
# Feature Setup

The Feature Setup windows let you configure a variety of IP camera features and functions. The following sections describe the Feature Setup windows in detail:



## Streaming Window

The Streaming window provides options for configuring audio and video streams from the IP camera. You can configure settings for the primary and an optional secondary video stream.

Configuring a secondary stream is useful for providing a video stream that is at a lower resolution than the primary stream to third-party devices or software.

Both streams support H.264 and MJPEG for video, and G.711 A-law and G.711 u-law for audio.

When configuring video streams, be aware of the following guidelines:

- The resolution of the primary stream must be higher than the resolution of the secondary stream.
- You cannot configure a maximum frame rate of 30 for the primary stream if the secondary stream is enabled.
- Multiple secondary frame rates are supported. Table 4-1 shows the frame rate combinations of primary and secondary streams with a 16:9 aspect ratio, and Table 4-2 shows the frame rate combinations of primary and secondary streams with a 4:3 aspect ratio. If a secondary frame rate that is not shown in this table is selected in Cisco Video Surveillance Manager, the IP camera uses the closest available frame rate.

**Note** If you configure the camera for 768 x 432, 704 x 400, and 352 x 208 resolutions and then downgrade the firmware, the camera might reboot. Before downgrading, change the resolution back to an older resolution.

*Table 4-1 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| 1280 x 800 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M | – | – | – |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M | – | – | – |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 1024 x 576 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | 960 x 544 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | 768 x 432 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 704 x 400 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |

*Table 4-1 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| 1280 x 720 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M | | | |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M | | | |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 1024 x 576 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | 960 x 544 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | 768 x 432 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 704 x 400 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |

*Table 4-1 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| 1024 x 576 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M | 1024 x 576 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | 960 x 544 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | 768 x 432 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 704 x 400 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 960 x 544 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M | 960 x 544 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | 768 x 432 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |

*Table 4-1 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 704 x 400 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 768 x 432 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 768 x 432 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M | 704 x 400 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |

*Table 4-1 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 704 x 400 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 704 x 400 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 640 x 368 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 640 x 368 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |

*Table 4-1 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 352 x 208 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M | 352 x 208 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | | | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 320 x 192 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M | 320 x 192 | 10, 15 | 64K, 128K, 256K, 384K, 768K |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| | | | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 192 x 112 | 20, 25, 30 | 64K, 128K, 256K, 384K | 192 x 112 | 10, 15 | 64K, 128K, 256K |
| | 10, 15 | 64K, 128K, 256K | | 1, 3, 5, 6, 8 | 64K, 128K |
| | 1, 3, 5, 6, 8 | 64K, 128K | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K |
| 160 x 96 | 20, 25, 30 | 64K, 128K, 256K, 384K | 160 x 96 | 10, 15 | 64K, 128K, 256K |
| | 10, 15 | 64K, 128K, 256K | | 1, 3, 5, 6, 8 | 64K, 128K |
| | 1, 3, 5, 6, 8 | 64K, 128K | | | |

*Table 4-2 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 4:3 Aspect Ratios*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| 720 x 576 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 720 x 576 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M | 704 x 576 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 288 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K |
| 704 x 576 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 704 x 576 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M | 352 x 288 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K |
| 720 x 480 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 720 x 480 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M | 704 x 480 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | 352 x 240 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K |
| 704 x 480 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M | 704 x 480 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K, 1M | 352 x 240 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M |
| | | | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K |

*Table 4-2 Cisco Video Surveillance 3000 Series IP Camera Video Stream Support for 4:3 Aspect Ratios*

| Primary (H264) | FPS | Bit Rate | Secondary (H264 or MJPEG) | FPS | Bit Rate |
|---|---|---|---|---|---|
| 352 x 240 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | 352 x 240 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K | | | |
| 352 x 288 | 20, 25, 30 | 64K, 128K, 256K, 384K, 768K, 1M, 2M | 352 x 288 | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M |
| | 10, 15 | 64K, 128K, 256K, 384K, 768K, 1M | | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K |
| | 1, 3, 5, 6, 8 | 64K, 128K, 256K, 384K, 768K | | | |

To display the Streaming window, perform the following steps:

**Procedure**

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Streaming**.

The Streaming window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-3 describes the options in the Streaming window.

*Table 4-3 Streaming Window Options*

| Option | Description |
|---|---|
| **Current Stream Area** | |
| Stream | Choose the video stream (Stream 1 or Stream 2) to which the configuration settings in the Streaming window apply. Stream 1 is the primary stream, and Stream 2 is the secondary stream. |
| Enable Stream | Check this check box to cause the IP camera to send audio/video data on the selected stream. |

*Table 4-3 Streaming Window Options (continued)*

| Option | Description |
|---|---|
| **Streaming Area** | |
| **Note** Each video stream uses its own set of streaming options. The settings shown in the **Streaming Area** apply to the currently selected stream only. | |
| RTSP Port | Transmission Control Protocol (TCP) port on which the IP camera receives Real-Time Streaming Protocol (RTSP) commands. You must configure this port if you want to allow third-party devices or software to access video streams from the IP camera.<br>RTSP is a standard for connecting a client to control streaming data over the web.<br>Valid values are 554 and 1024 through 65535. The default port is 554. |
| Video Source Port | Universal Datagram Protocol (UDP) port on which the IP camera transmits Video Real-Time Transport Protocol (RTP) data.<br>Valid values are even numbers 1024 through 65534. The default port is 1024. |
| Audio Source Port | UDP port on which the IP camera transmits audio RTP data<br>Valid values are even numbers 1024 through 65534. The default value is 1026. |
| Max RTP Packet Size | Maximum number of bytes per data packets that are sent in each RTP request.<br>Configure a lower number if you are streaming video to a cell phone that requires smaller data packets.<br>Valid values are 400 through 1400. The default value is 1400. |
| Enable Multicast | Check this check box to send video and audio data as a multicast stream.<br>When multicast is enabled, the IP camera sends video and audio to the multicast addresses that you designate. Multicast enables several devices to receive the video signal from the IP camera simultaneously. |
| Multicast Address | Enter the multicast IP address on which the IP camera sends a multicast audio/video stream. |
| Multicast Video Port | Enter the port on which the IP camera sends a multicast video stream.<br>Valid values are even numbers 1024 through 65532. |
| Multicast Audio Port | Enter the port on which the IP camera sends a multicast audio stream.<br>Valid values are even numbers 1024 through 65532. |
| Time to Live | Enter the number of hops, which specifies the number of network devices that an audio/video stream can pass before arriving at its destination or being dropped.<br>Valid values are 1 through 255. |
| **Video Area** | |
| **Note** Each video stream uses its own set of video options. The settings shown in the **Video Area** apply to the currently selected stream only. | |
| Video Standard | Choose the system for video transmission: NTSC or PAL.<br>The setting that you make affects each channel that is enabled. |

*Table 4-3 Streaming Window Options (continued)*

| Option | Description |
|---|---|
| Video Codec | Choose the codec for video transmission: H.264 or MJPEG. Both options are supported on the primary and secondary streams. |
| Video Resolution | Choose the resolution for video transmission. The resolutions in this drop-down list depend on the video standard that you selected. |
| Maximum Frame Rate | Choose the maximum frame rate of the video stream. |
| Video Quality Control | Choose an option for the video quality of the video stream from the IP camera:<br>• **Constant Bit Rate**—Available for the primary stream only. Specifies that the video stream is output at or close to the constant bit rate that you choose.<br>You can select one of the Mbps values in the drop-down menu. The default value is 4 Mbps. A higher bit rate provides better video quality but consumes more bandwidth.<br>You can also select the Customized option to enter a rate within the valid range, depending on resolution and frame rate.<br>• **Fixed Quality**—Specifies that video is output at a fixed quality, which ranges from Very High to Low. The bit rate may vary to maintain this quality. The default fixed quality is Normal. A higher fixed quality provides better video quality but consumes more bandwidth.<br>You can use these options to help manage bandwidth use in your network. For example, if the IP camera is focused on an area with little movement, such as an emergency exit, you can configure it with a low fixed quality. |
| **Analog Video Area** | |
| **Note** This option applies to the primary stream only. | |
| Enable Analog Video Port | Check this check box if you want the IP camera to enable analog video for installation purposes. To enable analog video, the following settings are required:<br>• The primary video stream frame rate must be set to 15 fps or lower.<br>• The secondary video stream must be disabled. |
| **Audio Area** | |
| Enable Audio | Check this check box if you want to enable audio. |
| Audio Codec | Choose the audio codec to use for encoding audio:<br>• **G.711 A-Law**—Encodes 14-bit signed linear PCM samples to logarithmic 8-bit samples.<br>• **G.711 u-Law**—Encodes 13-bit signed linear PCM samples to logarithmic 8-bit samples.<br>**Note** The G.711 A-law algorithm provides more quantization levels at lower signal levels whereas the G.711 μ-law algorithm tends to give more resolution to higher range signals. |
| Audio Sampling Rate | *Display only.* Indicates the sampling rate of the audio stream from the IP camera |

*Table 4-3 Streaming Window Options (continued)*

| Option | Description |
|---|---|
| Audio Resolution | *Display only.* Indicates the resolution for audio transmission from the IP camera. |

# Camera Window

The Camera window provides options for selecting a microphone, making certain video adjustments, exposure control, and configuring the operation of the IP camera day and night filters.

A microphone captures audio at the camera location. This audio is sent to the PC that you use to view video from the IP camera. You can listen to the audio when viewing video in the Camera Video & Control window.

The IP camera day and night filters allow the IP camera to optimize its video image for various lighting conditions. When the IP camera uses its day filter, it is operating in *day mode*. In this mode, the camera displays video images in color. When the IP camera uses its night filter, it is in *night mode*. In this mode, the camera displays video images in black and white.

To display the Camera window, perform the following steps:

**Procedure**

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Camera**.

The Camera window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-4 describes the options in the Camera window.

*Table 4-4 Camera Window Options*

| Option | Description |
|---|---|
| **Microphone** | |
| Microphone Type | The Cisco IP camera supports only an external microphone. Audio is captured by an optional external microphone, available from third-parties. |

*Table 4-4 Camera Window Options (continued)*

| Option | Description |
|---|---|
| **Day/Night Filter Area** | |
| Switch Mode | Choose the day/night mode for the IP camera:<br>• **Day**—IP camera always remains in day mode.<br>• **Night**—IP camera always remains in night mode.<br>• **Auto**—IP camera automatically switches between day and night mode based on the lighting condition threshold that you specify.<br>When the IP camera is in Auto mode, it attempts to avoid frequent or unnecessary changes between day mode and night mode (such as can occur when an IP camera is set up on a street where car headlights could cause constant changes between these modes). When the IP camera detects that a switch from day to night mode might be necessary, it monitors the light level for 10 seconds. If the light level remains below or above the configured Day to Night Threshold for the entire 10 seconds, the IP camera switches modes. Otherwise, the IP camera remains in the current mode.<br>If the IP camera goes through 3 day/night mode transitions within a 60 second period, the camera stops detecting and implementing day/night changes for a period of 5 minutes from the point of the third transition. During these 5 minutes, the IP camera remains in the current day or night mode.<br>• **Night External**—IP camera switches to night mode based on external Input port. It switches to day mode when the external Input port is not in the triggered status. Check the external Input port of "Alarm I/O Ports." Output port is optional and can be used to trigger devices connected externally.<br>• **Night Schedule**—IP camera switches to and from Night mode based on the Start and End times. Start Time - Enter the time, in 24 hour format, when camera enters Night mode. End Time - Enter the time, in 24 hour format, when camera exists Night mode.<br>**Note** If you configure a Night Schedule, make sure that the time on the IP camera is set correctly. |
| Day to Night Threshold | The Day to Night Threshold option is available only when the Switch Mode is set to Auto. Choose a value that specifies the relative light threshold at which the IP camera switches from day to night mode. A lower value designates that the IP camera switches from day to night mode in brighter conditions. A higher value designated that the IP camera switches modes in darker conditions.<br>The default value is 45. |

*Table 4-4 Camera Window Options (continued)*

| Option | Description |
|---|---|
| Night to Day Threshold | The Night to Day Threshold option is available only when the Switch Mode is set to Auto. Choose a value that specifies the relative light threshold at which the IP camera switches from night to day mode. A lower value designates that the IP camera switches from night to day mode in darker conditions. A higher value designated that the IP camera switches modes in lighter conditions.<br>The default value is 85. |
| Input | The Input option is available only when the Switch Mode is set to Night External. Choose the Input port that is connected an external device that is to trigger the switch to night mode. |
| Output | Choose the Output port that is connected to an external device that is to be triggered.<br>This option is not when the Switch Mode is set to Day. |
| Start Time | The Start Time option is available only when the Switch Mode is set to Night Schedule. Enter the time, in 24 hour format, when the camera enables its night filter. |
| End Time | The Start Time option is available only when the Switch Mode is set to Night Schedule. Enter the time, in 24 hour format, when the camera disables its night filter. |
| **Camera Tamper Area** | |
| Enable camera tamper detection | Check this check box to enable the camera tamper feature.<br>When enabled, this feature causes the IP camera to generate alerts when any of the following events occur and persist for a designated period:<br>• The IP camera view is changed<br>• The IP camera view is blocked<br>• The IP camera view is substantially out of focus |
| Minimum duration | Enter the minimum length of time that a tamper event persists before a tamper alert is generated. To prevent false alerts, the IP camera waits for this period after detecting a tamper event before it generates an alert. If the tamper event is resolved (the IP camera view is returned to its original setting, the IP camera view blockage is removed, or the IP camera is put back in focus), an alert is not generated.<br>Valid values are 10 to 600 seconds. |

# Video Overlay Window

The Video Overlay window provides options for configuring overlay information that appears on the video image in the Camera Video & Control window.

To display the Video Overlay window, perform the following steps:

**Procedure**

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Video Overlay**.

The Video Overlay window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-5 describes the options in the Video Overlay window.

*Table 4-5 Video Overlay Window Options*

| Option | Description |
|---|---|
| **Text Overlay Area** | |
| Enable Date/Time Display | Check this check box to display the time from the internal clock of the IP camera as an overlay on the video image from the IP camera. |
| Date/Time alignment in Overlay | Choose whether the Date/Time is to be aligned to the **Left**, **Center**, or **Right** |
| Enable Text Display | Check this check box to display the text that you enter in the Display Text field as an overlay on the video image from the IP camera.<br>This option can be useful for identifying this IP camera in an installation with several IP cameras. |
| Text Alignment in Overlay | Choose whether the text overlay is to be aligned to the **Left**, **Center**, or **Right**. |
| Text Format | Specifies the text format to use for the text overlay. Currently, English (ASCII) is the only available text format. |
| Display Text | If you check the Enable Text Display check box, the text that you enter in this field appears as an overlay on the video image from the IP camera.<br>The text can contain up to 26 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / : = @ ^ _ ` { } ~ |
| Overlay Placement | Choose whether the text overlay is to appear at the **Top of Image** or **Bottom of Image**. |

# IO Ports Window

The IO Ports window lets you configure various options for the two input and two output ports on the IP camera. A state change of an input ports triggers a camera to take configured actions. Output ports send signals that can control external devices, such as alarms or door switches.

The IP camera can trigger an action only when the input that is received on an input port comes from a contact that is in a normally closed condition. The camera triggers the action when the contact changes to an open condition.

To display the IO Ports window, perform the following steps:

### Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **IO Ports**.

The IO Ports window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-6 describes the options in the IO Ports window.

*Table 4-6 IO Ports Window Options*

| Option | Description |
|---|---|
| **Input Ports Area** | |
| Port # | *Display only.* Indicates input port 1. |
| Current State | *Display only.* Indicates the current state (high or low) of the corresponding port. |
| Event Trigger | Choose the state (Rising or Falling) that triggers designated camera actions. When an input port changes to the configured state, the camera determines that an event has occurred and takes the actions that you have configured. |
| **Output Ports** | |
| Port # | *Display only.* Indicates output port 1 and output port 2. |
| Current State | *Display only.* Indicates the current state (high or low) of the corresponding port. |
| Default State | Choose the state (low or high) to which the corresponding port is set when the IP camera powers on or resets.<br>The port changes to this state when you click **Save**.<br>The default setting is High. |
| Event Action | *Display only.* Indicates the current state (high or low) to which the output port changes when an event occurs. |
| Automatic Reset | Check this check box if you want the corresponding output port to go back to its default state after an event occurs. |
| Duration | If you checked the Automatic Reset check box, enter the amount of time, in milliseconds, that elapses before the port goes back to its default state after an event changes it from the default state. |

# Event Notification Window

The Event Notification window provides options for how the IP camera handles system triggers and generates event notification. A system trigger is any of the following:

- A change of state from low to high or from high to low on an input port of the IP camera. For related information about input ports, see the "IO Ports Window" section on page 4-15.

- Motion that the IP camera detects. For related information about motion detection, see the "Motion Detection" rows in Table 3-1.
- An activity that is defined by a camera app.

When a system trigger occurs, it causes the IP camera to execute certain configured event notifications:

- Email notification—An event can cause the IP camera to send a notification e-mail message to designated recipients. The message can include a video clip or a snapshot of the activity that triggered the event.

  This message includes the same information that is provided with HTTP notification.
- Output port state change—Changes the state of an IP camera output port from low to high or from high to low.
- Syslog server message—Sends a notification message to the designated Syslog server.
- HTTP notification—IP camera sends notification to a remote system via HTTP. This information includes the following:
  - Device ID—ID of the IP camera.
  - Device name—Name of the IP camera.
  - IP address—IP address of the IP camera.
  - MAC address—MAC address of the IP camera.
  - Channel ID—Channel identification number (1 for primary stream or 2 for secondary stream).
  - Channel name—Name that is configured for the channel.
  - Date and time—Date and time that the event occurred.
  - Active post Count—Sequence number of the notification for this event.
  - Event type—Type of event.
  - Event state—Indicates whether the event is active or inactive at the time that the event was detected for this notification.
  - Event description—Description of the event.
  - Input port ID—If the event was triggered by an input port state change, port ID of the port
  - Region index—If the event was triggered by motion detection, identification number of the region in which the IP camera detected motion.
  - Sensitivity level—If the event was triggered by motion detection, sensitivity that is configured for the region in which motion was detected.
  - Detection threshold—If the event was triggered by motion detection, threshold that is configured for the region in which motion was detected.
- FTP notification—An event can cause the IP camera to upload a video clip or a snapshot of the activity that triggered the event to an FTP server.

The Event Notification window also allows you to designate schedules. If a trigger takes place within a designated schedule, the IP camera takes the actions that you configure.

### Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Event**.

The Event Notification window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You may need to scroll down to it.

Table 4-7 describes the options in the Event Notification window.

***Table 4-7 Event Notification Window Options***

| Option | Description |
|---|---|
| **Event Triggering Area** | |
| Triggered by | Check the desired check boxes to designate the events that trigger actions:<br>• **Input 1**—Event is triggered when input port 1 on the IP camera changes state from high to low.<br>• **Motion Detection**—Event is triggered when the camera detects motion, if motion detection is configured as described the "Motion Detection" rows in Table 3-1 on page 3-1.<br>• **App**—Event is triggered by an activity that is defined by an app that is running on the IP camera. |
| Actions | Check the desired check boxes to designate that actions that the IP camera takes when the corresponding trigger occurs.<br>• **Email**—Sends information about the event in an e-mail message to the designated recipient. You design the recipient and configure other e-mail options in other fields in this window.<br>• **Output 1**—Changes the state of the output 1 port on the IP camera as defined in the Port window.<br>• **Syslog**—Sends information about the event to a designated Syslog server.<br>• **HTTP**—Sends information about the event as an HTTP stream to a remote system.<br>• **FTP**—Uploads a snapshot or video clip of the event to an FTP server. |
| Interval | Choose the time interval (in minutes) from the drop-down list to wait after an event occurs before detecting the next event. |
| **Event Scheduling Area** | |
| Scheduling Grid | Designate the times at which an event causes the IP camera to take the designed actions. If an event occurs during a time that is not designated, the IP camera does not take any action.<br>Each cell in this grid represents one hour on the corresponding day, starting at 12:00 a.m. (0:00). To designate times, click the desired cells. Selected cells appear shaded.<br>To select all times, click the **Set All** button.<br>To deselect all times, click the **Clear All** button.<br>To change the scheduling settings to the last saved configuration, click **Undo All**. |

*Table 4-7 Event Notification Window Options (continued)*

| Option | Description |
|---|---|
| **Set All** button | Selects all cells in the scheduling grid. |
| **Clear All** button | Deselects all cells in the scheduling grid. |
| **Undo All** button | Deselects cells in the scheduling grid that you selected since last saving Event Notification window settings. |
| **HTTP Notification Area** | |
| High Availability | Check this check box if you want to send HTTP messages to a secondary HTTP server in the event that the primary HTTP server is unreachable. |
| Primary HTTP Server | Identify the primary server to which HTTP messages are sent by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| URL Base | Enter a string to be used as the prefix in the HTTP URL. The HTTP URL is sent in this format:<br>http://<*IP address*>/<*URL Base*>?<*system-provided-name-value-pairs*><br>where *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* is information about the event. |
| Port Number | Enter the port number that receives messages on the primary server to which HTTP messages are sent. |
| User Name | If authentication is required on the primary server to which HTTP messages are sent, enter the user name. |
| Password | If authentication is required on the primary server to which HTTP messages are sent, enter the password. |
| HTTP Authentication | If authentication is required on the primary server to which HTTP messages are sent, choose the authentication method from the drop-down list. |
| Secondary HTTP Server | If the High Availability check box is checked, you can identify an optional secondary server to which HTTP messages are sent by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| URL Base | Enter a string to be used as the prefix in the HTTP URL for the secondary server. The HTTP URL is sent in this format:<br>http://<*IP address*>/<*URL Base*>?<*system-provided-name-value-pairs*><br>where *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* is information about the event. |
| Port Number | Enter the port number that receives messages on the secondary server to which HTTP messages are sent. |
| User Name | If authentication is required on the secondary server to which HTTP messages are sent, enter the user name. |
| Password | If authentication is required on the secondary server to which HTTP messages are sent, enter the password. |

*Table 4-7 Event Notification Window Options (continued)*

| Option | Description |
|---|---|
| **Set All** button | Selects all cells in the scheduling grid. |
| **Clear All** button | Deselects all cells in the scheduling grid. |
| **Undo All** button | Deselects cells in the scheduling grid that you selected since last saving Event Notification window settings. |
| **HTTP Notification Area** | |
| High Availability | Check this check box if you want to send HTTP messages to a secondary HTTP server in the event that the primary HTTP server is unreachable. |
| Primary HTTP Server | Identify the primary server to which HTTP messages are sent by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| URL Base | Enter a string to be used as the prefix in the HTTP URL. The HTTP URL is sent in this format:<br>http://<*IP address*>/<*URL Base*>?<*system-provided-name-value-pairs*><br>where *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* is information about the event. |
| Port Number | Enter the port number that receives messages on the primary server to which HTTP messages are sent. |
| User Name | If authentication is required on the primary server to which HTTP messages are sent, enter the user name. |
| Password | If authentication is required on the primary server to which HTTP messages are sent, enter the password. |
| HTTP Authentication | If authentication is required on the primary server to which HTTP messages are sent, choose the authentication method from the drop-down list. |
| Secondary HTTP Server | If the High Availability check box is checked, you can identify an optional secondary server to which HTTP messages are sent by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| URL Base | Enter a string to be used as the prefix in the HTTP URL for the secondary server. The HTTP URL is sent in this format:<br>http://<*IP address*>/<*URL Base*>?<*system-provided-name-value-pairs*><br>where *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* is information about the event. |
| Port Number | Enter the port number that receives messages on the secondary server to which HTTP messages are sent. |
| User Name | If authentication is required on the secondary server to which HTTP messages are sent, enter the user name. |
| Password | If authentication is required on the secondary server to which HTTP messages are sent, enter the password. |

*Table 4-7 Event Notification Window Options (continued)*

| Option | Description |
|---|---|
| HTTP Authentication | If authentication is required on the secondary server to which HTTP messages are sent, choose the authentication method from the drop-down list. |
| **Email Notification Area** | |
| Primary SMTP Server | Identify the primary SMTP server that is used for sending e-mail by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| Primary SMTP Port | Enter the port number for the primary SMTP server. The default SMTP port number is 25. |
| POP Server | Identify the primary POP server that is used for sending e-mail by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.<br>This field is dimmed if you do not choose **Requires POP Before SMTP** in the Authentication field that follows. |
| Authentication | If the primary SMTP server requires authentication to send e-mail, choose the appropriate authentication type from the drop-down list. The authentication type typically is the same as that for the POP3 server that you use to receive e-mail. |
| Account Name | If the primary SMTP server requires authentication, enter the account name for the server. |
| Password | If the primary SMTP server requires authentication, enter the account password for the server. |
| Secondary SMTP Server | Identify an optional secondary SMTP server that is used for sending e-mail by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| Secondary SMTP Port | Enter the port number for the secondary SMTP server. The default SMTP port number is 25. |
| POP Server | Identify an optional secondary POP server that is used for sending e-mail by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.<br>This field is dimmed if you do not choose **Requires POP Before SMTP** in the Authentication field that follows. |
| Authentication | If the secondary SMTP server requires authentication to send e-mail, choose the appropriate authentication type from the drop-down list. The authentication type typically is the same as that for the POP3 server that you use to receive e-mail. |
| Account Name | If the secondary SMTP server requires authentication, enter the account name for the server. |
| Password | If the secondary SMTP server requires authentication, enter the account password for the server. |
| Send To | Enter an e-mail address to which an e-mail message is sent when an event occurs. |

*Table 4-7 Event Notification Window Options (continued)*

| Option | Description |
|---|---|
| Show From Address As | Enter the e-mail address to be shown in the From field for the e-mail message that is sent when an event occurs. |
| Subject | Enter the text to be shown in the Subject field for the e-mail messages that the IP camera sends when events occur. The subject can contain up to 118 characters, including spaces. |
| Attach Video Streaming URL Address | Check this check box to include in the e-mail message body the URL from which the recipient can access the live video stream from the camera on which the event was detected. |
| Attach Snapshot | Check this check box to include with the e-mail message a still picture from the beginning of the event. This snapshot is stored on the IP camera until the message is sent.<br>This functionality is available only when the secondary video stream is enabled. |
| Attach Video Clip | This option is available if the secondary video stream (H.264 only) is enabled.<br>Check this check box and enter the following values to include with the e-mail message a video clip of the event:<br>• **Pre-Capture Length**—Enter the amount of video (in seconds) before the event to include in the video clip.<br>**Note** The maximum pre-capture length is 5 seconds.<br>• **Post-Capture Length**—Enter the amount of video (in seconds) after the event to include in the video clip.<br>**Note** The maximum combined pre-capture and post-capture length is 10 seconds.<br>This video clip is stored on the IP camera until the message is sent. |
| **FTP Notification Area** | |
| Primary FTP Server | Identify the primary FTP server to which snapshots or video clips are uploaded by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| Primary FTP Port | Enter the port number that receives messages on the primary FTP server. The default FTP port number is 21. |
| User Name | Enter the primary FTP server login user name. |
| Password | Enter the primary FTP server login password. |
| Enable Passive Mode | Check this check box to enable the passive mode feature of the primary FTP server. |
| Secondary FTP Server | Identify an optional secondary FTP server to which snapshots or video clips are uploaded by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| Secondary FTP Port | Enter the port number that receives messages on the secondary FTP server. The default FTP port number is 21. |
| User Name | Enter the secondary FTP server login user name. |

*Table 4-7 Event Notification Window Options (continued)*

| Option | Description |
|---|---|
| Password | Enter the secondary FTP server login password. |
| Enable Passive Mode | Check this check box to enable the passive mode feature of the secondary FTP server. |
| Upload Snapshot | Check this check box to upload a snapshot of the activity that triggered the event.<br>This functionality is available only when the secondary video stream is enabled. |
| Upload Video Clip | Check this check box and enter the following values to upload a video clip of the activity that triggered the event:<br>• **Pre-Capture Length**—Enter the amount of video (in seconds) before the event to include in the video clip. The default pre-capture length is 0 seconds.<br>**Note** The maximum pre-capture length is 5 seconds.<br>• **Post-Capture Length**—Enter the amount of video (in seconds) after the event to include in the video clip. The default post-capture length is 5 seconds.<br>**Note** The maximum combined pre-capture and post-capture length is 10 seconds. |

# Alert Notification Window

The Alert Notification window provides options for how the IP camera handles health triggers and generates event notification. A health trigger is any of the following:

- Loss of video input to the IP camera
- Tampering that the IP camera detects (if IP camera tamper detection is configured as described the "Camera Tamper Area" rows in Table 4-4)
- An alert that is triggered by any of the following:
  - An IP camera app is stopped, restarted, or uninstalled
  - The IP Camera app manager settings are restored to their factory default values
  - An SD or MicroSD card inserted, removed, or formatted
  - The IP Camera is reboots continually

When a health event occurs, it triggers the IP camera to take certain configured actions:

- Email notification—An event can cause the IP camera to send a notification e-mail message to designated recipients. The message can include a video clip or a snapshot of the activity that triggered the event.

  This message includes the same information that is provided with HTTP notification.
- Output port state change—Changes the state of an IP camera output port from low to high or from high to low.
- Syslog server message—Sends a notification message to the designated Syslog server.

- HTTP notification—IP camera sends notification to a remote system via HTTP. This information includes the following:
  - Device ID—ID of the IP camera.
  - Device name—Name of the IP camera.
  - IP address—IP address of the IP camera.
  - MAC address—MAC address of the IP camera.
  - Channel ID—Channel identification number (1 for primary stream or 2 for secondary stream).
  - Channel name—Name that is configured for the channel.
  - Date and time—Date and time that the event occurred.
  - Active post Count—Sequence number of the notification for this event.
  - Event type—Type of event.
  - Event state—Indicates whether the event is active or inactive at the time that the event was detected for this notification.
  - Event description—Description of the event.
  - Input port ID—If the event was triggered by an input port state change, port ID of the port
  - Region index—If the event was triggered by motion detection, identification number of the region in which the IP camera detected motion.
  - Sensitivity level—If the event was triggered by motion detection, sensitivity that is configured for the region in which motion was detected.
  - Detection threshold—If the event was triggered by motion detection, threshold that is configured for the region in which motion was detected.
- FTP notification—An event can cause the IP camera to upload a video clip or a snapshot of the activity that triggered the event to an FTP server.

The Event Notification window also allows you to designate schedules. If an event takes place within a designated schedule, the IP camera takes the actions that you configure.

### Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Alert**.

The Alert Notification window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You may need to scroll down to it.

Table 4-8 describes the options in the Alert Notification window.

*Table 4-8 Alert Notification Window Options*

| Option | Description |
|---|---|
| **Alert Triggering Area** | |
| Triggered by | Check the desired check boxes to designate the alerts that trigger actions:<br>• **Video Loss**—Alert is triggered if the IP camera loses input to its codec sensor module.<br>• **Tamper**—Alert is triggered when the camera detects tampering, if camera tamper detection is configured as described the "Camera Tamper Area" rows in Table 4-4.<br>• **Alert**—Alert is triggered by any of the following:<br>– An IP camera app is stopped, restarted, or uninstalled<br>– The IP Camera app manager settings are restored to their factory default values<br>– An SD or MicroSD card inserted, removed, or formatted<br>– The IP Camera is reboots continually |
| Actions | Check the desired check boxes to designate that actions that the IP camera takes when the corresponding trigger occurs.<br>• **Email**—Sends information about the alert in an e-mail message to the designated recipient. You design the recipient and configure other e-mail options in other fields in this window.<br>• **Output 1**—Changes the state of the output 1 port on the IP camera as defined in the Port window.<br>• **Syslog**—Sends information about the alert to a designated Syslog server.<br>• **HTTP**—Sends information about the alert as an HTTP stream to a remote system. |
| **HTTP Notification Area** | |
| HTTP Server | Identify the server to which HTTP messages are sent by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| URL Base | Enter a string to be used as the prefix in the HTTP URL. The HTTP URL is sent in this format:<br>http://<*IP address*>/<*URL Base*>?<*system-provided-name-value-pairs*><br>where *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* is information about the event. |
| Port Number | Enter the port number that receives messages on the primary server to which HTTP messages are sent. |
| User Name | If authentication is required on the primary server to which HTTP messages are sent, enter the user name. |
| Password | If authentication is required on the primary server to which HTTP messages are sent, enter the password. |

*Table 4-8 Alert Notification Window Options (continued)*

| Option | Description |
|---|---|
| HTTP Authentication | If authentication is required on the primary server to which HTTP messages are sent, choose the authentication method from the drop-down list. |
| **Email Notification Area** | |
| SMTP Server | Identify the SMTP server that is used for sending e-mail by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field. |
| SMTP Port | Enter the port number for the SMTP server. The default SMTP port number is 25. |
| POP Server | Identify the POP server that is used for sending e-mail by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.<br>This field is dimmed if you do not choose **Requires POP Before SMTP** in the Authentication field that follows. |
| Authentication | If the SMTP server requires authentication to send e-mail, choose the appropriate authentication type from the drop-down list. The authentication type typically is the same as that for the POP3 server that you use to receive e-mail. |
| Account Name | If the SMTP server requires authentication, enter the account name for the server. |
| Password | If the SMTP server requires authentication, enter the account password for the server. |
| Password | If the secondary SMTP server requires authentication, enter the account password for the server. |
| Send To | Enter an e-mail address to which an e-mail message is sent when an event occurs. |
| Show From Address As | Enter the e-mail address to be shown in the From field for the e-mail message that is sent when an event occurs. |
| Subject | Enter the text to be shown in the Subject field for the e-mail messages that the IP camera sends when events occur. The subject can contain up to 118 characters, including spaces. |

# Local Storage

The Local Storage window allows you to enable storing video on a local storage device in case of a network loss. You can download these video recordings from the Local Storage window.

When you use local storage, be aware of the following:

- You can configure the IP camera to save all recordings (*continuous recording mode*) to the SD or MicroSD card, or to save only recording that are made when the IP camera looses network connectivity (*network loss mode*).
- The IP camera supports an SD or MicroSD card with a maximum storage capacity of 32 GB. For efficiency and performance of the local storage feature, Cisco recommends that you use a SD or MicroSD card with a storage capacity of 32 GB.

- 1 GB of the storage capacity on an SD or MicroSD card is reserved for system use and is not available to store recordings.
- When you put an SD or MicroSD card in the IP camera for the first time, the card is formatted automatically if the card does not have the ext2 file system and if the directory structure that is required for recording is not present on the card. A card with a storage capacity of 32 GB can take up to 15 minutes to format.
- If you move an SD or MicroSD card from one IP camera to another, the IP camera to which you moved the card does not format the card automatically. This feature allows you to manually recover any video that is stored on the card by downloading the video from the IP camera user interface. You must format the card before you enable recording for it in the new IP camera.
- If you are not using the IP camera with Cisco VSM, set the system time and time zone from the IP camera user interface before you enable recording to an SD or MicroSD card. If you are using the IP camera with Cisco VSM, enable recording through the Cisco VSM user interface, which synchronizes the camera time with the NTP server. Changing the system time after recording starts can cause issues.
- The continuous recording feature enables VSM to "auto-merge" video archive that has gaps due to network or other issues (assuming that camera was not affected), using camera storage as a temporary archiving medium. It also enables archiving only video that is close to generated events. Either the primary stream or secondary stream can recorded in this mode.
- Grooming starts when continuous recording is enabled and operates as follows:
  1. Groom files that are marked as deleted.
  2. Groom the oldest files on the local SD or MicroSD card when available space on the card is less than 1 GB.
- An IP camera has limited bandwidth for simultaneous reading from and writing to an SD or MicroSD card, which can affect the amount of data that you can copy from the card when recording to the card is enabled. For optimum performance of the IP camera, set the maximum bit rate for the recorded stream to 6 Mbps or lower. At higher bit rates, video may not be copied from the card before the video is groomed.
- Recording MJPEG streams to an SD or MicroSD card is not recommended because the relatively high bit rate of these streams can affect system performance. If you do record MJPEG streams, Cisco recommends that you stop recording before you use the IP camera user interface to copy MJPEG recordings from the card.
- The system allows one active download of video from an SD card or MicroSD card at a time. If VSM is copying data from a card (due to a user or system initiated copy operation), you cannot initiate another download from the IP camera user interface until the VSM download completes. Similarly, if you are using the IP camera user interface to download video from a SD or MicroSD card, video cannot be downloaded from VSM until this download completes.

To display the Local Storage window, perform the following steps:

**Procedure**

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Local Storage**.

The Local Storage window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-9 describes the options in the Local Storage window.

**Note** To use the features in the Recordings area, ActiveX must be installed on your client PC. If ActiveX is not installed, the Recordings area displays a message with this information. To install ActiveX, From the window IP camera web-based interface that instructs you to install the Cisco Camera UI Control , click **Install** in the yellow banner. If a Security Warning dialog box appears, click **Install**.

**Caution** To prevent corruption to data on an SD or MicroSD card or the inability of the IP camera to detect the card again, before removing an SD or MicroSD card from an IP camera, stop recording to the card and use the **Unmount** button (described in Table 4-9 ) to prepare the card for ejection. In addition, use care when inserting, removing, and handling the card to avoid damaging the card.

***Table 4-9 Local Storage Window Options***

| Option | Description |
|---|---|
| **SD/MicroSD Information Area** | |
| Serial Number | *Display only.* Serial number of the SD or MicroSD card that is installed in the IP camera. |
| Total Size | *Display only.* Total storage capacity in megabytes of the SD or MicroSD card. |
| Free Space | *Display only.* Free storage space in megabytes of the SD or MicroSD card. |
| Model | *Display only.* Model number of the SD or MicroSD card. |
| Manufacturer | *Display only.* Manufacturer of the SD or MicroSD card. |
| Mount/Unmount (toggle button) | Mount button—When you insert an SD or MicroSD card, the IP camera typically mounts it automatically. If you see a message that indicates that the card is not mounted, click this button to mount it.<br>Unmount button—Click on this button to prepare an SD or MicroSD card for ejection from the IP camera. |
| Format | Formats an SD or MicroSD card.<br>Use this button to format a card if you switch recording modes or switch the video stream configuration. |
| **Settings Area** | |
| Enable recording to Local Storage on network loss | This options causes the IP camera to save video recordings to its local SD or MicroSD card if the IP camera looses network connectivity. When the network connectivity is restored, recording to the card stops.<br>This option and the **Enable continuous recording** option cannot be enabled at the same time. |

*Table 4-9 Local Storage Window Options (continued)*

| Option | Description |
|---|---|
| Enable Encryption | Available only if **Enable recording to Local Storage on network loss is** enabled. Check to encrypt video that is recorded to the local SD or MicroSD card during a loss of network connectivity. |
| Encryption Method | When encryption is enabled, choose one of the following encryption methods:<br>• AES 256<br>• AES 128<br>• RC2 64 |
| Enable continuous recording | This options causes the IP camera to save all recordings to its local SD or MicroSD card.<br>This option and the **Enable recording to Local Storage on network loss** option cannot be enabled at the same time. |
| Continuous recording stream | Choose which video stream is recorded with continuous recording is enabled. Options are:<br>• Stream 1<br>• Stream 2 |
| Save | Click this button to save changes that you make in the **Settings** area. |
| **Recordings Area (requires a supported version of Microsoft Internet Explorer)** | |
| Recordings list | Displays a list of video recording on the local SD or MicroSD card and the following information and options for each recording:<br>• Select check box. Check the check box next to a recording to select that recording for download or deletion.<br>• Size—Size of the recording in MB.<br>• Name—System-assigned name of the recording.<br>• Start Time (UTC)—Start time of the recording in UTC format.<br>• End Time (UTC)—End time of the recording in UTC format.<br>• Download From (UTC)—To download a recording or part of a recording to your local drive or a network drive, enter the time in UTC format that the video that you want from the recording started.<br>• Duration——To download a recording or part of a recording to your local drive or a network drive, enter the duration of the video that you want from the recording is in hh:mm:ss format. The recording begins from the time that you entered in the Download From field and lasts for the time that you enter in the Duration field.<br>• Progress(%)—The percentage of a video file download operation that has completed.<br>• Status—The status of a video file download or delete operation. |

*Table 4-9 Local Storage Window Options (continued)*

| Option | Description |
|---|---|
| Download | To download a video recording to your local drive or a network drive, check the Select check box for the recording that you want, then click the **Download** button. Follow the on-screen prompts to save the recording.<br><br>When you save a recording, the system creates a directory called Recordings_*TimeStamp* in the location that you choose and saves recordings in that directory. If the recording that you download contains more than 10 minutes of video, the system divides the recording into separate files that contains 10 minutes of video each.<br><br>**Note** Network-loss recordings that are created on an IP camera that is running firmware 2.0.0 cannot be downloaded with the 1.4.1 SD utility. |
| Delete | To delete a video recording from the SD or MicroSD card in the IP camera, check the Select check box for the recording that you want, then click the **Delete** button.<br><br>You can quickly select all video recordings in the list by right-clicking in the Recordings list and then choosing **Select All**. |
| Refresh | To refresh the list of video recording so that the list shows the latest information about the recordings on the SD or MicroSD card in the IP camera, click the **Refresh** button. |
| Cancel | This button appears when a video recording is downloading. To cancel the download operation, click the **Cancel** button. |