# Contents

About this guide ................................. viii

Video unit configuration

All manufacturers .................................... 2
  Troubleshooting H.264 video streaming ........ 2
  Enable audio out anti-jitter buffering ........ 3
ACTi .................................................. 4
  Configuring network connection ............ 4
  Select ACTi video streams ............ 4
  Upgrading ACTi unit firmware ............. 4
Arecont .............................................. 5
  Configure Arecont cropped field of view ... 5
  Configuring Arecont camera image settings 6
    Configure picture settings ............... 7
    Configure illumination settings ........ 7
    Configure exposure settings ........... 8
    Configure day/night settings .......... 9
    Configure frequency ................... 10
    Configure camera orientation .......... 11
  Upgrading Arecont unit firmware .......... 11
  Configuring Arecont H.264 units ........ 11
ATEME ............................................... 12
  Configure VSIP-2 units .................... 12
  Configure VSS-441-R4TE units ........ 13
Axis .................................................. 15
  Configure Axis H.264 cameras .......... 15
  Configure recording schedules .......... 15
  Configure trickling for Axis units ...... 16
  Configuring the Axis T8310 Video Surveillance Control Board .... 17
  Configure multi-view areas ................ 20
Creating PTZ patterns .......................................................... 21
Configure PTZ patterns ......................................................... 21
Edit PTZ presets ................................................................. 22
Configuring PTZ control for the Q8721/22-E ................................. 23
Configuring hostname address resolution .................................. 24

Basler . .................................................................................. 26
Change the default port for input pin events ................................. 26
Configuring Basler units ........................................................... 27
  Set the encoder type for all video streams .......................... 27
  Configure the frame rate ..................................................... 28
  Configure Basler BIP2 input/output pins .......................... 29
  Configure Basler BIP2-640c-dn units .......................... 29

Bosch . .................................................................................. 30
  Configure video analytics .................................................. 30
  Configuring Bosch H.264 units .............................................. 31
    Configure the video resolution ......................................... 31
  Configure Bosch audio inputs ............................................ 32
  Configuring Bosch Divar 700 DVRs ................................. 33
    Configure Analog cameras .............................................. 33
    Configure network cameras ............................................ 33
    Configure recording settings ........................................... 34
  Configuring Bosch VRM units ........................................... 35
    Enable audio recording .................................................. 36
  Configure the Bosch Intuikey CCTV keyboard ...................... 37
  Configuring Bosch units to receive hardware motion detection events ........................................... 39
  Configuring the VJT XTCXF transcoder .................................. 40

Canon . .................................................................................. 41
  Configuring Canon VB-C60 and VB-C500D units ................. 41
    Grant user access ......................................................... 41
    Enable MJPEG streaming ................................................ 41
    Enable PTZ control for VB-C60 units ........................ 42
  Configuring Canon VB-H41 for unit motion detection .......... 42

Cisco . .................................................................................. 43

Comtex . .............................................................................. 44
  Configure WB-H811 units .................................................. 44
Configure PTZ for WB-H811 units .................................................. 44

**Dynacolor** ................................................................. 45

**Epiphan** ........................................................................ 46
Configure VGA Broadcaster Lite units ........................................ 46

**ImmerVision** .................................................................... 48
Configuring ImmerVision Panomorph camera lenses .................... 48
Use the dewarping feature ....................................................... 50

**Interlogix** ...................................................................... 52
Configure Discovery 105-E (UVE-101) units .............................. 52
Enable software motion detection .............................................. 53
Configuring VisioWave units .................................................. 53
Add VisioWave units ................................................................ 53
Configure video ports .......................................................... 54
Enable PTZ ........................................................................... 54

**IQinVision** ...................................................................... 56
Configuring virtual zones ....................................................... 56
Using H.264 multicast streaming .............................................. 56

**Mango DSP** ..................................................................... 57
Configure input pin wiring ...................................................... 58
Configure input pin events on the standby Archiver ..................... 58
Change the default port for input pin events ............................... 58

**Mavix** ............................................................................. 60
Configuring MediaRacer units ................................................ 60
Add Mavix MediaRacer units .................................................. 60
Configure PTZ controls ........................................................ 61
Change the IP address .......................................................... 62
Configure MediaRacer 152 units ............................................. 63
Configure MediaRacer 250 units ............................................. 64
Select H.264 or MPEG-4 streaming ......................................... 64
Configure the stream settings ................................................. 65

**Oncam Grandeye** ............................................................. 66
Configure Oncam Grandeye 360° fish-eye camera lenses ............ 66
Use the dewarping feature ..................................................... 68
Configure digital zoom presets ............................................... 69

**OTN** ............................................................................... 70
Configuring MVIDIPv4 units ........................................ 70
Disable IGMPv3 support ........................................ 70
Enable MPEG-4 start code lookup offset ...................... 71

Panasonic .......................................................... 72
Configuring H.264 software motion detection .................. 72
Configuring multi-streaming in MJPEG .......................... 72
Configuring I/O pins ................................................. 73
Configure capture resolutions .................................... 74
Configuring edge analytics for WJ-NT314 units .............. 74
Configure WJ-GXE500 (DG-GXE500) units ..................... 75
Use auto-pan with Panasonic units ............................ 75
Configuring the Panasonic WV-CU950 Ethernet keyboard ...... 76
  Configuring the keyboard ...................................... 76
  Security Center configuration ................................ 77
Configuring Variable Image Quality on Specified area (VIQS) ... 78
Configuring Auto tracking ......................................... 79

Pelco ............................................................... 81
Configuring motion detection .................................... 81
Adding NET54xx encoder series ................................ 81
Configuring dual-streaming for Pelco IP series ............... 81
Configuring NET5301T units .................................... 81
Configuring Pelco Sarix units .................................. 82
Naming Sarix Spectra HD PTZ preset tours ..................... 82

Samsung ............................................................ 83
Configure SNP-3750 units ....................................... 83
Configure Samsung ONVIF units to stream at the proper framerate ... 84
Creating video profiles ........................................... 85

Sanyo ............................................................... 86
Configure VCC-HD5X00 units .................................. 86
Add Sanyo ONVIF units ......................................... 86

Sentry 360 .......................................................... 87
Configuring resolution and stream settings on a 1.3 or 2 megapixel unit ... 87
Setting the resolution for a 5 or 10 megapixel unit .......... 88
Configure Sentry 360-degree fish-eye camera lenses ........ 89
Use the dewarping feature ....................................... 91
Configure digital zoom presets .......................... . 92
Change the default port for motion events ............... . 93

Sony .................................................................. . 95
Configure Sony 5th generation cameras ................... . 95
Creating Sony PTZ patterns ................................. . 95
  Define presets .................................................. . 95
  Configure the preset tour ................................... . 96
  Test the Sony PTZ pattern ................................... . 98

Using the Copy configuration tool ......................... . 99
Configure Sony edge recording and video trickling ........ . 100
Maintaining 4:3 aspect ratio for the SNC-ZP550 ......... . 101
Configuring 6th generation units to stream at 60 frames per second . 103

UDP Technology .................................................. . 105

Verint ............................................................... . 106
Configure S1808e-A and S1816e-A units ................. . 106

Videotec ............................................................ . 107
Configuring the wiper on the Ulisse Compact IR360 .. . 107

Vivotek ............................................................. . 108
Configure IP8161 units ....................................... . 108
Configure Vivotek FE8171V fish-eye cameras .......... . 108
  Enable watermarking on the FE8171V fish-eye camera . 108
  Configure Vivotek FE8171V fish-eye cameras lenses .... . 109
  Use the dewarping feature ................................. . 110
Configure digital zoom presets ........................... . 112
About this guide

Some supported video units can be directly integrated into Security Center; that is you just connect the unit to your network and then add the unit to your Security Center system from the Config Tool. Other supported video units require additional set up from their web-based configuration page before they can be added to Security Center.

This guide explains the pre-configuration instructions for selected video units, and any additional configuration steps required for some video unit features to work in Security Center 5.2 SR2. It supplements the Security Center Administrator Guide.

NOTE For details such as firmware and certification status of the video units supported by Security Center, see the Supported Devices list on Genetec’s Technical Assistance Portal (GTAP) at https://gtap.genetec.com.

This guide is written for installers, integrators, and Security Center administrators. It assumes you are familiar with the following concepts and systems:

- Microsoft Windows operating system
- Networking concepts and computer hardware knowledge
- Security and video surveillance system concepts
- Security Center applications
Video unit configuration

This section contains the pre-configuration instructions for adding selected video units in Security Center 5.2 SR2. It also includes additional configuration steps required for some video unit features to work in Security Center. This section is organized by manufacturer and/or model.

This section includes the following topics:

- "All manufacturers" on page 2
- "ACTi" on page 4
- "Arecont" on page 5
- "ATEME" on page 12
- "Axis" on page 15
- "Basler" on page 26
- "Bosch" on page 30
- "Canon" on page 41
- "Cisco" on page 43
- "Comtex" on page 44
- "Dynacolor" on page 45
- "Epiphan" on page 46
- "Interlogix" on page 52
- "IQinVision" on page 56
- "Mango DSP" on page 57
- "Mavix" on page 60
- "Oncam Grandeye" on page 66
- "OTN" on page 70
- "Panasonic" on page 72
- "Pelco" on page 81
- "Samsung" on page 83
- "Sanyo" on page 86
- "Sentry 360" on page 87
- "Sony" on page 95
- "UDP Technology" on page 105
- "Verint" on page 106
- "Vivotek" on page 108
This section includes video unit configuration information pertaining to all manufacturers.

This section includes the following topics:

- "Troubleshooting H.264 video streaming" on page 2
- "Enable audio out anti-jitter buffering" on page 3

### Troubleshooting H.264 video streaming

If you are having problems viewing H.264 streams, you can disable the `AVCodec_ErrorRecognition` advanced setting.

1. From the Video task in Config Tool, select the Archiver to configure.
2. Click the Resources tab.
3. At the bottom of the Resources tab, click the Advanced settings button.
4. In the Advanced settings dialog box, click the Additional settings button.
5. In the Additional settings dialog box, click [ ].
6. In the Name column, type `AVCodec_ErrorRecognition`.
7. In the Value column, type 0.
8. Click Close.
9. In the Advanced settings dialog box, click OK.
10. In the Resources tab, click Apply.

You are asked to restart the Archiver. Click Yes.
Enable audio out anti-jitter buffering

Axis, Sony, and Verint extensions can be configured to use the audio out anti-jitter buffer. With this feature enabled, the Archiver buffers the audio packet before sending it to the unit’s audio decoder, eliminating any jittering that may occur. To enable this feature, you need to activate the `AudioOutDelay` advanced setting.

1. From the Video task in Config Tool, select the Archiver to configure.
2. Click the Resources tab.
3. At the bottom of the Resources tab, click the Advanced settings button.
4. In the Advanced settings dialog box, click the Additional settings button.
5. In the Additional settings dialog box, click .
6. In the Name column, type `AudioOutDelay`.
7. In the Value column, type `400`.
8. Click Close.
9. In the Advanced settings dialog box, click OK.
10. In the Resources tab, click Apply.
    You are asked to restart the Archiver. Click Yes.
ACTi

This section describes the additional configuration steps required for some ACTi units to work in Security Center.

• "Configuring network connection" on page 4
• "Select ACTi video streams" on page 4
• "Upgrading ACTi unit firmware" on page 4

Configuring network connection

To ensure that ACTi units have a valid network connection, the unit must be connected to the network using a WAN port (not a LAN port).

Select ACTi video streams

Multi-streaming cannot be used with the ACTi extension in Security Center. You must select which video stream to use for ACTi cameras in the Config Tool.

1 From the Logical view task in Config Tool, select the camera to configure.
2 Click the Hardware tab.
3 From the Video stream drop-down list, select MJPEG, MPEG-4, or H.264.
4 Click Apply.

After you are done: Configure the video stream settings as usual in the Video tab.

Upgrading ACTi unit firmware

To upgrade ACTi unit firmware, you must use the unit’s Web page, or the ACTi IP Utility. For more information, see your ACTi manufacturer documentation.
This section describes the additional configuration steps required for some Arecont unit features to work in Security Center.

- "Configure Arecont cropped field of view" on page 5
- "Configuring Arecont camera image settings" on page 6
- "Upgrading Arecont unit firmware" on page 11
- "Configuring Arecont H.264 units" on page 11

**Configure Arecont cropped field of view**

You can specify the settings of a cropped field of view for Arecont units with H.264 and MJPEG video streams.

1. From the Video task in Config Tool, select the camera to configure.
2. Click the Video tab, and set the Crop image setting to ON.

3. Select the number of pixels to remove from the Left, Right, Top, and Bottom of the image. The Video image size with your modifications is displayed underneath.

   **NOTE** The resolution of the video may not exactly match the Video image size.

4. Click Apply to save your changes.
Configuring Arecont camera image settings

You can configure additional camera image setting in the Hardware tab of Arecont cameras in Config Tool.

This section includes the following topics:

• "Configure picture settings" on page 7
• "Configure illumination settings" on page 7
• "Configure exposure settings" on page 8
• "Configure day/night settings" on page 9
• "Configure frequency" on page 10
• "Configure camera orientation" on page 11
Configure picture settings

You can configure the following picture settings in the Hardware tab of Arecont cameras in Config Tool:

- **Sharpness.** Adjusts the image crispness.
- **Blue.** Adjusts the blue tint. This setting changes the camera’s automatic white balance. Valid value are from -64 to +64 for panoramic models, and -10 to +10 for others camera models.
  
  **NOTE** It takes a few seconds for the camera to adjust to the new setting.

- **Red.** Adjusts the red tint. This setting changes the camera's automatic white balance. Valid value are from -64 to +64 for panoramic models, and -10 to +10 for others camera models.
  
  **NOTE** It takes a few seconds for the camera to adjust to the new setting.

Configure illumination settings

You can configure the following illumination settings in the Hardware tab of Arecont cameras in Config Tool:

- **Illumination mode.** Adjusts the camera's white balance settings based on the illumination in the scene. From the drop-down list, choose one of the following options:
  - *Automatic.* The camera's white balance is adjusted automatically.
  - *Indoor.* Assumes the camera is located indoors with tungsten or fluorescent lighting.
  - *Outdoor.* Assumes the camera is located outdoors with natural lighting.
  - *Mix.* Assumes the camera is located indoors with natural lighting.
  - *Mix.* Assumes the camera is located somewhere where there is a mix of tungsten or fluorescent lighting, and natural lighting.
Configure exposure settings

You can configure the following exposure settings in the Hardware tab of Arecont cameras in Config Tool:

- **Auto exposure.** When this option is ON, it maintains the user-defined image brightness under changing lighting conditions.
- **Exposure Window.** If the camera is not a panoramic model, you can specify the auto exposure window size and position.
  a Next to the Auto Exposure setting, click Exposure window.
  b To re-size the exposure window, do one of the following:
    - In the Size and position section, enter the X, Y, W, and H coordinates.
      X is the Top-left pixel, Y is the Bottom-left pixel, W is the Top-right pixel, and H is the bottom-right pixel.
    - Drag the green zone to the size you want.
      If you have a cropped field of view, then the exposure window must be contained within the cropped field of view. For more information about setting a cropped field of view, see "Configure Arecont cropped field of view" on page 5.
  c Click OK.
- **Low light mode.** Adjusts the exposure to increase performance under low light conditions. Exposure time is the amount of time the sensor is exposed to light. Short exposures result in less light, creating darker images, and longer exposures create brighter images.
- **High Speed.** Allows you to set a fixed exposure time from the Short Exposure slider.

![Image of Arecont Security Center Video Unit Configuration Guide](image)

- **Speed.** Enables short exposures ranging from 10 to 80ms. The exposure time increases in low light conditions.
- **Balanced.** Enables medium exposures ranging from 20 to 80ms in low light conditions, resulting in a higher exposure time.
- **Quality.** Enables longer exposures ranging from 40 to 200ms. Motion blur may increase, but video contains less noise under low light conditions.
- **Moon Light.** Enables exposures of up to 500 ms if necessary. This mode results in more motion blur for fast moving objects.

- **Short Exposure.** Sets the fixed exposure time when you set the Low light mode to High Speed.

**Configure day/night settings**

You can configure the following day/night settings in the *Hardware* tab of Arecont unit entities in Config Tool.

**NOTE** These settings are only supported on dual-sensor cameras (for example, the AV135 and A3130), and cameras equipped with an IR filter (DN and IR models).

**NOTE** Low values reduce motion blur, but may result in noisier video. Make sure you have enough illumination to improve the image quality.
• Day/Night mode. Determines whether the camera operates in daytime or nighttime modes, which adjusts the amount of light.
  - Auto. Allows the camera to switch from daytime to nighttime conditions automatically, based on the Switching Gain and Toggle Guard settings.
  - Day. Forces Day mode, and disables Night mode.
  - Night. Forces Night mode, and disables Day mode.

• Switching Gain. Determines the level of darkness required for the camera to switch from Day to Night mode when the Day/Night mode is set to Auto. Small values cause the camera to switch to Night mode when there is still a lot light in the scene, and larger values cause the camera to stay in Day mode much longer.
  **TIP** For AV3130 and AV3135 units, you can set the gain from 0 to 18, and for other units you can set it from 64 to 512.

• Toggle Guard. Adjusts the level of brightness required to switch from Night to Day mode. This setting should be adjusted to prevent the camera from toggling modes during transitional lighting periods.
  **TIP** Setting this option to 0 corresponds to the camera switching at 100%. For AV3130 and AV3135 units you can set the toggle guard value from 0 to 6, and for other units you can set it from 1 to 4.

**Configure frequency**

The frequency feature prevents flicker caused by lightning power line frequency.

**NOTES**

- This setting has no effect when the dominant light is sunlight.
- This setting loses effect if the camera’s Low Light Mode exposure option is set to High Speed, and the Short Exposure value does not match the power line frequency. The Short Exposure value matches the power line frequency when it is close to a multiple of 8.3ms for 60 Hz, and a multiple of 10ms for 50Hz.

For information about configuring Arecont exposure settings, see “Configuring Arecont camera image settings” on page 6.

1. In the Video task of the Config Tool, select the unit to configure.
2. Click the Properties tab.
3. In the Others section, select one of the following options:
   - For North America or Japan: 60 Hz
   - For Europe or China: 50 Hz

4. Click Apply.
Configure camera orientation

You can set the camera's orientation in the Hardware tab of Arecont cameras in Config Tool.

1. In the Logical View of the Config Tool, select the camera to configure.
2. Click the Hardware tab.
3. For the Image Rotation drop-down list, select 0 or 180.
4. Click Apply.

Upgrading Arecont unit firmware

To upgrade the firmware for Arecont units, you must use the Arecont Firmware Loader. Before you upgrade, you must ensure that the unit is not streaming video. If the unit is streaming video, remove the schedule from the camera.

Configuring Arecont H.264 units

To use key frame-related functions (such as still alarms) with Arecont H.264 cameras, you must set a high frame rate, or modify the frame interval between key frames. To change the interval setting, use the following URL: http://<camera.ip>/setreg?page=3&reg=21&val=<value meant to replace the 50>. For example, if your camera IP is 10.1.24.35 and you want to change the interval setting to five, you would type: http://10.1.24.35/setreg?page=3&reg=21&val=5.

NOTE If you are using an Arecont SurroundVideo IP Camera, you must replace the 21 in the URL with 100 (http://10.1.24.35/setreg?page=3&reg=100&val=5).
This section describes the additional configuration steps required for some ATEME units to work in Security Center.

This section includes the following topics:

- "Configure VSIP-2 units" on page 12
- "Configure VSS-441-R4TE units" on page 13

## Configure VSIP-2 units

Complete the following configuration steps before adding ATEME VSIP-2 units to the Config Tool:

1. Open the unit’s Web page.
2. Click Video Settings > Physical Input.
3. On the Physical Video Input Settings page, set the Scan mode to Progressive.
4. Click Save to apply your changes.
Configure VSS-441-R4TE units

Before adding ATEME VSS-441-R4TE units in Security Center, you need to configure the video inputs, enable all video streams, and configure the serial port on the unit's Web page.

1. Open the unit's Web page.
2. Click Video Settings > Physical Input.
3. On the Physical Video Input Settings page, click the Video 1 input tab.
4. From the Color System drop-down list, select NTSC.
5. From the Scan Mode drop-down list, select Progressive.

6. Repeat Step 3 to Step 5 for every video input.
7. Click Save.
8. Click Streaming settings > Video Stream Settings.
9. On the Video Streams Settings page, click the Video 1 input tab, and then click the Stream 1 tab.
10 Select the Enable stream option.

11 Repeat Step 9 and Step 10 for every video input, and every video input stream.

12 Click Save.

13 Click Serial Interface > Tunneling.

14 On the Serial Interface Tunneling page, configure the serial port as desired.

   NOTE   The port settings should match your PTZ camera settings.

15 Click Save.
This section describes the additional configuration steps required for some Axis unit features to work in Security Center.

This section includes the following topics:

- "Configure Axis H.264 cameras" on page 15
- "Configure recording schedules" on page 15
- "Configure trickling for Axis units" on page 16
- "Configuring the Axis T8310 Video Surveillance Control Board" on page 17
- "Configure multi-view areas" on page 20
- "Creating PTZ patterns" on page 21
- "Configuring PTZ control for the Q8721/22-E" on page 23
- "Configuring hostname address resolution" on page 24

**Configure Axis H.264 cameras**

To increase the image quality and decrease the bit rate for Axis H.264 video streams, the recording stream can be configured to use the Main profile in Config Tool.

**NOTE** The Main profile is only supported on some Axis H.264 models. If the Profile option is not available in Config Tool, then the camera does not support the profile selection feature.

1. From the Logical view in Config Tool, select a camera to configure.
2. Click the Video tab, click the stream1 tab.
3. From the Profile drop-down list, select Main profile.
4. Click Apply.

**Configure recording schedules**

Best practice: For Axis units with firmware prior to version 5.40, it is best practice to create scheduled events using the unit's Web page, instead of configuring the recording schedules in the Recording tab in Config Tool. The shorter the sequence the better; therefore, it is also recommended to create multiple scheduled events per day rather than one large one.
Configure trickling for Axis units

Best practice: To improve readability when trickling with Axis units, use an SDHC memory card or an SD card with a speed class of four or higher, and use H.264 streaming. For more information about which SD cards are recommended for use with your unit, see your Axis documentation.

To avoid having an Axis camera’s SD card fill up and stop recording when trickling is enabled, the `EdgeTransferRemoveRecordingOnUnit` advanced setting must be activated.

1. From the Video task in Config Tool, select the Archiver to configure.
2. Click the Resources tab.
3. At the bottom of the Resources tab, click the Advanced settings button.
4. In the Advanced settings dialog box, click the Additional settings button.
5. In the Additional settings dialog box, click 🐤.

6. In the Name column, type `EdgeTransferRemoveRecordingOnUnit`.
7. In the Value column, type `1`.
8. Click Close.
9. In the Advanced settings dialog box, click OK.
10. In the Resources tab, click Apply.

You are asked to restart the Archiver. Click Yes.
Configuring the Axis T8310 Video Surveillance Control Board

The Axis T8310 Video Surveillance Control Board system allows you to control PTZ motors, switch between cameras, control playback, customize peripheral buttons, etc. It consists of three units that can be installed together, or as separate peripherals in Security Desk:

- **AXIS T8311.** A joystick that allows you to accurately control the pan/tilt/zoom functions of cameras on the network. It has three customizable axis, six customizable buttons, and is configured like any other joystick.
  
  For more information about configuring joysticks, see "Joystick configuration" in the Security Desk User Guide.

- **AXIS T8312.** A keyboard that allows you to navigate quickly between workspaces, cameras, views, and PTZ presets. It has 0-9 digits, and twelve customizable buttons.
• AXIS T8313. A jog dial that allows you to look through video frames while controlling the speed of the playback. The outer wheel of the jog dial controls the playback speed of the selected video in the Archive Player, and the playback speed of the selected video in *Instant replay* mode in the Live Viewer. The inner wheel navigates through the selected video forwards frame-by-frame, or backwards keyframe-by-keyframe. It also has six customizable buttons.
The AXIS T8312 and the AXIS T8313 can be used together as one external keyboard, and associated to Security Desk commands of your choice. The 12 customizable buttons on the T8312 keyboard are mapped first, followed by the 6 buttons on the T8313 jog dial.

Before you begin: If the CCTV keyboard is currently being used in another client application, disconnect it.

- In Security Desk, click Options > Peripherals > Keyboard > Disconnect.
  
  NOTE: If you cannot see the Disconnect button, clear the Connect to keyboard automatically option.

To configure the Axis CCTV keyboard:

1. In Security Desk, click the Home tab, and click Options > Peripherals > Keyboard.
2. From the Keyboard protocol drop-down list, select Axis Control Board.
3. From the Button column, select a button to configure.
4. Under Down command, expand the drop-down menu to see a list of commands you can choose from.

You can associate a Down command and Up command for each button. The Up command is optional.

5. Click Save.

The Axis CCTV keyboard is now ready to use in Security Desk.
Configure multi-view areas

The Axis multi-view feature enables the creation of additional streams by cropping the camera's field of view. Additional configuration is required for the Axis multi-view feature to work in Security Center.

1. Open the unit's Web page.
2. Click Setup > Video & Audio > View Areas.
3. Click the Add button.
   A new view area is created (Example: View Area 1).
4. Select the location and size of the new view area.
   You can modify the view area size by dragging the lower-right corner of the selected area.
5. Set the Aspect ratio to 4:3, 16:9, or 11:9.
6. Select the appropriate Video stream resolution for the area size.
   **IMPORTANT** You must manually set the video stream resolution in Security Center to match the resolution set in the unit's Web page for the multi-view feature to work.
7. Click Save.
8. Do one of the following:
   - If the unit is not yet part of the Security Center system, add it in the Config Tool. For more information on adding video units in Security Center, see "Adding video units to your system" in the Security Center Administrator Guide.
   - If the unit is already in the Security Center system, restart the Config Tool to update your changes.
Creating PTZ patterns

PTZ patterns can be created for some Axis cameras through the guard tour feature. An Axis guard tour is similar to a Security Center PTZ pattern; it is a series of presets (including camera position, iris, and focus settings) which can run in the Security Desk or Config Tool the same as any other PTZ pattern. Refer to your Axis camera’s documentation for more information on guard tours.

Configure PTZ patterns

Once an Axis camera that supports the guard tour feature is added in Security Center, ten empty patterns are automatically created, initially named "0 - Untitled" through "10 - Untitled". These patterns can then be renamed in the Config Tool, and configured in the Axis camera’s Web page.

IMPORTANT Do not create new patterns or rename patterns in the Axis camera’s Web page. This will result in unusable patterns. Instead, perform all of these actions in Security Center.

Before you begin: The following is required to configure PTZ patterns in Security Center:

- The Axis camera you are using must have the guard tour feature, and be running firmware version 4.40 or later. For a list of Axis cameras that currently support this feature, see the Supported Devices list on Genetec’s Technical Assistance Portal (GTAP): https://gtap.genetec.com/Library/SupportedDevices.aspx. Please note that you’ll be required to login using your e-mail address and password.
- Standard user privileges for working with PTZ patterns must be enabled.

To rename PTZ patterns:

1. From the Logical view task in Config Tool, select the Axis camera that contains the PTZ patterns you want to rename.
2. Click Live video in the Common tasks area.
3. In the PTZ advanced mode commands, select the pattern you want to rename from the Pattern drop-down list.
4. Click the Rename button.
5. In the dialog box that appears, enter a new name for the pattern.
6. Click Rename.
   The pattern’s new name is reflected in Security Center and in the Axis camera’s Setup configuration Web page.
7. Repeat Step 1 to Step 6 for each pattern to be configured.
To configure Axis guard tours:

1. Open the Axis camera’s Web page.
2. Follow the Axis documentation that comes with your camera to configure the Axis guard tours (PTZ patterns renamed in Security Center).

   **NOTE** Since Security Center creates empty Axis guard tours (PTZ patterns) when the camera is added, when you configure the guard tours in the camera’s Web page you are modifying the *existing* Security Center presets as opposed to adding new ones.

The configured Axis guard tours become available in Security Center to use as PTZ patterns for the camera.

After you are done: Test the Axis PTZ patterns in Security Center. They should run the same way as other PTZ patterns.

**Edit PTZ presets**

You can edit presets that are used in PTZ patterns on Axis cameras. When you make a change to a preset, it is immediately reflected in the PTZ pattern.

**IMPORTANT** Make all of your changes in Security Center, not in the camera’s Web page.

1. In the PTZ advanced mode commands in Config Tool or Security Desk, select the preset you want to edit from the Presets drop-down list.
2. With the PTZ controls, adjust the camera position, iris, zoom, and focus settings to the desired positions.
   - If you are working in the Security Desk, you can also click inside the tile and move the camera to a new position.
3. Click the Edit button.
   - The current position and settings of the camera are recorded. Changes to the preset are reflected for all PTZ patterns that use this preset on the Axis camera.
   - If a PTZ pattern using the preset is currently playing, it stops. If necessary, restart it. At this point changes to the preset take effect.
Configuring PTZ control for the Q8721/22-E

The Q8721-E and Q8722-E are units that have two cameras on the same unit. The Q8721-E has a Q1755 and Q1921, and the Q8722-E has a Q1755 and a Q1922. The PTZ control must be enabled on the Q1755 unit.

1. From the Video task in Config Tool, select the Q1755 unit and click the Peripherals tab.
2. Select the Serial (RS422/485) port.
3. In the Serial port properties dialog box enter the following settings:
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Baud rate: 2400
   - Mode: RS485 2-wire
4. Click Save.
5. Click the Properties tab, and select the External pan tilt module connected option.
6. Click Apply.
Configuring hostname address resolution

In order for Security Center to detect which units have changed their IP address and automatically reestablish a connection, the Allow hostname address resolution option must be selected in the Axis Extensions tab.

1. From the Video task in Config Tool, select the Archiver you want to configure and click the Extensions tab.
2. Under Installed extensions click Axis then select Allow hostname address resolution.

The discovery is performed every hour, but can be configured in minutes using the Advanced Settings dialog box.

To do this:
1. At the bottom of the the Extensions tab page, click Advanced settings.
2. Click the button.
3. Under Name enter UnitReenrollmentPeriod.
4 Under Value, enter in minutes how often you want the discovery to be performed. For example, if you want the discovery to be done every 15 minutes, enter 15.

5 In the Advanced settings dialog box, click Close.

6 In the Extensions tab, click Apply.
This section describes the additional configuration steps required for some Basler units and features to work in Security Center.

This section includes the following topics:

- "Change the default port for input pin events" on page 26
- "Configuring Basler units" on page 27
- "Configure Basler BIP2 input/output pins" on page 29
- "Configure Basler BIP2-640c-dn units" on page 29

**Change the default port for input pin events**

In order to receive input pin events from Basler units, the Archiver role needs to open a TCP port for its HTTP server. The default port is 8008. If this port is already in use on the Archiver role machine, you can change the default port.

To change the default port:

1. On the Archiver role machine, navigate to the installation directory, located in `C:\Program Files\Common Files\DVR Software 5.2\Extensions\Drivers\` on 32-bit machines, and `C:\Program Files (x86)\Common Files\DVR Software 5.2\Extensions\Drivers\` on 64-bit machines.
2. Open the `EventHttpServerConfiguration.xml` file in Notepad.

   Text similar to the following is displayed:

   ```xml
   <EventHttpServerConfiguration>
   <HttpServerPort>8008</HttpServerPort>
   </EventHttpServerConfiguration>
   ```

3. Change the value of the `HttpServerPort` from 8008 to something else, such as 8009.

   **NOTE** The value for the `HttpServerPort` must be the same for all standby Archivers associated with the unit.

4. Save the file, and restart the Archiver role.
Configuring Basler units

Complete the following configuration procedures before adding Basler units in Security Center.

This section includes the following topics:

- Set the encoder type for all video streams
- Configure the frame rate

Set the encoder type for all video streams

For each video stream you’ll be using, you need to select the encoder type you want to use to compress the stream.

1. Open the unit’s Web page.
2. Click Configuration > Camera Configuration > Streaming.
3. Click one of the video stream tabs.
4. From the Encoder Type drop-down list, select the desired encoder type for that stream.
   
   **NOTE** Multicast can only be used with Stream0. To use multicast with Stream0, set the Encoder Type to H.264 or MPEG-4.

5. Repeat Step 4 for each video stream you want to use.
NOTE You can disable Stream1 and Stream2 if you are not using them. From the Encoder type drop-down list, select Off. Only disable Stream2 if Stream1 is also disabled.

6 To save your settings, close the Streaming section of the unit’s Web page.

After you are done: If the unit was already part of your Security Center system, restart the unit to apply your changes.

Configure the frame rate

For Basler units to stream at the exact frame rate set in Security Center, you must configure the Exposure Mode setting on the unit’s Web page.

1 Open the unit’s Web page.
2 Click Configuration > Camera Configuration > Image Controls.
3 From the Exposure Mode drop-down list, select Prioritize: Framerate.
4 To apply your settings, close the Image Controls section of the unit’s Web page.

If you want the video streams to use a frame rate other than the values available in Security Center, you also need to change the Frame Rate Mode setting in the unit’s Web page.

5 Click the Camera Configuration > Streaming tab.
6 Click the Global tab.
7 From the Frame Rate Mode drop-down list, select the desired frames per second value.

   When you change the Global Frame Rate Mode setting, the frame rate values available in Security Center change. The values available in Security Center are 1:1, 1:2, 1:4, and 1:8 of the Global Frame Rate Mode value.

After you are done: If the unit was already part of your Security Center system, restart the unit to apply your changes.
Configure Basler BIP2 input/output pins

Basler BIP2 pins are bidirectional; they can be designated as inputs or outputs. Before adding Basler BIP2 cameras in Security Center, you must define the pins as inputs or outputs in the unit's Web page.

1. Open the unit’s Web page.
2. Click Configuration > Camera Configuration > Input/Output.
3. Click the Digital I/O tab, and then click the I/O 0 (pin 0) tab.
4. From the Direction drop-down list, select Input or Output, depending on how you want the pin to be configured.

**EXAMPLE** If you want to receive hardware motion detection events in Security Center you need to select Output for all the pins.

5. Repeat Step 3 and Step 4 for each available pin.

**NOTE** Basler BIP2 units only support one input.

6. To apply your settings, close the Input/Output section of the unit’s Web page.

After you are done: If the unit was already part of your Security Center system, restart the unit to apply your changes.

Configure Basler BIP2-640c-dn units

For Basler BIP2-640c-dn units to work at a high frame rate, additional configuration steps are required in Security Center.

**To configure H.264 streams at 100 fps:**

1. The camera must be configured for a sensor frame rate of 100 fps.
2. Stream0 of the camera must be configured for MJPEG, and a frame rate scaling of 1/8 (meaning Stream0 would yield only 12.5 fps).
3. Stream1 must be configured for H.264.
4. Stream2 must be switched off (the user cannot use MPEG4 simultaneously).

Depending on the complexity and the amount of movement in the scene, the frame rate may drop from 100 to 95. This happens particularly if the camera’s text overlays are activated.

**To configure MJPEG streams at 60 fps:**

1. The camera must be configured for a sensor frame rate of 60 fps.
2. Stream0 of the camera must be configured for MJPEG.
3. Stream1 and Stream2 must be switched off (the user cannot use H.264 or MPEG4 simultaneously).
This section describes the additional configuration steps required for some Bosch units and unit features to work in Security Center.

This section includes the following topics:

- "Configure video analytics" on page 30
- "Configuring Bosch H.264 units" on page 31
- "Configure Bosch audio inputs" on page 32
- "Configuring Bosch Divar 700 DVRs" on page 33
- "Configuring Bosch VRM units" on page 35
- "Configure the Bosch Intuikey CCTV keyboard" on page 37
- "Configuring Bosch units to receive hardware motion detection events" on page 39
- "Configuring the VJT XTCXF transcoder" on page 40

Configure video analytics

Before you begin: For video analytics (IVA) to work on Bosch units in Security Center, you will require the following:

- A valid video analytics license from the manufacturer must be installed on the unit.
- Your Security Center license must support edge analytics cameras.

NOTE The video analytics rules for the unit can only be configured using the Bosch Configuration Manager. To use the Bosch Configuration Manager, you will need a valid license from the manufacturer, and ActiveX must be installed.

To configure video analytics for Bosch units:

1. Open the Bosch Configuration Manager.
2. In the Network tab, select the unit to configure.
3. Click Alarm, and click the VCA tab.

NOTE In order to see the Alarm tab, Advanced Mode must be enabled.

4. From the Analysis type drop-down list, select the video analytics type you have a license for.
5. Click the Configuration button.
6. In the IVA Wizard window, make any required changes to the video analytics rule configuration, and click OK.
7. Click Save.

If your unit was already part of the Security Center system, restart the Config Tool for your changes to take effect.
Configuring Bosch H.264 units

This section describes the additional configuration steps required for some Bosch H.264 unit features to work in Security Center.

Configure the video resolution

To configure the video resolution for Bosch H.264 units with firmware 4.50 and later, you must first select a base operation mode.

NOTE If the unit has two H.264 video streams, the settings for stream2 are limited to the settings specified for stream1.

1. In the Logical view of the Config Tool, select the camera to configure.
2. Click the Hardware tab.
3. From the Video Mode drop-down list, select a base operation mode.
   Depending on the mode you choose, the available resolutions and video quality settings for the two H.264 streams change. For example, to enable a video frame rate of 60 frames per second, select 1:720p 60fps, 2:Copy.

4. Click Apply.
5. Click the Video tab.
6 From the Resolution drop-down list, select the desired resolution.
7 Click Apply.

Configure Bosch audio inputs

When you add Bosch units with firmware 5.0 and later in Security Center, two microphone (audio input) entities appear under the unit as child devices in the camera’s Identity tab. In Security Center, you can only associate one microphone with a camera. Therefore, you need to select which microphone to use, select the data format, and associate the microphone to the camera.

1 In the Logical view of the Config Tool, select the Bosch unit.
2 Click the Hardware tab.
3 From the Microphone drop-down list, select the microphone you want to use with the camera.
4 Click Apply.
Configuring Bosch Divar 700 DVRs

Perform the following configuration steps in the Bosch Divar Web page before adding the associated units in Security Center.

- "Configure Analog cameras" on page 33
- "Configure network cameras" on page 33
- "Configure recording settings" on page 34

Configure Analog cameras

If there are analog cameras connected to the Bosch Divar 700, you must enable the video input for those units in the Divar’s Web page.

Before you begin: Connect the video output of the analog cameras to the Video In connections on the Divar. The number of connectors depends on the type of Divar you have. The maximum number of analog cameras you can have is 16.

1. Open the Bosch Divar 700’s Web page.
2. Click Configuration > Video & Audio.
3. Click the numbered tab corresponding to the Divar Video In connector an analog camera is connected to.
4. In the General tab, select the Enable video input option.
5. To enable PTZ on the camera, click the Control tab, and select the Enable PTZ option.
6. Select a Protocol from the drop-down list.
7. Select a Device address.
   **NOTE** Make the address the same as the Divar camera input.
8. Repeat Step 3 to Step 7 for each analog camera connected to the Divar.
9. Click Save > Close.
10. If the analog cameras are already part of your Security Center system, restart the Divar unit in order for the cameras to become visible in Security Center.

Configure network cameras

If there are network cameras connected to the Bosch Divar 700, you must configure those units in the Divar’s Web page.

**NOTE** The maximum number of network cameras you can have is 32. If you have analog cameras, connect them to the Divar Video In connectors starting at connector 1, and use the remaining connectors for the network cameras (for example, if connectors 1-7 are analog cameras, connectors 8-32 could be network cameras).

1. Open the Bosch Divar 700’s Web page.
2. Click Configuration > Video & Audio.
3. Click the numbered tab corresponding to a Video In connector for a network camera.
4 In the General tab, select the Enable video input option.
5 Do one of the following:
   - Click the [Manual setup] button, and type the IP address, Input, Stream, and Password information of the camera.
   - Click the [Auto detect] button if the feature is available for that camera.
6 To enable PTZ on the camera, click the Control tab, and select the Enable PTZ option.
7 Select a Protocol from the drop-down list.
8 Select a Device address.
   **NOTE** The address must be unique. It is recommended to use the same number as the input the camera is connected to.
9 Repeat Step 3 to Step 8 for each network camera connected to the Divar.
10 Click Save > Close.
11 If the network cameras are already part of your Security Center system, restart the Divar unit in order for the cameras to become visible in Security Center.

**Configure recording settings**

The Bosch Divar 700 can have a maximum of six recording profiles that you can use with the enabled cameras.

**IMPORTANT** If trickling is enabled for the Bosch Divar in Security Center, the Archiver will not record locally; instead, the Archiver will transfer the video recordings from the Divar. For more information about trickling recorded video, see “Configure cameras for trickling” in the Security Center Administrator Guide.

**NOTE** There can only be one active profile at a time. The selected profile is used for every camera connected to the Divar.
1 Open the Bosch Divar 700's Web page.
2 Click Configuration > Recording.
3 Click a Profile tab.
4 Click the numbered tab corresponding to the cameras connected to the Divar.
5 Do one of the following:
   - To record continuously or on a schedule, click the Normal tab.
     **NOTE** The Normal tab determines the Divar recording settings when that profile is active. The resolution and frame rate settings cannot be configured in the Normal tab; they will be overridden by the recording settings configured in Security Center.
     i Select a Normal recording mode (Continuous rec. or Events only).
     ii From the Quality drop-down list, select a recording quality value.
        This setting will affect the quality and bandwidth of the video streams coming from the Divar to Security Center.
To record on contact, click the Contact tab.

**NOTE** If recording on Contact is selected, the recording settings configured on the Divar will override the Security Center settings.

iii Select a Contact recording mode (Follows, Follows + post, or Fixed duration).

iv Select the Duration, Resolution, Quality, and Frame rate for the recording stream.

To record on motion, click the Motion tab.

**NOTE** If recording on Motion is selected, the recording settings configured on the Divar will override the Security Center settings.

v Set the Motion recording mode to Fixed duration.

vi Select the Duration, Resolution, Quality, and Frame rate for the recording stream.

6 Repeat Step 3 to Step 5 for each recording profile you want to create, and for each unit using that profile.

7 To set when each recording profile is active, click Configuration > Schedule > Schedule from the Divar’s home page.

8 Select a profile, and set the date and time that profile should record.

**NOTE** These schedules are independent of Security Center schedules.

9 Click Save > Close.

### Configuring Bosch VRM units

Best practice: For optimal performance, it is best practice to set the playback mode for Bosch VRM (Video Recording Manager) units to use *iSCSI connection*, which is a storage unit for network drives.

To use the *iSCSI connection* playback mode, make sure that all Archiver servers and cameras recording on the iSCSI have full read access to all iSCSI storage units managed by the Bosch VRM. For more information, please refer to the storage vendor’s documentation.
Enable audio recording

To play back and export Bosch VRM video recordings with both audio and video, you must enable audio recording on the unit using the Bosch VRM Configurator.

Before you begin: Make sure that the audio source is connected to the LineIn connector on the video unit.

1. Open the Bosch VRM Configurator.
2. Click System > Devices.
3. From the Devices list, select the unit to configure.
4. Click the Recording > Recording Profiles > Day tabs.

   **NOTE** If you want the unit to record audio at a different time, select a different day/time tab to configure.

5. Next to the Recording includes field, select the Audio option.
6. Apply your changes.

If the unit is already part of your Security Center system and is currently recording, restart the unit.
Configure the Bosch Intuikey CCTV keyboard

The top four buttons on Bosch Intuikey CCTV keyboards can control the Play, Pause, Next, and Previous commands of a camera sequence in the Security Desk. The default button association is the following:

<table>
<thead>
<tr>
<th>Button on Bosch keyboard</th>
<th>Command in Live Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pause</td>
<td>Pause</td>
</tr>
<tr>
<td>Play</td>
<td>Play/Resume</td>
</tr>
<tr>
<td>FF</td>
<td>Show next camera in the sequence</td>
</tr>
<tr>
<td>REW</td>
<td>Show previous camera in the sequence</td>
</tr>
</tbody>
</table>

You must configure the Bosch Intuikey CCTV keyboard before using it in the Security Desk.

Before you begin: Make sure that the RS-232 port of the Bosch Intuikey CCTV keyboard is connected to the COM port of the computer.

1 In the Security Desk, click the Home button, and click Options > Peripherals > Keyboard tab.
2  From the Keyboard protocol drop-down list, select Bosh Intuikey.
3  From the Communication port drop-down list, select the COM port you just connected the keyboard to.
4  From the Data bits drop-down list, select 8.
5  From the Parity drop-down list, select None.
6  From the Stop bits drop-down list, select One.
7  From the Baud rate drop-down list, select 19200.
8  Click the Connect button.
9  Click Save.
10 The keyboard is ready to use. For more information about camera sequences, see “Viewing a camera sequence” in the Security Desk User Guide.
In order to receive hardware motion detection events in Security Center, certain Bosch PTZ dome units such as the Autodome 800 HD, need to have a VCA profile configured on the unit's Web page.

1. Open the unit's Web page.
2. Click Settings at the top of the window.
3. Click Advanced Mode > Alarm > VCA.
4. From the VCA configuration drop-down menu select a profile.
5. From the Preset drop-down menu select a preset.
6. Click Set.
7. If your unit was already part of the Security Center system, restart the Archiver for your changes to take effect.
Configuring the VJT XTCXF transcoder

Up to four cameras can be added to the transcoder for use in Security Center, this must be done using the unit’s Web page.

1. Open the unit’s Web page.
2. At the top of the page click Settings.
3. From the menu on the left side, select Transcoder > Transcoder Setup. Wait for the transcoder to scan the network for compatible devices.
4. You can add up to four cameras. Enter the password for each camera if applicable. The Device number will represent the camera in Security Center.

5. Click Set.

Please note the following:

- Make sure that there is no browser connected to the Playback Webpage of the transcoder.
- Make sure the transcoder is connected to a single Archiver.
- A maximum of two streams can be requested in Security Center. Requesting more than two streams will result in a Waiting for signal error and no video will be received.
  A stream counts as being requested if it is being recorded, if it is being viewed live, or if software motion detection is being performed. Any combination of these conditions on a single stream counts as one request.
- Make sure that the archiving schedule of the encoder in Security Center is set to 'Disabled' if you are not recording the stream.
- The maximum input resolution is 1080p.
This section describes the additional configuration steps required for some Canon units and features to work in Security Center.

This section includes the following topics:

- "Configuring Canon VB-C60 and VB-C500D units" on page 41
- "Configuring Canon VB-H41 for unit motion detection" on page 42

### Configuring Canon VB-C60 and VB-C500D units

This section describes the additional configuration steps required for Canon VB-C60 and VB-C500D units to work in Security Center.

This section includes the following topics:

- "Grant user access" on page 41
- "Enable MJPEG streaming" on page 41
- "Enable PTZ control for VB-C60 units" on page 42

#### Grant user access

To control Canon VB-C60 and VB-C500D units in Security Center, you must grant the Security Center user access to the unit using the unit's Web page.

1. Open the Unit's Web page.
2. Click Access Control > Maintenance.
3. In the User Authority section, select the Privileged Camera Control, Camera Control, and Image Distribution options for the Authorized User.
4. Click Apply.

#### Enable MJPEG streaming

To stream MJPEG video in Security Center with Canon VB-C60 and VB-C500D units, you need to configure the stream settings from the unit's Web page.

1. Open the unit's Web page.
2. Click Video > Maintenance.
3. In the MJPEG section, configure the Video Quality, Video Size (resolution), and Capture Frame Rate settings.
   **IMPORTANT** If you change the Video Size setting, you must restart the MJPEG video stream.
4. Click Apply.
Enable PTZ control for VB-C60 units

**IMPORTANT** To use PTZ presets with Canon VB-C60 units in Security Center, you must create PTZ presets for the unit using the Preset Setting Tool (one of the Canon VB Administration tools) before adding the unit to Security Center. For more information about creating PTZ presets for Canon units, see the Canon manufacturer documentation.

Configuring Canon VB-H41 for unit motion detection

In order to perform unit motion detection with a Canon VB-H41 in Security Center, the motion detection needs to be set up on the unit’s Web page. To have access to the unit’s Web page the Canon *Admin Tools Certificate* needs to be installed. The certificate can be installed from the Setup CD-ROM included with the camera. For more information about installing it, and setting up unit motion detection, please see the Canon VB-H41 documentation.
Before adding Cisco 2500 series units in your Security Center system, the stream type and video settings must be configured in the unit’s Web page.

1. Open the unit’s Web page.
2. Enter the unit username and password.
3. Click Setup > Audio/Video > Video.

4. From the Streaming Mode Combination drop-down list, select the desired stream type.
5. Make any other changes to the video settings for the stream type you selected.
6. Click Save.
This section describes the additional configuration steps required for some Comtex units to work in Security Center.

**Configure WB-H811 units**

Complete the following configuration steps before adding the unit to the Config Tool:

1. Open the unit’s Web page.
2. Click Video Settings.
3. Under Streaming 1 Settings:
   - Set the Video Format to H.264.
   - Set the RTSP Path to v1h264 (this field is case sensitive).
4. Click Apply.

**Configure PTZ for WB-H811 units**

If you want to use PTZ with the Comtex WB-811 unit, the PTZ protocol, Camera ID, and Baud rate must be set using the unit’s Web page.
For Dynacolor NH061 and NH221 units to be able to stream MPEG-4, you need to configure the video streaming format in the unit’s Web page.

1. Open the unit’s Web page.
2. Click Streaming > Video Format.
3. From the Video Format drop-down list, select MJPEG + MPEG-4.
4. Click Save.
This section describes the additional configuration steps required for some Epiphan units to work in Security Center.

**Configure VGA Broadcaster Lite units**

The following stream configuration steps are required for Epiphan VGA Broadcaster Lite units to work in Security Center.

1. Open the unit’s Web page.
2. Click Configuration > Stream Setup.
3. From the Stream type drop-down list, select RTSP (H.264 codec).
4. Under RTP/UDP stream, deselect the Enable RTP/UDP stream option.
5. To prevent tearing during playback, select the Enhanced compatibility mode option under RTP/UDP stream.
6 Configure any other video settings as necessary.
7 For motion detection to work properly, set a high Bitrate value according to the resolution and frame rate you selected.
8 Click Apply.
This section describes the additional configuration steps required to be able to view and dewarp images in Security Center that were captured using an ImmerVision Panomorph lens. Dewarping allows you to zoom in on a Panomorph image, similar to the digital zoom feature in Security Desk. The zoomed image is dewarped, or flattened to show a rectangular image.

This section includes the following topics:
- "Configuring ImmerVision Panomorph camera lenses" on page 48
- "Use the dewarping feature" on page 50

### Configuring ImmerVision Panomorph camera lenses

Before viewing video with an ImmerVision camera lens in Security Desk, you must configure the lens in Config Tool.

1. From the Video task in Config Tool, select the camera to configure.
2. Click the Hardware tab.
3. From the Lens type drop-down list, select Panomorph.
4. Click the Edit button.

![Config Tool Hardware Tab](image)
In the Calibrate lens dialog box, do the following:

a. Select the Camera position.
b. Select the Panomorph Lens Type (RPL). The lens type is listed on the lens box.
c. Set the Dewarped resolution values. The resolution values must be a multiple of 4 and preferably at a 4:3 ratio. For example, 320x240 or 640x480.
   **NOTE** The resolution set here is the output resolution for the lens viewer. The actual camera feed resolution is set in the Video tab.
d. Click Calibrate. A message will display telling you if the lens was calibrated successfully.
   The calibration may fail for the following reasons:
   * it is too dark.
   **TIP** Calibrate your lens when it is bright. This ensures that the calibration will succeed and dewarping will work even when it is dark.
   * the lens is not installed or positioned correctly.
   * there is no lens or the lens type is wrong.
   **NOTE** If the camera is moved the lens should be Calibrated again.
e. Click Ok.

6. In the Hardware tab, click Apply.
   **NOTE** For settings to take effect after making changes in the Configure lens dialog box, the camera needs to be removed from all Security Desk tiles and Monitoring tasks and re-added.
Use the dewarping feature

The dewarping process is done in Security Desk. When you zoom into a ImmerVision pano-morph camera lens image in the Security Desk Monitoring task, it is dewarped and shown as a rectangular image.

1. From the Monitoring task in Security Desk, drag the ImmerVision camera that uses the panomorph lens in a tile.
2. To zoom in the image, use your mouse wheel, or draw a box on the region you want to zoom to.

**NOTE** If you zoom using your mouse wheel, it zooms to the center of the image, not where your cursor is pointing.
3 To navigate the zoomed image, click the image thumbnail at the top-left of the tile.

4 To zoom out, use the mouse wheel, or the zoom slider on the right-side of the tile.
This section describes the additional configuration steps required for some Interlogix units to work in Security Center.

This section includes the following topics:

- "Configure Discovery 105-E (UVE-101) units" on page 52
- "Configuring VisioWave units" on page 53

**Configure Discovery 105-E (UVE-101) units**

The following configuration must be performed before adding Discovery 105-E (UVE-101) units in Security Center.

1. Open the unit's Web page.
2. Click Administration.
3. Enter your username and password.
4. Click Video port format.
5. Set the Video port format to NTSC M or PAL depending on the camera connected to the encoder.
6. Click OK to save your changes.
Enable software motion detection

To enable software motion detection for Interlogix Discovery 105-E (UVE-101) units in Security Center, additional configuration is required in Config Tool.

1. In the Motion detection tab of the camera entity, click the Advanced settings button.
2. From the Preset drop-down list in the H.264 Advanced motion detection settings dialog box, select Custom.
3. Under Custom, set the following values:
   - Luma weight: 5
   - Chroma weight: 0
   - Vectors weight: 0
   - Macroblocks weight: 100
4. Click OK, and click Apply.

For more information about advanced motion detection settings, see “Advanced H.264 Motion Detection” the Security Center Administrator Guide.

Configuring VisioWave units

The Interlogix VisioWave driver can control multiple Interlogix units and PTZ motors. You must add and configure Interlogix VisioWave units using the Central Configuration Server application.

Before you begin: Make sure the Interlogix Central Configuration Server is installed.

Best practice: Perform these configuration steps before adding the unit to the Archiver.

- Add VisioWave units
- Configure video ports
- Enable PTZ

Add VisioWave units

1. Open the Central Configuration Server in Internet Explorer.
2. Click Equipment > New Video Equipment.
3. Enter the following information:
   a. In the Equipment name field, type a name for the unit.
   b. In the IP Address field, type the IP address of the unit.
   c. From the Product Hardware Range drop-down list, select the unit type (for example, EVOLUTION HD, or DISCOVERY 300).

   **NOTE** The number of inputs available depends on the unit type.
4. Click Next until the Serial Ports page.
5. Enter the following information:
Configure video ports

1. Open the *Central Configuration Server* in Internet Explorer.
2. Click Equipment.
3. In the Equipment list, select the unit to configure.
4. Click Video Inputs.
5. Click the input name you want to use.
6. Under ENABLE UDP in the Network section, clear the ALLOW IP FRAGMENTATION option.
7. Select the Input format you want to use, and click OK.
8. Click Apply in the upper-right corner of the *Central Configuration Server* window.
   When your changes are applied, a confirmation appears in the window.
9. Click OK.

Enable PTZ

To enable PTZ for VisioWave units, you must create a new PTZ camera for the unit's serial port in the Central Configuration Server.

1. Open the *Central Configuration Server* in Internet Explorer.
2. Click Equipment.
3. In the List of Video Equipment, select the unit to configure.
4. Click Serial Ports.
5. Select the serial port you created in "Add VisioWave units" on page 53, and configure it the same as the serial configuration of the camera.
6. Click OK.
7. Click Apply in the top-right corner of the *Central Configuration Server* window.
   When your changes are applied, a confirmation appears in the window.
8. Click OK.
9 In the *Central Configuration Server* main page, click Equipment.

![Central Configuration Server](image)

10 In the List of Video Equipment, select the unit to configure.

11 Click Serial Ports.

12 In the List of Serial Ports for Video Equipment, select the serial port you created in "Add VisioWave units" on page 53.

13 Click PTZ Cameras > New PTZ camera.

14 In the New PTZ Camera for Serial Port x page, do the following:
   - In the CAMERA NAME field, type a name for the PTZ camera
   - In the ADDRESS NUMBER field, type the number on the PTZ camera.
   - From the PTZ PROTOCOL drop-down list, select the PTZ protocol.
   - In the TCP PORT field, type the port number of the input you want to control.
     The port number must be 80XX, where XX is the input number.

15 Click OK.

16 Click Apply in the upper-right corner of the *Central Configuration Server* window.

   When your changes are applied, a confirmation appears in the window.

17 Click OK.

After you are done: If the VisioWave unit is already part of your Security Center system and you want to apply the changes you made in the *Central Configuration Server* (for example, if you added a PTZ camera to the unit), restart the unit.
This section describes the additional configuration steps required for some IQinVision unit features to work in Security Center.

This section includes the following topics:

- "Configuring virtual zones" on page 56
- "Using H.264 multicast streaming" on page 56

Configuring virtual zones

Virtual zones for IQinVision cameras must be created using the unit’s Web page. When you create or edit a zone, the video stream must be restarted by changing the stream quality, or restarting the unit.

Using H.264 multicast streaming

For the multicast address assigned by the Directory to become effective, allowing you to view multicast video with IQinVision cameras in H.264, you must restart the unit after adding it in Config Tool.
This section describes the additional configuration steps required for some Mango DSP unit features to work in Security Center.

This section includes the following topics:

- "Configure input pin wiring" on page 58
- "Configure input pin events on the standby Archiver" on page 58
- "Change the default port for input pin events" on page 58
Configure input pin wiring

Input pins on Mango units work with a logical circuit value of 0/1. Security Center closing and opening events are mapped as follows:

- To trigger an input pin closing event, the voltage on the pins should be dropped from 5 volts to 0 volts.
  - On Pegasus M units, the default value is 1. To change it to 0, short the pins.
- To trigger an input pin opening event, the voltage on the pins should be raised from 0 volts to 5 volts.
  - On Condor VS-8 and VS-16 units, the default value is 0. To change it to 1, apply 5 volts on the pins.

**NOTE** The voltage mentioned is approximate, for the exact voltage range; please see the documentation for your Mango DSP unit.

Configure input pin events on the standby Archiver

In order for input pin events to be received properly with two Archiver roles, the second Archiver role requires a specific configuration:

1. On the second Archiver role machine, navigate to the installation directory, located in `C:\Program Files\Common Files\DVR Software 5.2\Extensions\Drivers\` on 32-bit machines, and `C:\Program Files (x86)\Common Files\DVR Software 5.2\Extensions\Drivers\` on 64-bit machines.
2. Open the `Generic01DriverConfiguration.xml` file in Notepad.
   
   Text similar to the following is displayed:
   
   ```xml
   <MangoDspDriverConfiguration>
   <HttpServerNumber>1</HttpServerNumber>
   </MangoDspDriverConfiguration>
   ```
3. Change the value of the `HttpServerNumber` from 1 to 2.
4. Save the file, and restart the Archiver role.

Change the default port for input pin events

In order to receive input pin events from Mango units, the Archiver role needs to open a TCP port for its HTTP server. The default port is 8008. If this port is already in use on the Archiver role machine, you can change the default port.

To change the default port:

1. On the Archiver role machine, navigate to the installation directory, located in `C:\Program Files\Common Files\DVR Software 5.2\Extensions\Drivers\` on 32-bit machines, and `C:\Program Files (x86)\Common Files\DVR Software 5.2\Extensions\Drivers\` on 64-bit machines.
2 Open the *EventHttpServerConfiguration.xml* file in Notepad.

Text similar to the following is displayed:

```xml
<EventHttpServerConfiguration>
  <HttpServerPort>8008</HttpServerPort>
</EventHttpServerConfiguration>
```

3 Change the value of the `HttpServerPort` from 8008 to something else, such as 8009.

   **NOTE** The value for the `HttpServerPort` must be the same for all standby Archivers associated with the unit.

4 Save the file, and restart the Archiver role.
This section describes the additional configuration steps required for some Mavix units to work in Security Center.

This section includes the following topics:

- "Configuring MediaRacer units" on page 60
- "Configure MediaRacer 152 units" on page 63
- "Configure MediaRacer 250 units" on page 64

**Configuring MediaRacer units**

You must add and configure Mavix MediaRacer units using the Mavix Configurator before they can be used in Security Center.

**Add Mavix MediaRacer units**

1. Open the Mavix Configurator and enter Administrator as the default username and Admin as the password.
2. Click the Units icon.
3. In the Units dialog box, click Add.
4. In the Add Unit dialog box, type a name for the unit.
5. In the IP field, type the unit IP address.
6. From the Type drop-down list, select the unit model (for example, MediaRacer-250/C).
7. Click Ok.
8. In the Mavix Configurator window, click the Sites icon.
9. In the Site Configuration dialog box, click Add.
10. In the Add New Site dialog box, type a name for the site in the Site Name field, and click Ok.
    
    The new site is added to the Sites list in the Site Configuration dialog box.
11. From the Sites list in the Site Configuration dialog box, select the new site.
12. From the Units/Recorders/Players list, select the newly added MediaRacer unit, and click the > button to move the unit into the site.
Configure PTZ controls

For MediaRacer 152 and 250 units to support PTZ, the units must be configured in the Mavix Configurator, and the serial port must be associated manually with the camera when the unit is added in Security Center.

1. Open the Mavix Configurator and enter Administrator as the default username and Admin as the password.
2. Click the Configure icon.
3. In List A, select the MediaRacer unit to configure.
4. Click the RS232/RS485 tab.
5. From the Port drop-down list under Unit A, select the COM port used with the PTZ camera.
6. Under Settings, configure any other serial port settings required for the camera.
7. Click Apply.
8. Do one of the following:
   - If the unit is already part of your Security Center system, select the unit in the entity tree.
   - If the unit is not part of your Security Center system, add the unit using the specified serial port, and select the unit in the entity tree. For more information about adding video units, see "Adding Video Units" in the Security Center Administrator Guide.
9. In the Physical view of the Config Tool, click PTZ, and click PTZ.
10. In the Create PTZ dialog box, select the MediaRacer camera.
11. Select the Serial port(s) on the same unit option, and select the serial port specified in Step 5.
12. From the Protocol drop-down list, select the protocol for the camera.
13. Click OK.
Change the IP address

1. Open the Mavix Configurator and enter Administrator as the default username and Admin as the password.
2. Click the Update Firmware icon.
3. In the Unit Auto Update tab, type the current IP address of the unit.
4. Type the username and password for the unit.
5. Under MediaRacer, select 250.
6. In the Change IP settings section, click Read. The current unit IP address is displayed in the IP field.
7. Select the Change IP Settings option.
8. In the IP field, type the new IP address.
9. Type the Mask and Gateway information.
10. Click Update.
Configure MediaRacer 152 units

For Mavix MediaRacer 152 units to stream MPEG-4 video properly in Security Center, you must ensure that the unit firmware version matches the MPEG-4 version.

1. Open the Mavix Configurator and enter Administrator as the default username and Admin as the password.
2. Click the Update Firmware icon, and click Manual Update.
3. Enter the IP address, username, and password of the unit.
4. Under MediaRacer, select IXX.
5. In the Unit firmware version section, click Read.
6. Ensure that the Firmware version is at least 7.1.1.0, followed by the letter “r” (eg. 7.1.1.0r).
7. Ensure that the Codec is Mpeg4, and that the version matches the firmware version listed above it.
Configure MediaRacer 250 units

Mavix MediaRacer 250 units have a unique video input that provides two streams which can be configured independently using the Mavix Configurator.

- "Select H.264 or MPEG-4 streaming" on page 64
- "Configure the stream settings" on page 65

Select H.264 or MPEG-4 streaming

1. Open the Mavix Configurator and enter Administrator as the default username and Admin as the password.
2. Select the Update Firmware icon.
3. Under Connect to in the Manual Update tab, type the unit IP address.
4. Type the username and password of the unit.
5. Under MediaRacer, select 250.
6. From the drop-down list in the dialog box, select taskman.ini.
7  Click Get > Edit.
   The file opens in Notepad.
8  In the Video section, change the Coding= value to:
   - Coding=8 if you want to stream H.264.
   - Coding=5 if you want to stream MPEG-4.
9  Save the file, and click Put in the Manual Update tab.

**Configure the stream settings**

1  Open the Mavix Configurator and enter Administrator as the default username and Admin as the password.
2  Click the Configure icon.
3  In List A, select the MediaRacer 250 unit to configure.
4  Click the Video tab.
5  Click the Stream 1 tab, and configure the video stream settings as required.
6  Click the Stream 2 tab, and configure the video stream settings as required.
7  Click the OSD tab, and configure the On Screen Display text settings as required.
8  Click Apply.
This section describes the additional configuration steps required to use the fish-eye dewarping feature of Oncam Grandeye 360° cameras in Security Center. Dewarping allows you to zoom in on a 360° image, similar to the digital zoom feature in Security Desk. The zoomed image is dewarped, or flattened to show a rectangular image.

This section includes the following topics:

- "Configure Oncam Grandeye 360° fish-eye camera lenses" on page 66
- "Use the dewarping feature" on page 68
- "Configure digital zoom presets" on page 69

**Configure Oncam Grandeye 360° fish-eye camera lenses**

Before viewing video with an Oncam Grandeye 360° fish-eye camera lens in Security Desk, you must configure the lens in Config Tool.

1. From the Video task in Config Tool, select the camera to configure.
2. Click the Hardware tab.
3. From the Lens type drop-down list, select Oncam Grandeye.

4. Click the Edit (📝) button.
5 In the Configure lens dialog box, do the following:

- Using the Width and Height fields to set the Maximum Dewarped resolution values.
- Select the Quality.
- Select the Camera position.
- To set the center position of the fish-eye, drag the left mouse button.
- To adjust the radius of the fish-eye, drag the right mouse button.

**NOTE** The blue region represents the area that can be dewarped in a Security Desk tile.

- Click Ok.

6 In the Hardware tab, click Apply.

**NOTE** For settings to take effect after making changes in the Configure lens dialog box, the camera needs to be removed from all Security Desk tiles and Monitoring tasks and re-added.
Use the dewarping feature

The dewarping process is done in Security Desk. When you zoom into a Oncam Grandeye 360° fish-eye camera lens image in the Security Desk Monitoring task, it is dewarped and shown as a rectangular image. The dewarping time varies, depending on your computer and the dewarped resolution. For example, the dewarping time will be four times longer using a 640x480 resolution instead of a 320x240 resolution.

1. From the Monitoring task in Security Desk, drag the Oncam Grandeye 360° camera in a tile.
2. To zoom in the image, use your mouse wheel, or draw a box on the region you want to zoom to.

**NOTE** If you zoom using your mouse wheel, it zooms to the center of the image, not where your cursor is pointing.

3. To navigate the zoomed image, click the image thumbnail at the top-left of the tile.

4. To zoom out, use the mouse wheel, or the zoom slider on the right-side of the tile.
Configure digital zoom presets

You can create digital zoom presets for Oncam Grandeye 360° cameras and other non-ptz cameras, similar to PTZ presets in Security Desk.

NOTES

• Digital zoom presets are not supported on PTZ cameras.
• You can create as many presets as you want.

To create a digital zoom preset:

1. From the Monitoring task in Security Desk, drag the Oncam Grandeye 360° camera in a tile.
2. Zoom to the position you want to create a preset for.
3. In the camera widget, click Add.

The digital zoom preset uses the camera's current zoom position.

4. Type a name for the preset.
5. Click Create.

You can now zoom to the preset by selecting it from the Digital zoom presets drop-down list.

From the Preset ( ) button next to the Digital zoom presets drop-down list, you can also perform the following tasks:

• Reload. Return to the preset if you've moved out of the preset region.
• Save. Re-save the preset as the current zoom position.
• Rename. Rename the current preset.
• Remove. Delete the current preset.
• Create. Click to create another preset.
This section describes the additional configuration steps required for some OTN units to work in Security Center.

### Configuring MVIDIPv4 units

Due to specific OTN MVIDIPv4 unit behavior, proper reception and decoding of the MPEG-4 video stream requires extra configuration to work in Security Center.

#### Disable IGMPv3 support

Because MVIDIPv4 units use a different IP address than the control channel, video streams are filtered out of potential multicast sources by the IGMPv3 protocol. For proper reception of MVIDIPv4 video streams, you must disable the IGMPv3 advanced setting on the Directory and Archiver Server machines. If you are streaming video in multicast, the advanced setting must also be disabled on your workstation.

1. From the Video task in Config Tool, select the Archiver to configure.
2. Click the Resources tab.
3. At the bottom of the Resources tab, click the Advanced settings button.
4. In the Advanced settings dialog box, click the Additional settings button.
5. In the Additional settings dialog box, click .
6. In the Name column, type IGMPv3Enabled.
7. In the Value column, type 0.
8. Click Close.
9. In the Advanced settings dialog box, click OK.
10 In the Resources tab, click Apply.
   You are asked to restart the Archiver. Click Yes.

**Enable MPEG-4 start code lookup offset**

MVIDIPv4 units sometimes develop offset start codes in the MPEG-4 video stream. As a solution, the MPEG-4 start code lookup value must be increased so that the video stream will be found in Security Center. This advanced setting must be modified on the Client and Server machines for proper archiving and video decoding.

1 From the Video task in Config Tool, select the Archiver to configure.
2 Click the Resources tab.
3 At the bottom of the Resources tab, click the Advanced settings button.
4 In the Advanced settings dialog box, click the Additional settings button.
5 In the Additional settings dialog box, click +.

6 In the Name column, type IGMPv3Enabled.
7 In the Value column, type 0.
8 Click Close.
9 In the Advanced settings dialog box, click OK.
10 In the Resources tab, click Apply.
   You are asked to restart the Archiver. Click Yes.
This section describes the additional configuration steps required for some Panasonic units and unit features to work in Security Center.

- "Configuring H.264 software motion detection" on page 72
- "Configuring multi-streaming in MJPEG" on page 72
- "Configuring I/O pins" on page 73
- "Configure capture resolutions" on page 74
- "Configuring edge analytics for WJ-NT314 units" on page 74
- "Configure WJ-GXE500 (DG-GXE500) units" on page 75
- "Use auto-pan with Panasonic units" on page 75
- "Configuring the Panasonic WV-CU950 Ethernet keyboard" on page 76
- "Configuring Variable Image Quality on Specified area (VIQS)" on page 78
- "Configuring Auto tracking" on page 79

**Configuring H.264 software motion detection**

Software motion detection is based on metadata sent from the camera which is affected by the Sensitivity setting on the unit’s Web page. For best results, increase the Sensitivity value on the unit’s Web page before you configure software motion detection in H.264.

**Configuring multi-streaming in MJPEG**

Multi-streaming in MJPEG is supported on certain Panasonic cameras in Security Center. In the Video tab of Panasonic camera entities in Config Tool, the Quality setting must be the same for both video streams, and can only be configured from stream 1.
Configuring I/O pins

Panasonic units DG-NS202, WV-NS954, WV-NW964, WV-NP502, WV-508, and WV-NW502S do not have a hardwired pin configuration. The input and output pins cannot be configured for these units through their Web page, because Security Center will enforce the following configuration:

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Panasonic description</th>
<th>Security Center pin configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alarm In</td>
<td>IN</td>
</tr>
<tr>
<td>2</td>
<td>Alarm In/Alarm Out</td>
<td>OUT</td>
</tr>
<tr>
<td>3</td>
<td>Alarm In/Auxiliary Out</td>
<td>IN</td>
</tr>
<tr>
<td>4</td>
<td>Ground</td>
<td>Ground</td>
</tr>
</tbody>
</table>

NOTE Panasonic pin types other than input/output, such as auxiliary pins, are not supported in Security Center.
Configure capture resolutions

For Panasonic megapixel cameras (for example, 1.3 megapixels or 3.0 megapixels) to stream at the correct resolution, you must configure the image capture mode on the unit’s Web page before adding the unit in Security Center.

1. Open the unit’s Web page.
2. Click Setup > Image.
3. From the Image capture mode drop-down list, select the desired resolution.
   
   **NOTE** On some models you may have to select an Aspect ratio instead of an Image capture mode

4. Click Set.

Configuring edge analytics for WJ-NT314 units

To use edge analytics with Panasonic WJ-NT314 encoders, it must be configured for each active channel using the unit’s Web page.
Configure WJ-GXE500 (DG-GXE500) units

To view multicast video with Panasonic WJ-GXE500 (DG-GXE500) cameras in H.264 or MPEG-4, you must configure the following settings in Config Tool.

**NOTE** With Panasonic DG-GXE500 cameras, you can stream a maximum of three channels simultaneously.

1. From the Logical View in Config Tool, select the camera to configure.
2. Click the Video tab.
3. From the Priority drop-down list, select **Constant**.
4. Set the Bit rate slider value in between **64-2048**.
5. Click **Apply**.

Use auto-pan with Panasonic units

The auto-pan feature is supported with some Panasonic units in Security Center. It must be configured in the Specific commands dialog box.

1. In Security Desk, select the PTZ camera in the canvas tile.
2. Using the PTZ-in-tile feature, move the camera to the desired position.
3. Click the **Specific Commands** button.
4. From the Specific commands dialog box, click **Set auto pan start point**, and click **Execute command**.

This sets the auto pan start point to the current camera position.

5. Click **Close**.
6 To select an auto pan stop point, move the camera to the desired stopping point, and click Specific Commands (③) button.

7 In the Specific commands dialog box, click Set auto pan stop point, and click Execute command.
   
   **NOTE** The auto pan feature does not support tilt commands.

8 Click Start autopan, and click Execute command.
   
   The camera pans between the two points you configured.
   
   **NOTE** When the camera is panning, clicking another PTZ command cancels the autopan.
   
   The only exceptions are the Zoom commands.

9 To stop the auto pan, click Stop autopan, and click Execute command.

10 Click Close.

### Configuring the Panasonic WV-CU950 Ethernet keyboard

In order to use the Panasonic WV-CU950 Ethernet keyboard with Security Center, the keyboard must be configured, and the Panasonic Ethernet keyboard protocol must be set in the Peripherals tab of Security Desk.

#### Configuring the keyboard

Before you begin: Unplug the keyboard.

1 On the back of the controller, set Mode selection switches 1, 4, and 5 to ON.

2 On the back of the controller, set the CONTROLLER NO to 1.

3 Plug the controller into a power source.
4 Turn on the power while holding down the MON (ESC), O and CAM (SET) buttons. The LCD display will prompt you for a password.

![IP Addr Setup Mode](image)

5 Enter the administrator password. The factory default is "650".

**NOTE** To delete a character, press the clear button.

6 If the password was entered correctly, The IP Address setting will appear on the LCD display. Press the CAM (SET) button to edit the default. Enter a unique IP address for the controller.

**NOTE** Use the Shuttle Ring to move the cursor.

![IP Address](image)

7 Rotate the JogDial to until Subnet Mask appears on the LCD display, then press the CAM (SET) button to edit the default setting. Enter a Subnet Mask.

![Subnet Mask](image)

8 Use the JogDial and the CAM (SET) button to edit of the following items:

- **Gateway**: Enter a Gateway address.
- **Keyboard ID**: Leave this at the default setting (1).
- **Server IP Address**: IP Address where Security Center is running.
- **Server ID**: Leave this at the default setting (1).

9 Press the MON (ESC) button to complete the setup.

**Security Center configuration**

The Keyboard protocol and IP address needs to be set in Config Tool for the WV-CU950 controller to work in Security Center.

1 From the Config Tool Home page, select Options > Peripherals, then click the Keyboard tab.

2 From the Keyboard protocol drop-down menu, select Panasonic Ethernet.
3 Select the Connect to keyboard automatically option.
4 Under Ethernet Port enter the keyboard’s IPv4 address that was configured in Step 6.
5 Click Save.

Configuring Variable Image Quality on Specified area (VIQS)

The VIQS feature is supported with some Panasonic units in Security Center. It must be configured in the Hardware tab of the camera.

1 From the Logical View in Config Tool, select the camera to configure.
2 Click the Hardware tab.
3 Set H.264 VIQS to ON.
4 Next to the H.264 VIQS setting, click VIQS window.

5 To re-size the camera view area, do one of the following:
   a In the Size and position section, enter the X, Y, W, and H coordinates.
      X is the Top-left pixel, Y is the Bottom-left pixel, W is the Top-right pixel, and H is the bottom-right pixel.
6 Drag the green area to the size you want.
7 Click OK. 
Select ON beside Stream 1 and/or Stream 2 to apply the new VIQS area.

**Configuring Auto tracking**

You can configure the Auto tracking settings in the Properties tab of Panasonic unit entities in Config Tool.

1 In the Video task of the Config Tool, select the unit to configure.
2 Click the Properties tab.
3 Expand the Auto tracking menu.
4 Configure the following:
   - Camera height. Specify the height of the camera in meters. For more information on how to measure this value correctly, see your Panasonic documentation.
   - Self return. Turn this option ON to have the unit resume auto tracking after it loses the tracking target, or a manual PTZ action is performed.
   - Self return timer. Specifies how long (in seconds) the camera will take to resume auto tracking when Self return is ON.
   - Seek to preset. Specifies a preset that the unit will seek to before resuming auto tracking when Self return is ON.
This section describes the additional configuration steps required for some Pelco units to work in Security Center.

This section includes the following topics:

- "Configuring motion detection" on page 81
- "Adding NET54xx encoder series" on page 81
- "Configuring dual-streaming for Pelco IP series" on page 81
- "Configuring NET5301T units" on page 81
- "Configuring Pelco Sarix units" on page 82
- "Naming Sarix Spectra HD PTZ preset tours" on page 82

Configuring motion detection

Best practice: When using H.264 motion detection with Pelco units, it is recommended that you disable all automatic image adjustments on the unit’s Web page.

Adding NET54xx encoder series

The NET54xx encoder series can have a range of one to four channels. Each channel must have a different IP address. Therefore, units like the NET5402T which have two channels, must be added twice in Security Center, once for each IP address.

Configuring dual-streaming for Pelco IP series

When using dual-streaming with Pelco IP series units, the video stream settings for each stream are linked. For example, the video settings you define for the primary stream tab (MPEG-4-1) are automatically applied in the secondary stream tab (MPEG-4-2).

Configuring NET5301T units

To use PTZ on Pelco NET5301 units in Security Center, you must enable PTZ and configure the serial port in the camera Hardware tab in Config Tool.
Configuring Pelco Sarix units

Note the following when using Pelco Sarix units in Security Center:

- The video quality settings of the secondary stream are dependent on the primary stream. The video settings of the second stream cannot be changed without first setting the primary stream video settings to the desired values.
- Motion detection settings depend on the resolution of the primary stream. If the resolution is changed, the Archiver will re-send the motion detection settings to the unit.
- Configuring the Quality setting in the camera's Video tab may have no effect on the unit.
- The greyed-out fields in the camera's Video tab (frame rate and resolution) may not display the values configured on the unit.
- The maximum frame rate available changes depending on the bit rate and the resolution set in the Video tab.

Naming Sarix Spectra HD PTZ preset tours

PTZ preset tours must be named “Endura X” using the unit’s Web page where X represents the pattern number in Security Center. For example, a tour named “Endura 1” in the unit’s Web page is available as Pattern 1 in the Security Desk Patterns menu.
This section describes the additional configuration steps required for some Samsung units to work in Security Center.

This section includes the following topics:

- "Configure SNP-3750 units" on page 83
- "Configure Samsung ONVIF units to stream at the proper framerate" on page 84
- "Creating video profiles" on page 85

### Configure SNP-3750 units

To configure the video stream resolution for SNP-3750 units using either MPEG-4 or MJPEG streaming:

1. Open the unit’s Web page.
2. Click Video Setup > Streaming.
3. Choose the desired resolution from the Unicast Image Resolution drop-down list.
4. If using MJPEG streaming, you must also modify the video resolution on the machine that is running the Config Tool.
5. On the Config Tool machine, navigate to the SNP-3750 cam file, located in: C:\Program Files\Common Files\DVR Software 4.x\Extensions\Cam Files\Samsung SNP3750.cam on 32-bit machines, and C:\Program Files (x86)\Common Files\DVR Software 4.x\Extensions\Cam Files\Samsung SNP3750.cam on 64-bit machines.
6. Open the SNP3750.cam file in Notepad.
7. Locate the following line:
   `<MjpegURLs>public/video.cgi?ch=1&resolution=cif</MjpegURLs>`
8. Replace `cif` with the desired resolution: qncif, cif, or 4cif.
   **NOTE** Use lowercase text only.
9. If the unit is already part of your Security Center system, remove and delete the unit from Security Center, and add it using the Config Tool station where the cam file has been modified.
Configure Samsung ONVIF units to stream at the proper framerate

For Samsung ONVIF units to stream at a proper frame rate in Security Center, the Email/FTP profile feature on the video stream being used must be disabled in the unit's Web page.

1. Open the unit's Web page.
2. In the Setup menu, navigate to the Video Profile page.
3. In the Video Profile page, create a new video profile.
   For example, if you are streaming in MJPEG, create a new MJPEG profile in one of the ten empty Video Profile slots.
4. For the new video profile, select the Email/FTP profile option.
5. For all other default video profiles used in Security Center (MJPEG, MPEG-4, and H.264), deselect the Email/FTP profile option.
Creating video profiles

Before a Samsung unit can be added in Security Center, you must create video profiles for each H.264 stream available in Security Center. For example, if Security Center offers three streams and there is one H.264 stream available by default in the unit’s Web Page, you must create two more H.264 video profiles.

1. Open the unit’s Web page.
2. In the Setup menu, navigate to the Video profile page on the left.
3. Select an empty profile, provide a Name, select H.264 from the Codec list then click Apply.

4. Repeat Step 3 as needed.
   You can now add the unit to SecurityCenter.
This section describes the additional configuration steps required for some Sanyo, and Sanyo ONVIF compliant units to work in Security Center.

This section includes the following topics:
- "Configure VCC-HD5X00 units" on page 86
- "Add Sanyo ONVIF units" on page 86

**Configure VCC-HD5X00 units**

Your unit must have two video streams that are configured before adding the unit to the Config Tool.

1. Open the unit's Web page.
2. Click on VIDEO/AUDIO.
3. Under STREAM, set STREAM 1 to H.264, and STREAM 2 to JPEG.

**Add Sanyo ONVIF units**

For Sanyo ONVIF compliant units to work in Security Center, specific HTTP port settings are required when the units are added in the Config Tool.

1. From the Video tab in the Config Tool, click the Video unit button.
2. In the Manufacturer field, select Sanyo.
3. Select the Product type, and enter the appropriate IP address.
4. In the HTTP port field, enter 8080.
5. Enter the appropriate username and password.
6. Click Add.
This section describes the additional configuration steps required to use the fish-eye dewarping feature of Sentry 360 cameras in Security Center. Dewarping allows you to zoom in on a 360° image, similar to the digital zoom feature in Security Desk. The zoomed image is dewarped, or flattened to show a rectangular image. While most of the configuration steps are the same for all Sentry 360 units, the resolution and stream configuration for 1.3 and 2 megapixel units is different. If you are using a 1.3 or 2 megapixel unit, see "Configuring resolution and stream settings on a 1.3 or 2 megapixel unit" on page 87.

This section includes the following topics:

- "Configuring resolution and stream settings on a 1.3 or 2 megapixel unit" on page 87
- "Setting the resolution for a 5 or 10 megapixel unit" on page 88
- "Configure Sentry 360-degree fish-eye camera lenses" on page 89
- "Use the dewarping feature" on page 91
- "Configure digital zoom presets" on page 92

### Configuring resolution and stream settings on a 1.3 or 2 megapixel unit

The resolution and stream settings for a 1.3 or 2 megapixel unit need to be done on the unit’s Web page.

1. Open the unit’s Web page.
2. Select the Streaming tab and then click Video Format.
3. Under Video Resolution, select the desired stream from the drop-down menu and then select the desired resolution using the radio buttons.

NOTE A maximum of two streams is supported at the same time.

4. Click Save.

After you are done: If the unit was already part of your Security Center system, restart it to apply your changes.

Setting the resolution for a 5 or 10 megapixel unit

You cannot change the resolution for a 5 or 10 megapixel unit from the unit’s Web page. The resolution is set when you add the unit to Security Center.

1. From the Video task in Config Tool, select the Archiver you want to add the camera to.
2. Click Add an entity, and select Video unit.
3. In the Manual add dialog box beside Manufacturer, select Sentry360.
4. From the Product type drop-down menu select the desired resolution.

![Product type selection](image)

5. Complete the other settings, and click Add.
   For more information about how to add a unit to Security Center, see "Adding video units to your system" in the *Security Center Administrator Guide*.

**Configure Sentry 360-degree fish-eye camera lenses**

Before viewing video with a Sentry 360 fish-eye camera lens in Security Desk, you must configure the lens in Config Tool.

1. From the Video task in Config Tool, select the camera to configure.
2. Click the Hardware tab.
3. From the Lens type drop-down list, select Sentry 360.

4. Click the Edit (🔧) button.
5  In the Calibrate lens dialog box, do the following:

a  Using the Width and Height fields, set the Dewarped resolution values.

b  To set the center position of the fish-eye, drag the left mouse button.

c  To adjust the radius of the fish-eye, drag the right mouse button.

**NOTE**  The blue region represents the area that can be dewarped in a Security Desk tile.

d  Click Ok.

6  In the Hardware tab, click Apply.

**NOTE**  For settings to take effect after making changes in the Configure lens dialog box, the camera needs to be removed from all Security Desk tiles and Monitoring tasks and re-added.

### Use the dewarping feature

The dewarping process is done in Security Desk. When you zoom into a Sentry 360 fish-eye camera lens image in the Security Desk Monitoring task, it is dewarped and shown as a rectangular image.

1  From the Monitoring task in Security Desk, drag the Sentry 360 camera in a tile.
2 To zoom in the image, use your mouse wheel, or draw a box on the region you want to zoom to.

NOTE If you zoom using your mouse wheel, it zooms to the center of the image, not where your cursor is pointing.

3 To navigate the zoomed image, click the image thumbnail at the top-left of the tile.

4 To zoom out, use the mouse wheel, or the zoom slider on the right-side of the tile.

Configure digital zoom presets

You can create digital zoom presets for Sentry 360 cameras and other non-ptz cameras, similar to PTZ presets in Security Desk.

NOTES

- Digital zoom presets are not supported on PTZ cameras.
- You can create as many presets as you want.

To create a digital zoom preset:
1 From the Monitoring task in Security Desk, drag the Sentry 360 camera in a tile.
2 Zoom to the position you want to create a preset for.
3 In the camera widget, click Add.

The digital zoom preset uses the camera's current zoom position.

4 Type a name for the preset.

5 Click Create.

You can now zoom to the preset by selecting it from the Digital zoom presets drop-down list.

From the Preset (_bbox) button next to the Digital zoom presets drop-down list, you can also perform the following tasks:

- **Reload.** Return to the preset if you've moved out of the preset region.
- **Save.** Re-save the preset as the current zoom position.
- **Rename.** Rename the current preset.
- **Remove.** Delete the current preset.
- **Create.** Click to create another preset.

**Change the default port for motion events**

In order to receive motion events from Sentry units, the Archiver role needs to open a TCP port for its HTTP server. The default port is 8008. If this port is already in use on the Archiver role machine, you can change the default port.

To change the default port:

1 On the Archiver role machine, navigate to the installation directory, located in `C:\Program Files\Common Files\DVR Software 5.2\Extensions\Drivers` on 32-bit machines, and `C:\Program Files (x86)\Common Files\DVR Software 5.2\Extensions\Drivers` on 64-bit machines.

2 Open the `EventHttpServerConfiguration.xml` file in Notepad.

Text similar to the following is displayed:

```
<EventHttpServerConfiguration>
```
<HttpServerPort>8008</HttpServerPort>
</EventHttpServerConfiguration>

3 Change the value of the HttpServerPort from 8008 to something else, such as 8009.
   NOTE The value for the HttpServerPort must be the same for all standby Archivers associated
   with the unit.

4 Save the file, and restart the Archiver role.
This section describes the additional configuration steps required for some Sony unit features to work in Security Center.

- "Configure Sony 5th generation cameras" on page 95
- "Creating Sony PTZ patterns" on page 95
- "Using the Copy configuration tool" on page 99
- "Configure Sony edge recording and video trickling" on page 100
- "Maintaining 4:3 aspect ratio for the SNC-ZP550" on page 101.
- "Configuring 6th generation units to stream at 60 frames per second" on page 103

### Configure Sony 5th generation cameras

**Best practice:** To avoid Sony 5th generation cameras from going offline, it is recommended to set the Transaction timeout to 60 seconds. To do this:

1. Open Config Tool.
2. From the Home page, click the System task, and then click the Roles tab.
3. Select the Archiver that is managing the Sony unit, and then click the Extensions tab.
4. Click the Sony extension.
5. From the Transaction timeout drop-down list in the General section, select 50 sec.
6. Click Apply.

### Creating Sony PTZ patterns

PTZ patterns can be created for some Sony cameras through the Preset Tour feature. A Sony Preset Tour is similar to a Security Center PTZ pattern; it is a series of presets (which includes camera positioning, iris, and focus settings), which can be run in the Security Desk or Config Tool the same as any other PTZ pattern. For more information about Preset Tours, refer to your Sony camera’s documentation.

There are three steps to creating Sony PTZ patterns:

- Define presets
- Configure the preset tour
- Test the Sony PTZ pattern

#### Define presets

- You must define two or more PTZ presets on the Sony camera in the Config Tool before you can create a preset tour in the unit’s Web page.
- In the Config Tool or Security Desk, select the Sony PTZ camera to configure.
2 Do one of the following:
   - If you are in the Config Tool, click the Live video button.
   - If you are in Security Desk, select the camera in the tile.
3 In the PTZ controls toolbar, click the advanced mode button.
4 From the Presets drop-down list, select a preset number, and click the Edit button.
5 Using the PTZ controls, move the camera to a new position.
6 Click the Edit button again.

Configure the preset tour

Once you have defined two or more PTZ presets in Security Center, you must create and configure a preset tour in the Sony unit’s Web page.

1 Open the Sony unit’s Web page.
2 Click Setup.
3 Enter username and password of the unit.
4 Click Preset position > PresetTour.

5 Set the Tour option to On.

6 Set the Resume time on inactivity option to On, and type a value (in seconds).
   **NOTE** The Resume time on inactivity option is how much time it takes to resume a PTZ pattern after an operator has moved the PTZ camera. If the option is set to Off, the PTZ pattern must be restarted manually.

   Best practice: Set the value to 120 seconds

7 Select the preset tour you want to configure (A, B, C, D, or E), and set the Tour to On.

8 Under Sequence in the drop-down list, select a previously defined preset you created in Config Tool, and click Add.

9 Repeat Step 8 for each preset you want to add to the sequence.

10 To change the order of the presets, select the preset and click the Up or Down button.

11 Select the Speed of the camera. The higher the value, the faster the camera moves. You can also select Fastest.
12 Beside Stay time, enter the amount of time you would like the camera to stay at each preset position.

13 (Optional) Use the Preview and Stop buttons, to start and stop a preview of the selected tour.

14 Beside Effective period select Always.

15 Click OK.

You now can use the preset tour (sequence) as a PTZ pattern in Security Center.

Test the Sony PTZ pattern

1 In the Config Tool or Security Desk, select the Sony PTZ camera to be tested.

2 Do one of the following:
   - If you are in the Config Tool, click the Live video button.
   - If you are in Security Desk, select the camera in the tile.

3 In the PTZ controls toolbar, click the advanced mode button.

4 From the Patterns drop-down list, select a pattern to play.
   
   **NOTE** Pattern 0 in Security Center represents preset tour A on the Sony unit, 1=B, 2=C, 3=D, and 4=E.

5 Click the Play button.
Using the Copy configuration tool

When using the Copy configuration tool in Security Center with Sony 5th Generation units, the camera configuration is dependant on the unit configuration. Therefore, you must copy the unit configuration before copying the camera configuration.
Configure Sony edge recording and video trickling

Video trickling is supported on Sony units with firmware 1.61 and later in Security Center through the Sony Edge Storage (edge recording) feature. To use edge recording and video trickling on Sony cameras, you need to enable the Edge Storage, and configure some additional settings on the unit's Web page.

1. Open the unit’s Web page.
2. Click Setup > Edge Storage.

3. In the Edge Storage option, click On, and then click OK.
   
   **NOTE** If you set the Effective period option to Always, edge recording is stopped if you change the video stream type.

4. Click the Image memory tab, and then click the Common tab.
5. In the Image memory option, click Off, and then click OK.
6. Click the Alarm recording tab.
7. In the Alarm recording option, click Off, and then click OK.
8. Click the Periodical recording tab.
9. In the Periodical recording option, click Off, and then click OK.
10 Click the FTP client tab, and then click the Common tab.
11 In the FTP client option, click Off, and then click OK.
12 Click the Alarm sending tab.
13 In the Alarm sending option, click Off, and then click OK.
14 Click the Periodical sending tab.
15 In the Periodical sending option, click Off, and then click OK.
16 Click the e-Mail (SMTP) tab, and then click the Alarm sending tab.
17 In the Alarm sending option, click On.
18 In the File attachment option, click Off, and then click OK.
19 Click the Periodical sending tab.
20 In the Periodical sending option, click Off, and then click OK.

21 Click the System tab, and then click the Installation tab.
22 In the Video out option, click Off, and then click OK.

Maintaining 4:3 aspect ratio for the SNC-ZP550

Some units such as the SNC-ZP550 do not support resolutions with a 4:3 aspect ratio, the image will be stretched when viewing the stream. For example, if you choose to view a 620x480 stream it will actually display a stretched 620x368 stream. As a workaround, enable the Letterbox option on the unit's Web page to preserve the 4:3 aspect ratio.

1 Open the unit's Web page.
2. Click Setup > Camera and select the Video codec tab.
3. Turn the Letterbox option On.
Configuring 6th generation units to stream at 60 frames per second

To stream at 60 fps, Wide dynamic range should be enabled and the Mode must be set to High frame rate.

1. From the Logical view task in Config Tool, select the camera to configure.
2. Click the Hardware tab.
3. Select the Wide dynamic range option.
4. From the Mode drop-down list, select High frame rate.
5. Click Apply.

**NOTE** If you set the Mode to High frame rate, the Wide dynamic range level on the unit will be decreased as streaming at a high framerate (60 fps) requires that the Wide dynamic range level be low. The Wide dynamic range level is set on the unit's Web page under Settings > System > Installation.
UDP Technology

Complete the following configuration steps before adding UDP units to the Config Tool:

1. Open the unit’s Web page.
2. Click Basic Configuration tab > Web Server.
3. Under HTTP(S) Settings, select the HTTP option and click Apply.
   **IMPORTANT** If this option is not enabled, automatic unit discovery will not work in Security Center.
4. Click the Video & Audio tab, and select Codec.
5. Under Video Stream Codec Settings, click the First Stream tab and select H.264 from the Video Codec list, then click Apply.
6. Click the Second Stream tab, and select MPEG4 from the Video Codec list, then click Apply.
7. Click the System Options tab, and select RTSP/RTP.
8. Select the Does not include NAL unit header option.
9. Click the UNICAST tab, and select Enable RTP Session.
10. Under RTP Configuration-first stream, make sure the Session name parameter displays firststream.
11. Under RTP Configuration-second stream, make sure the Session name parameter displays secondstream.
12. Click Apply.
This section describes the additional configuration steps required for some Verint units to work in Security Center.

**Configure S1808e-A and S1816e-A units**

By default there are four Mic In audio inputs used in Security Center, but S1808e-A and S1816e-A units support up to eight Line In. For these units to use the Line In audio type, you must change the input type in Security Center.

1. In the Video tab in the Config Tool, select the unit to configure.
2. Click the Peripherals tab.
3. Select the microphone to be configured, and click the Edit button.
4. From the Input type drop-down list in the Properties tab, select Line In.
5. Click Save.
6. For the new audio inputs to be available, restart the unit in Security Center.
This section describes how to start the wiper on the Ulisse Compact IR360.

**Configuring the wiper on the Ulisse Compact IR360**

To start and stop the wiper, use the PTZ widget in Security Desk.

1. From the Monitoring task in Security Desk, drag the Ulisse Compact IR360 into a tile.
2. In the PTZ widget click the Toggle to advanced mode button.
3. Under Auxiliaries, select 3-Untitled.
4. Click the Rename button and rename the Auxiliary as Wiper.
5. Click the Start auxiliary command button to start the wiper, and click the Stop auxiliary command button to stop it.
This section describes the additional configuration steps required for some Vivotek units to work in Security Center.

This section includes the following topics:

- "Configure IP8161 units" on page 108

Configure IP8161 units

To stream video at 30 frames per second with Vivotek IP8161 units, you must perform additional configuration steps in the unit’s Web page.

1. Open the unit’s Web page.
2. Click Configuration > Video/Audio.
3. On the Video and Audio Settings page, select Stream 1, and click Change.
4. From the Priority drop-down list in the Stream 1 dialog box, select Frame Rate.
5. Click Set.

Configure Vivotek FE8171V fish-eye cameras

This section describes the additional configuration steps required to use the fish-eye dewarping feature of Vivotek FE8171V fish-eye cameras in Security Center. Dewarping allows you to zoom in on a 360° image, similar to the digital zoom feature in Security Desk. The zoomed image is dewarped, or flattened to show a rectangular image.

This section includes the following topics:

- "Enable watermarking on the FE8171V fish-eye camera" on page 108
- "Configure Vivotek FE8171V fish-eye cameras lenses" on page 109
- "Use the dewarping feature" on page 110

Enable watermarking on the FE8171V fish-eye camera

In order to dewarp an image in Security Center, you must enable watermarking on the camera before it’s added to Security Center.

To do this:

1. Open a web browser.
2. Navigate to the following address: http://<IP ADDRESS>/cgi-bin/admin/set-param.cgi?videoin_c0_enablewatermark=1
**Configure Vivotek FE8171V fish-eye cameras lenses**

Before viewing video with a Vivotek FE8171V fish-eye camera lens in Security Desk, you must configure the lens in Config Tool.

1. From the Video task in Config Tool, select the camera.
2. Click the Hardware tab.
3. From the Lens type drop-down list, select Vivotek.
4. Click the Edit (-pencil) button.
5 In the Configure lens dialog box, do the following:

- Using the Width and Height fields to set the Maximum Dewarped resolution values.
- Select the Camera position.
- To set the center position of the fish-eye, drag the left mouse button.
- To adjust the radius of the fish-eye, drag the right mouse button.
  **NOTE** The blue region represents the area that can be dewarped in a Security Desk tile.
- Click Ok.

6 In the Hardware tab, click Apply.
  **NOTE** For settings to take effect after making changes in the Configure lens dialog box, the camera needs to be removed from all Security Desk tiles and Monitoring tasks and re-added.

**Use the dewarping feature**

The dewarping process is done in Security Desk. When you zoom into a Vivotek FE8171V fish-eye camera lens image in the Security Desk Monitoring task, it is dewarped and shown as a rectangular image. The dewarping time varies, depending on your computer and the dewarped resolution. For example, the dewarping time will be four times longer using a 640x480 resolution instead of a 320x240 resolution.

1 From the Monitoring task in Security Desk, drag the Vivotek FE8171V fish-eye camera in a tile.
2 To zoom in the image, use your mouse wheel, or draw a box on the region you want to zoom to.

![Zoom In Image](image1)

**NOTE** If you zoom using your mouse wheel, it zooms to the center of the image, not where your cursor is pointing.

3 To navigate the zoomed image, click the image thumbnail at the top-left of the tile.

![Zoom Out Image](image2)

4 To zoom out, use the mouse wheel, or the zoom slider on the right-side of the tile.

![Zoom Slider](image3)
Configure digital zoom presets

You can create digital zoom presets for Vivotek FE8171V fish-eye cameras and other non-PTZ cameras, similar to PTZ presets in Security Desk.

NOTES

• Digital zoom presets are not supported on PTZ cameras.
• You can create as many presets as you want.

To create a digital zoom preset:

1. From the Monitoring task in Security Desk, drag the Vivotek FE8171V fish-eye camera in a tile.
2. Zoom to the position you want to create a preset for.
3. In the camera widget, click Add.

The digital zoom preset uses the camera's current zoom position.

4. Type a name for the preset.
5. Click Create.

You can now zoom to the preset by selecting it from the Digital zoom presets drop-down list.

From the Preset (.swifted) button next to the Digital zoom presets drop-down list, you can also perform the following tasks:

• *Reload*. Return to the preset if you've moved out of the preset region.
• *Save*. Re-save the preset as the current zoom position.
• *Rename*. Rename the current preset.
• *Remove*. Delete the current preset.
• *Create*. Click to create another preset.
Where to find product documentation

You can find our product documentation in the following locations:

• **Installation package.** The documentation is available in the *Documentation* folder of the installation package. Some of the documents also have a direct download link to the latest version of the document.

• **Genetec Technical Assistance Portal (GTAP).** The latest version of the documentation is available from the GTAP *Documents* page. Note, you’ll need a username and password to log on to GTAP.

• **Help.** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. To access the help, click Help, press F1, or tap the ? (question mark) in the different client applications.
Technical support

Genetec Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a Genetec customer, you have access to the Genetec Technical Assistance Portal (GTAP), where you can find information and search for answers to your product questions.

- **Genetec Technical Assistance Portal (GTAP).** GTAP is a support website that provides in-depth support information, such as FAQs, knowledge base articles, user guides, supported device lists, training videos, product tools, and much more.
  
  Prior to contacting GTAC or opening a support case, it is important to look at this website for potential fixes, workarounds, or known issues. You can log in to GTAP or sign up at https://gtap.genetec.com.

- **Genetec Technical Assistance Center (GTAC).** If you cannot find your answers on GTAP, you can open a support case online at https://gtap.genetec.com. For GTAC’s contact information in your region see the Contact page at https://gtap.genetec.com.
  
  **NOTE** Before contacting GTAC, please have your System ID (available from the About button in your client application) and your SMA contract number (if applicable) ready.

- **Licensing.**
  - For license activations or resets, please contact GTAC at https://gtap.genetec.com.
  - For issues with license content or part numbers, or concerns about an order, please contact Genetec Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
  - If you require a demo license or have questions regarding pricing, please contact Genetec Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Additional resources

If you require additional resources other than the Genetec Technical Assistance Center, the following is available to you:

- **GTAP Forum.** The Forum is an easy to use message board that allows clients and Genetec staff to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in or sign up at https://gtapforum.genetec.com.

- **Technical training.** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/Services.