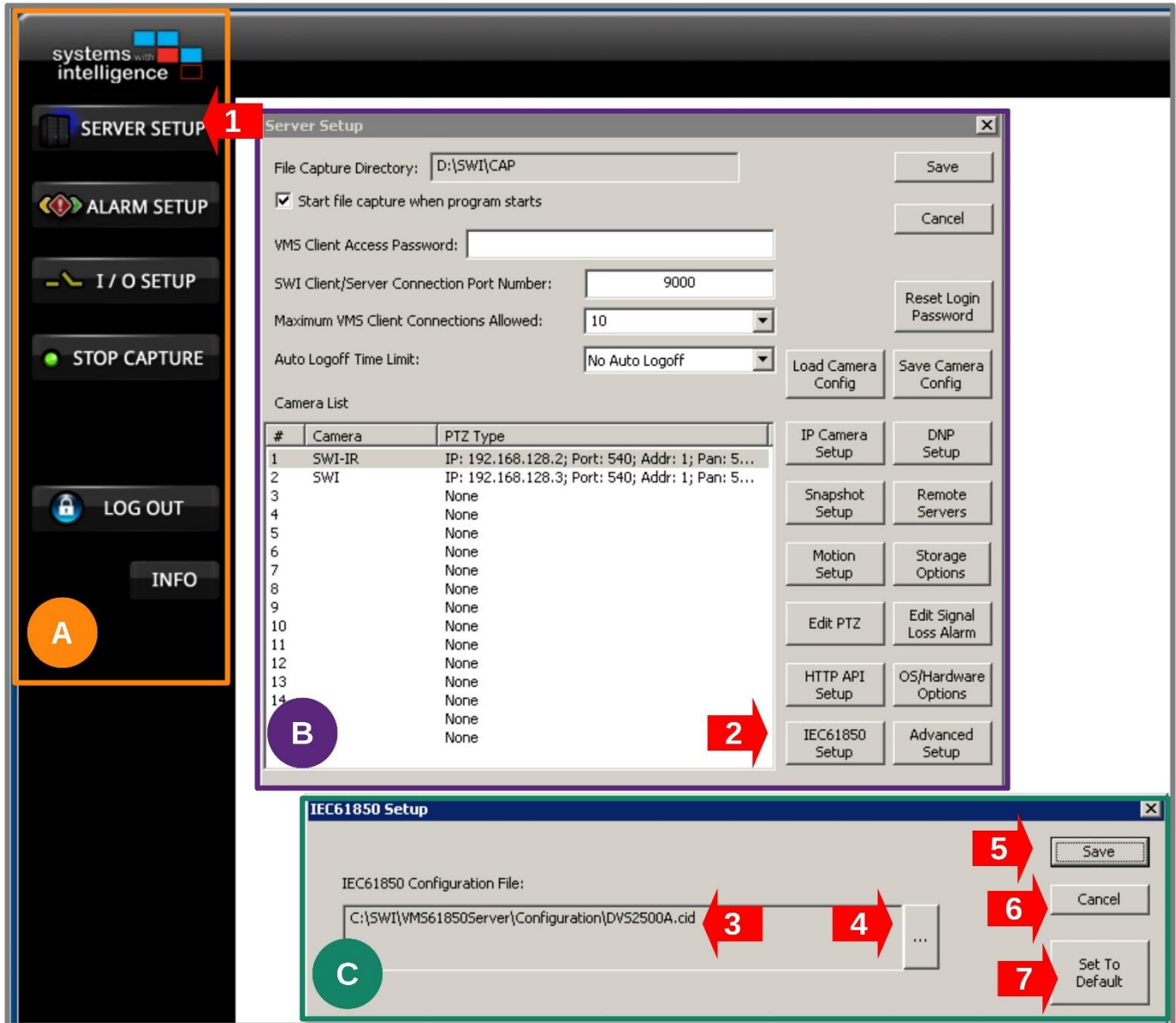


Figure 5-24 IEC61850 Setup

If you have your CID file, place it in the DVS and then follow the instruction in Figure 5-24.

1. Click the “Server Setup” button.
2. Press the “IEC61850 Setup” button.
3. The dialog “IEC61850 Setup” dialog box is displayed, and the current file used is listed.
4. Click the “...” button to browse for your file.
5. Press the “Save” button, the VMS61850 Server will restart.
6. Press the “Cancel” button to discard the changes.
7. Press the “Set To Default” to return to factory settings

5.3.15 Reserved

Reserved for future development.

5.3.16 Advanced setup

This feature is accessible by SWI Support personnel for troubleshooting purposes.

5.4 Alarm Setup

E-mail notification is a fast and convenient way to receive information from the VMS. Figure 5-25 shows a typical e-mail notification. Detailed instructions to configure the alarms and the e-mail notification are found “d017-0001-401-00_VMS_Client_UG.pdf”.

You must complete the setup below if you want to receive e-mail notification and your IT administrator must provide this information: Mail Server URL, Account Name and Password. Internet access may also be required.

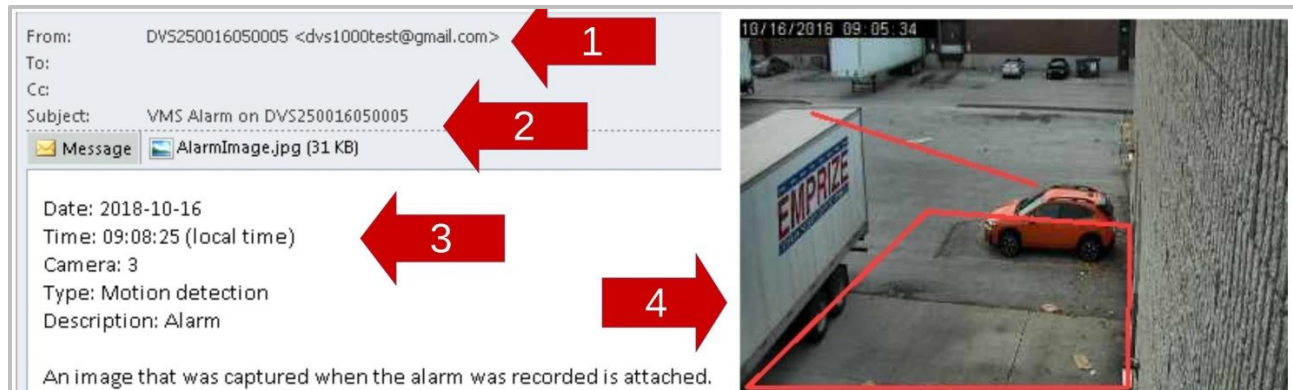


Figure 5-25 VMS E-mail Notification Alarm

Please note the main elements:

1. The server that sent the e-mail (arrow 1)
2. The subject indicates the serial number of the DVS (arrow 2)
3. The body of the e-mail contains: date, time and alarm type (arrow 3)
4. The attachment is a snapshot showing the trigger (arrow 4).

Note: To send emails using domain names instead of IP addresses, the DNS Server must be specified on the DVS's NIC (e.g. using Mail Server URL instead of Mail Server IP Address).

The Alarm Setup dialog for the “Legacy Mode” method is shown in Figure 5-26:

1. Alarm Age Limit: specifies how long the alarms should be stored in the local database before they are discarded or overwritten.
2. Minimum Time Between Alarms: this parameter dictates the delay between e-mails in order to avoid notification flooding.
3. Send Method: Legacy, App Password, None.
4. Email Address of Sender – provided by your IT Administrator. This is the email address associated with the DVS – in the example above the email address is “dvs1000test@gmail.com”.
5. Name of Sender – provided by your IT Administrator. This is the descriptive name for the email address – in the example above the descriptive name for the email address is “DVS250016050005”.
6. Mail Server URL – provided by IT Administrator.
7. Mail Server Account Name – provided by your IT Administrator.
8. Mail Server Account Password – provided by your IT Administrator.
9. Password Confirmation: retype the password in this field.
10. Port – provided by your IT Administrator.
11. Timeout – provided by your IT Administrator.
12. Authentication – provided by your IT Administrator. These are the mail server configuration parameters. Access to the company's email server is required in order to send emails from the DVS. Please see your local IT system administrator for mail server setup parameters.
13. Mail Server Use SSL – provided by your IT Administrator.

14. Alarm Retry Timeout: your selection – how long should the server wait after a timeout before a retry.
15. Send Test Email: Once the email configuration is completed, the user can verify email connectivity by sending a test email to a specified email address.
16. Press the Save button to preserve the configuration. Press the Cancel button to discard the changes.

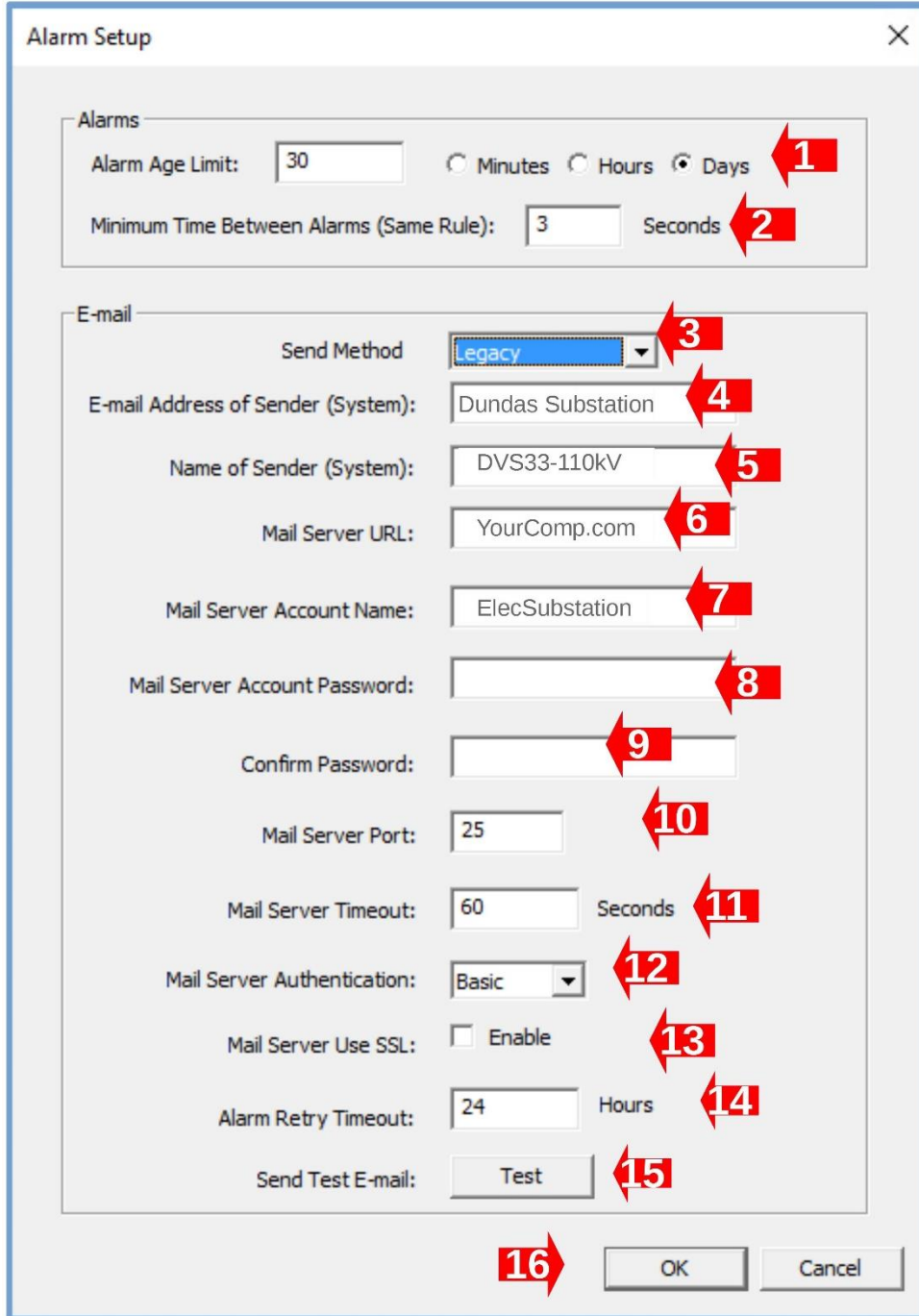


Figure 5-26 Alarm Setup- Legacy Mode

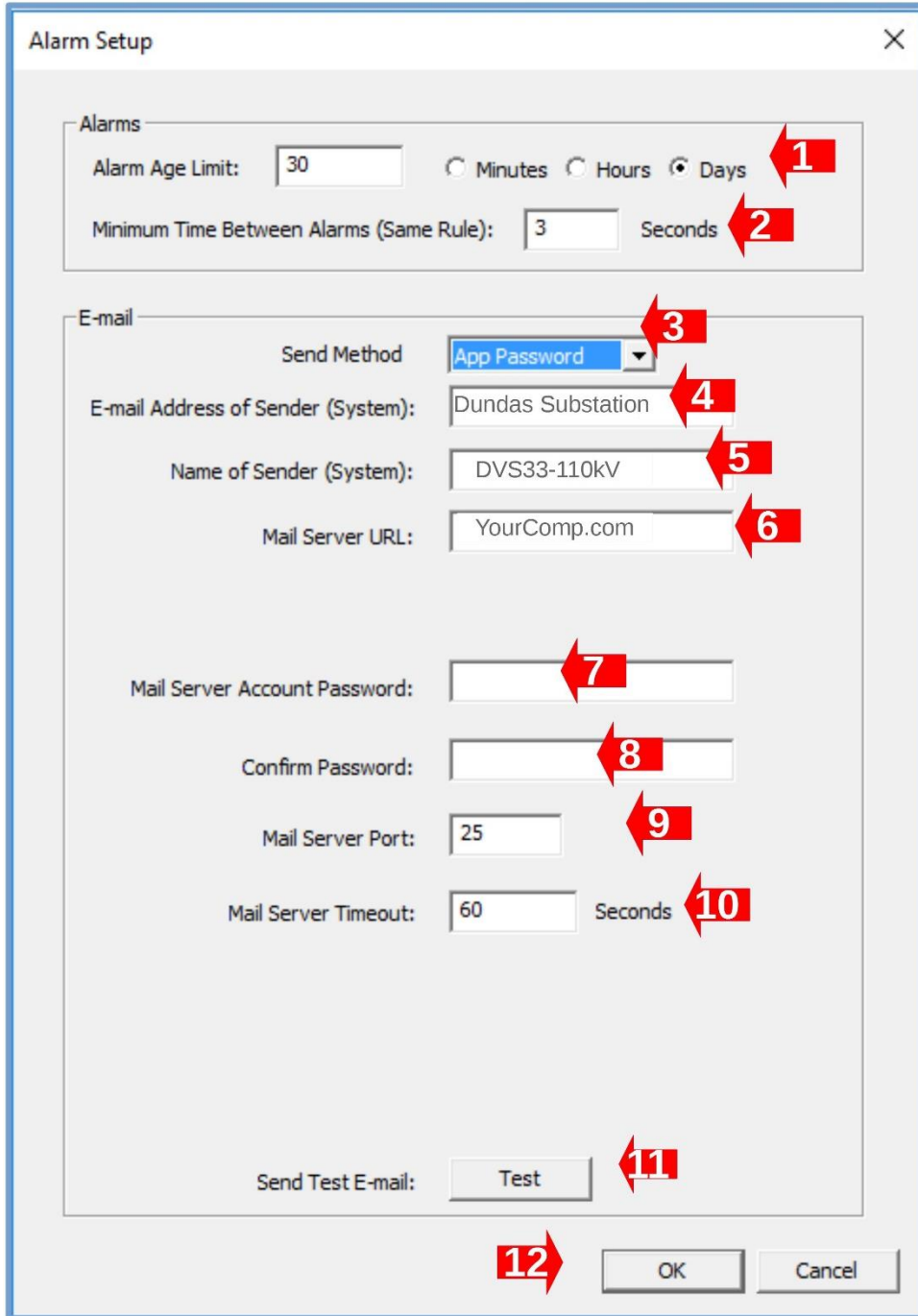


Figure 5-27 Alarm Setup- App Password

The Alarm Setup dialog for the “App Password” method is shown in Figure 5-27:

1. Alarm Age Limit: specifies how long the alarms should be stored in the local database before they are discarded or overwritten.
2. Minimum Time Between Alarms: this parameter dictates the delay between e-mails in order to avoid notification flooding.
3. Send Method: Legacy, App Password, None.
4. Email Address of Sender – provided by your IT Administrator. This is the email address associated with the DVS – in the example above is “dvs1000test@gmail.com”.

5. Name of Sender – provided by your IT Administrator. This is the descriptive name for the email address – in the example above is “DVS250016050005”.
6. Mail Server URL – provided by IT Administrator.
7. Mail Server Account Password – provided by your IT Administrator.
8. Password Confirmation: retype the password in this field.
9. Port – provided by your IT Administrator.
10. Timeout – provided by your IT Administrator.
11. Send Test Email: Once the email configuration is completed, the user can verify email connectivity by sending a test email to a specified email address.
12. Press the Save button to preserve the configuration. Press the Cancel button to discard the changes.

5.5 Stop Capture

Press this button to stop local recording of video. You could use this functionality when personnel is present for service and this may trigger a large number of alarms and recordings and overflow the storage drive. The caption of the button will change to “Start Capture” – press the button and enable the recordings.

Note: Video recording will start on DVS boot-up depending on the parameters set in VMS2000 Server Setup – see Figure 5-5 arrow 17 in section 5.3.



VMS2000 Server

2024.01.15

User's Guide



Systems With Intelligence Inc.
6889 Rexwood Road, Unit #9
Mississauga, Ontario, CANADA
L4V 1R2

Tel: +1-289-562-0126

Fax: +1-289-562-0152

General Inquiries:
info@SystemsWithIntelligence.com

Sales Inquiries:
sales@SystemsWithIntelligence.com

Product Support:
support@SystemsWithIntelligence.com