avigilon™
a Motorola Solutions Company

Avigilon Control Center™ Enterprise Client User Guide

Version 6.14

© 2006 - 2019, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON CONTROL CENTER, ACC, ACCESS CONTROL MANAGER, ACM, AVIGILON PRESENCE DETECTOR, APD, HIGH DEFINITION STREAM MANAGEMENT (HDSM), HDSM, HDSM SmartCodec, AVIGILON APPEARANCE SEARCH, and RIALTO are trademarks of Avigilon Corporation. Intel and Intel Core are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. ONVIF is a trademark of Onvif, Inc. App Store is a trademark of Apple Inc. Google Play and Google Authenticator are trademarks of Google LLC. FreeOTP Authenticator is a trademark of Red Hat, Inc. in the United States and other countries. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark. Avigilon Corporation protects its innovations with patents issued in the United States of America and other jurisdictions worldwide (see **avigilon.com/patents**). Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Avigilon Corporation or its licensors.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

PDF-CLIENT6-E-H

Revision: 3 - EN

20191210

Table of Contents

What is the Avigilon Control Center Client? 1
System Requirements 1
Avigilon Certified Solution 1
ACC™ Client Software Requirements 1
Updating the Help Files 2
For More Information 2
Technical Support 2
Upgrades 2
Feedback 2
Getting Started 3
Starting Up and Shutting Down 3
Starting Up the Client Software 3
Shutting Down the Client Software 3
Logging In to and Out of a Site 3
Logging In 4
Logging Out 4
Changing the Administrator Password 5
Navigating the Client 5
Application Window Features 6
System Explorer Icons 7
Initial System Setup 8
System Administration 9
Monitoring Site Health 9
General Information: 10
Network Adapters: 11
Hard Drives: 12
Power Supplies: 12
Cooling Devices: 12
Temperature Probes: 13
Devices: 13
Managing User Connections 14
Accessing the Setup Tab 14
Site Settings 14
Naming a Site 15
Corporate Hierarchy 15

Managing Users and Groups Across Multiple Sites 15
Best Practices 16
Setting Up a Corporate Hierarchy 16
Ranks 17
Unranked Groups 18
Deleted Ranks 18
Ranked Site Families 19
Managing Servers in a Site 19
Connecting Servers to Sites 19
Disconnecting a Server from a Site 20
Connecting Site Families 21
Disconnecting Site Families 22
Upgrading Servers in a Site 22
Removing an Upgrade Installer 23
Connecting/Disconnecting Cameras and Devices 24
Discovering a Device 24
Connecting a Device to a Server 25
Editing the Device Connection to a Server 27
Failover Connections 27
Setting Up a Failover Connection 28
Example 28
Disconnecting a Device from a Server 31
Upgrading Camera Firmware 31
Replacing a Device 32
Adding an ACM™ Appliance to Your Site 33
Before Adding ACM to ACC 33
Connecting ACC to an ACM Appliance 35
Linking Doors to Cameras 35
Adding a Rule for an ACM Appliance Event 36
Users and Groups 37
Adding a User 37
Editing and Deleting a User 38
Adding Groups 39
Editing and Deleting a Group 40
Importing Active Directory Groups and Users 41
Enabling the Active Directory 41
Importing a Group 42
Importing a User 42

Assigning an Imported User to a Group 42
Importing ACM Roles 43
External Notifications 44
Setting Up the Email Server 44
Configuring Email Notifications 44
Editing and Deleting an Email Notification 45
Central Station Monitoring 46
Enabling Central Station Monitoring 46
Configuring Notification Options 46
Create Central Station Monitoring Rules 47
License Plate Recognition 48
Adding a Watch List 48
Editing a Watch List 49
Exporting a Watch List 50
Deleting a Watch List 50
Alarms 50
Adding a New Alarm 50
Editing and Deleting Alarms 53
Rules 53
Adding a Rule 53
Editing and Deleting a Rule 54
Licensing the Site 54
Activating a License 55
Deactivating a License 55
Reactivating a License 56
Automatic Licensing 56
Manual Licensing 57
Backing Up System Settings 58
Restoring System Settings 59
Scheduling Site Events 61
Server Settings 62
Naming a Server 62
Recording Schedule 62
Adding and Editing a Recording Schedule Template 63
Editing and Deleting a Template 63
Setting Up a Weekly Recording Schedule 64
Recording and Bandwidth 64
POS Transactions 65

Adding a POS Transaction Source 66
Adding a Transaction Source Data Format 66
Adding a Transaction Exception 68
Editing and Deleting a POS Transaction Source 69
Setting Up License Plate Recognition 69
Storage Management 70
Enabling Continuous Archive 70
Resetting Continuous Archive 72
Archiving Recorded Video On Demand 72
Enabling Server-Based Analytics 73
Enabling the Avigilon Appearance Search™ Feature 73
Device Settings 74
General 74
Setting a Device's Identity 74
Analytics Mode 75
Enabling an Analytics Mode 75
Configuring PTZ 76
Changing the Camera Operating Priority 77
Rebooting a Device 77
Network 78
Image and Display 78
Changing Image and Display Settings 79
Zooming and Focusing the Camera Lens 81
Measuring Pixels in the Field of View 82
Dewarping a Fisheye Lens 83
Configuring Infrared LEDs 83
Compression and Image Rate 84
Manually Adjusting Recorded Video Streams 85
Enabling Idle Scene Mode 86
Enabling HDSM SmartCodec™ Technology Settings 87
Image Dimensions 88
Teach By Example 88
Teach By Example Recommendations 89
Assigning Teach Markers 89
Managing Teach Markers 90
Applying Teach Markers to the Device 90
Removing Teach Markers from the Device 91
Viewing Teach Marker Status 91

Analytic Events 92
Adding Video Analytics Events 92
Editing and Deleting Video Analytics Events 93
Privacy Zones 93
Adding a Privacy Zone 94
Editing and Deleting a Privacy Zone 94
Manual Recording 94
Analytics Settings 95
Configuring Classified Object Detection 95
Enabling or Disabling Video Analytics Display 97
Enabling Video Analytics Display 97
Disabling Video Analytics Display 97
Self-Learning on Video Analytics Devices 98
Progress Bar 98
Resetting the Learning Progress 98
Unusual Motion Learning Progress 99
Resetting the Learning Progress 99
Configuring Rialto™ Video Analytics Appliances 100
Configuring Avigilon Presence Detector™ Sensors 101
Motion Detection 102
Setting Up Pixel Motion Detection 102
Setting Up Classified Object Motion Detection 104
Configuring the Video Intercom 106
Authorizing ACC Operators to Answer the Video Intercom 106
Recording Video When the Call Button is Active 107
Digital Inputs and Outputs 108
Setting Up Digital Inputs 108
Setting Up Digital Outputs 109
Configuring Standby Mode 109
Microphone 110
Speaker 111
Application Preferences 112
General Settings 112
Video Display Settings 113
Displaying Analog Video in Deinterlaced Mode 113
Displaying Logical IDs 113
Displaying Device Preview 113
Changing Display Quality 114
Changing Display Adjustment Settings 114

Overlay Settings 114
Displaying Image Overlays 115
Joystick Settings 116
Configuring an Avigilon USB Professional Joystick Keyboard For Left-Hand Use 116
Configuring a Standard USB Joystick 116
Discovering Sites 117
Managing Site Logs 117
Live Monitoring 119
Organizing Views 119
Adding and Removing a View 119
View Layouts 120
Selecting a Layout for a View 120
Editing a View Layout 120
Making a View Full Screen 121
Ending Full Screen Mode 121
Cycling Through Views 121
Saved Views 121
Saving a New View 121
Opening a Saved View 122
Editing a Saved View 122
Renaming a Saved View 122
Deleting a Saved View 122
Collaborating 122
Sharing a View 123
Leaving a Shared View 123
Virtual Matrix 123
Controlling Virtual Matrix Monitors 123
Editing Virtual Matrix Monitors 124
Controlling Live Video 124
Adding and Removing Cameras in a View 124
Adding a Camera to a View 124
Removing a Camera from a View 125
Viewing Live and Recorded Video 125
Cycling Through Cameras 125
Standby Mode 126
Zooming and Panning in a Video 126
Using the Zoom Tools 126
Using the Pan Tools 126

Maximizing and Restoring an Image Panel 126
Maximizing an Image Panel 126
Restoring an Image Panel 126
Making Image Panel Display Adjustments 127
Using Digital Defog 127
Changing Day/Night Mode 128
Listening to Audio in a View 128
Broadcasting Audio in a View 128
Using Instant Replay 129
PTZ Cameras 129
Controlling PTZ Cameras 129
Programming PTZ Tours 132
Triggering Manual Recording 133
Camera Recording States 133
Starting and Stopping Manual Recording 133
Triggering Digital Outputs 133
Answering a Video Intercom Call 134
Answering a Call 134
Ending a Call 135
Ignoring a Call 135
Granting Door Access 135
Identity Verification 135
Monitoring Door Access 136
Monitoring Live POS Transactions 136
Triggering Custom Keyboard Commands 136
Working with Maps 137
Adding a Map 137
Using a Map 139
Editing and Deleting a Map 141
Working with Web Pages 141
Adding a Web Page 141
Using a Web Page 141
Editing and Deleting a Web Page 142
Monitoring License Plates 142
License Plate Overlay 142
Reviewing License Plate Matches 142
Investigating Events 144
Controlling Recorded Video 144

Adding and Removing Cameras in a View 144
Adding a Camera to a View 144
Removing a Camera from a View 144
Viewing Live and Recorded Video 144
Requesting Dual Authorization 145
Playing Recorded Video with the Timeline 145
Using the Timeline 146
Viewing Unusual Motion Events 147
Filtering Unusual Motion Events 148
Synchronizing Recorded Video Playback 148
Enabling Synchronized Recorded Video Playback 148
Disabling Synchronized Recorded Video Playback 149
Initiating a Search 149
Bookmarking Recorded Video 149
Adding a Bookmark 149
Exporting, Editing, or Deleting a Bookmark 150
Zooming and Panning in a Video 150
Using the Zoom Tools 150
Using the Pan Tools 150
Maximizing and Restoring an Image Panel 150
Maximizing an Image Panel 150
Restoring an Image Panel 151
Making Image Panel Display Adjustments 151
Listening to Audio in a View 151
Reviewing Recorded POS Transactions 152
Triggering Custom Keyboard Commands 152
Monitoring Alarms 152
Accessing the Alarms Tab 152
Reviewing Alarms 153
Reviewing Alarm Video 153
Acknowledging an Alarm 153
Assigning an Alarm 154
Bookmarking an Alarm 154
Purging an Alarm 154
Searching Alarms 154
Exporting Alarms 154
Arming Image Panels 154
Search 156

Avigilon Appearance Search Query 156
Initiating a Search 156
Searching by Description 156
Searching Recorded Video 157
Reviewing Search Results 158
Reference Images 158
Using the Search Results Graph 159
Sorting Search Results 159
Reviewing Search Result Video 159
Changing Sites or Cameras 160
Restarting a Search 160
Refining Search Results 160
Removing Search Results 161
Bookmarking Search Results 161
Bookmarking Starred Results 161
Bookmarking Selected Results 162
Exporting Search Results 162
Exporting Starred Results 162
Blurring Exports 162
Exporting Selected Results 163
Identity Search 163
Performing an Identity Search 163
Reviewing Search Results 164
Reviewing Search Result Video 164
Starting an Avigilon Appearance Search Query 164
Changing Doors 165
Changing the Time Range 165
Bookmarking Search Results 165
Exporting Search Results 165
Performing a Motion Search 166
Viewing Search Results 167
Performing an Event Search 167
Viewing Search Results 168
Performing a License Plate Search 168
Viewing Search Results 169
Performing a Thumbnail Search 169
Viewing Search Results 170
Performing Text Source Transactions Search 170

Viewing Search Results 171
Performing an Alarm Search 171
Viewing Search Results 172
Performing a Bookmark Search 172
Viewing Search Results 172
Managing Multiple Bookmarks 173
Export 173
Exporting a Snapshot of an Image 173
Exporting Native Video 175
Exporting AVI Video 177
Exporting Still Images 179
Exporting a Print Image 180
Exporting WAV Audio 181
Appendix 182
Detailed Feature Descriptions 182
Email Notification Trigger Descriptions 182
Group Permission Descriptions 183
Video Analytics Event Descriptions 186
Rule Event and Action Descriptions 189
Rule Events 189
Rule Actions 195
Rule Conditions 197
Alarm Trigger Source Descriptions 197
Updating the ACC Client Software 198
Supported License Plates 199
License Plates Supported by LPR6 199
License Plates Supported by LPR5 199
Reporting Bugs 201
Keyboard Commands 201
Image Panel & Camera Commands 201
View Tab Commands 203
View Layout Commands 204
Playback Commands 205
PTZ Commands (Digital and Mechanical) 206

What is the Avigilon Control Center Client?

The Avigilon Control Center (ACC) Client software works with the Avigilon Control Center Server software to give you access and control of your surveillance system.

The Client software allows you to view live and recorded video, monitor events, and control user access to the Avigilon Control Center system. The Client software also gives you the ability to configure your surveillance system.

The Client software can run on the same computer as the Server software, or run on a remote computer that connects to the site through a local area network (LAN) or a wide area network (WAN).

What you can do in the Client software depends on the Server software edition. There are three editions of the Server software available: Core, Standard and Enterprise. Visit the Avigilon website for an overview of the features available in each edition: **http://avigilon.com/products/video-surveillance/avigilon-control-center/editions/**.

System Requirements

Avigilon Certified Solution

- 2 Monitor or 4 Monitor Professional High Performance Remote Monitoring Workstation
  - Preloaded with ACC Client software.
  - Supports high resolution monitors.
  - Includes the adapters and accessories for quick deployment.
  - Includes Avigilon warranty and support.

ACC™ Client Software Requirements

System Requirement	Minimum requirements	Recommended requirements
Monitor resolution	1280 x 1024	1920 x 1200
OS*	Windows 7 (32-bit or 64-bit), Windows 8.1 (32-bit or 64-bit) or Windows 10 (32-bit or 64-bit), Microsoft .NET Framework 6.4.2	Windows 10 (64-bit)
CPU	Intel® dual-core CPU (2.0 GHz)	Intel® Core™ i5 (Quad-core, 3.3 GHz)
System RAM	4 GB DDR3	8 GB DDR4
Video card	PCI Express, DirectX 10.0 compliant with 256 MB RAM	NVIDIA Quadro® K620
Network card	1 Gbps	1 Gbps
Hard disk space	500 MB	500 MB

* For all Windows versions, it is recommended that the latest Microsoft service pack be deployed.

Updating the Help Files

The help files for the Avigilon Control Center Client software and Virtual Matrix software are stored with the Avigilon Control Center Server application.

If one of these components is updated before the others, the help files may be out of date or describe features that are not currently supported by your system.

- If the help files describe a new feature that is not currently supported by your copy of the software, upgrade to the latest version of the software.
- If the help files are out of date, download the latest help files from the Avigilon website: **avigilon.com**. Once downloaded, run the help installer on the server.

  The help file installers are divided into the following regional language packs:

  - Americas
    - English
    - French
    - Spanish
  - Asia
    - Japanese
  - Western Europe
    - Dutch
    - French
    - German
    - Italian
    - Spanish
  - Middle East
    - Arabic

For More Information

Visit Avigilon at **avigilon.com** for additional product documentation.

Technical Support

To contact Avigilon Technical Support, go to **avigilon.com/contact-us**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check for available upgrades at: **avigilon.com/support-and-downloads**.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**.

Getting Started

Once the Avigilon Control Center Client software has been installed, you can start using the High Definition Stream Management (HDSM)™ technology surveillance system immediately. Refer to any of the procedures in this section to help you get started.

Starting Up and Shutting Down

The Avigilon Control Center Client software can be started or shut down at anytime — video recording is not affected because it is controlled separately by the Server software.

Starting Up the Client Software

Perform one of the following:

- In the Start menu, select **All Programs** or **All Apps** > **Avigilon** > **Avigilon Control Center Client**.
- Double-click  or  desktop shortcut icon.
- From the Avigilon Control Center Admin Tool, click **Launch Control Center Client**. For more information, see the *Avigilon Control Center Server User Guide*.

When you are prompted, log in to your site. You can only access cameras and video after you log in.

For more information, see *Logging In to and Out of a Site* below.

Shutting Down the Client Software

1. In the top-right corner of the Client software, select  > **Exit**.
2. When the confirmation dialog box appears, click **Yes**.

Logging In to and Out of a Site

To access any of the features in your ACC surveillance system, you must log in to a site.

The default administrator access uses `administrator` as the username and no password. If this is the first time you are logging into the system, you will be prompted to enter a new password. For more information, see *Changing the Administrator Password* on page 5.

Logging In

1. Open the Site Login tab. The Site Login tab is automatically displayed if you are launching the Client software for the first time.

   To manually access the Site Login tab, do one of the following:

   - From the top-right corner of the window, select > **Log In...**.
   - From the top-left corner of the application window, click to open the New Task menu, then click .

2. On the left side of the Site Login tab, select one or more sites.

   If the site you want to log into is not shown, click **Find Site...** to discover the site.

3. Enter your username and password for the selected sites.

   Or, select the **Use current Windows credentials** check box to automatically use the same username and password as your computer.

   NOTE: If you are unable to login using your current Windows credentials, your system may be using Kerberos as a network authentication protocol. Contact your network administrator for help.

4. Click **Log In**.
5. If Two-Factor Authentication is required, a dialog box is displayed.
   a. The first time you log in, a QR code is displayed. On your mobile device, scan the QR code with a TOTP authenticator app like the Google Authenticator™ mobile app or the FreeOTP Authenticator™ mobile app. If you cannot scan the QR code, enter the 20-character key into the authenticator app.

      The authenticator app will display a 6-character verification code.

   b. The next time you log in, use the authenticator app to get your verification code.
   c. Enter the code in the **Verification Code:** box.

      Tip: Select the **Trust this device for 30 days** check box to avoid entering a verification code each time you log in.

   d. Click **OK**.

   You are logged in to the selected sites.

If you want to be notified when new or disconnected sites come online, select the **Notify me when additional sites become available** check box.

If you want to see the login page each time you launch the Client software, select the **Show this tab on startup** check box. If you prefer not to login each time, you can disable this option and configure automatic login from the Client Settings dialog box.

Logging Out

You can log out of one or all sites at any time.

To...	Do this...
Log out of one or select sites	• In the System Explorer, select one or more sites then right-click and select **Log Out**.
Log out of all sites	1. In the top-right corner of the Client, select > **Log Out**. 2. In the confirmation dialog box, click **Yes**.

Changing the Administrator Password

After you login with the default administrator credentials for the first time, you are immediately prompted to change the password.

1. After you login, the Change Password dialog is displayed.
2. Enter a new password and then confirm the new password.

   The password must meet the minimum strength requirements.

   - — password meets the strength requirements.
   - — password does not meet the strength requirements, enter a new password.

   The password strength is defined by how easy it is for an unauthorized user to guess. If your password does not meet the strength requirements, try entering a series of words that is easy for you to remember but difficult for others to guess.
3. Click **OK**.

Tip: If you forget the administrator password, resetting the password is difficult and impacts every server in the site. To avoid this issue, it is highly recommended that you create at least one other administrator level user as a backup.

Navigating the Client

Once you log in, the Avigilon Control Center Client application window is populated with all the features that are available to you.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

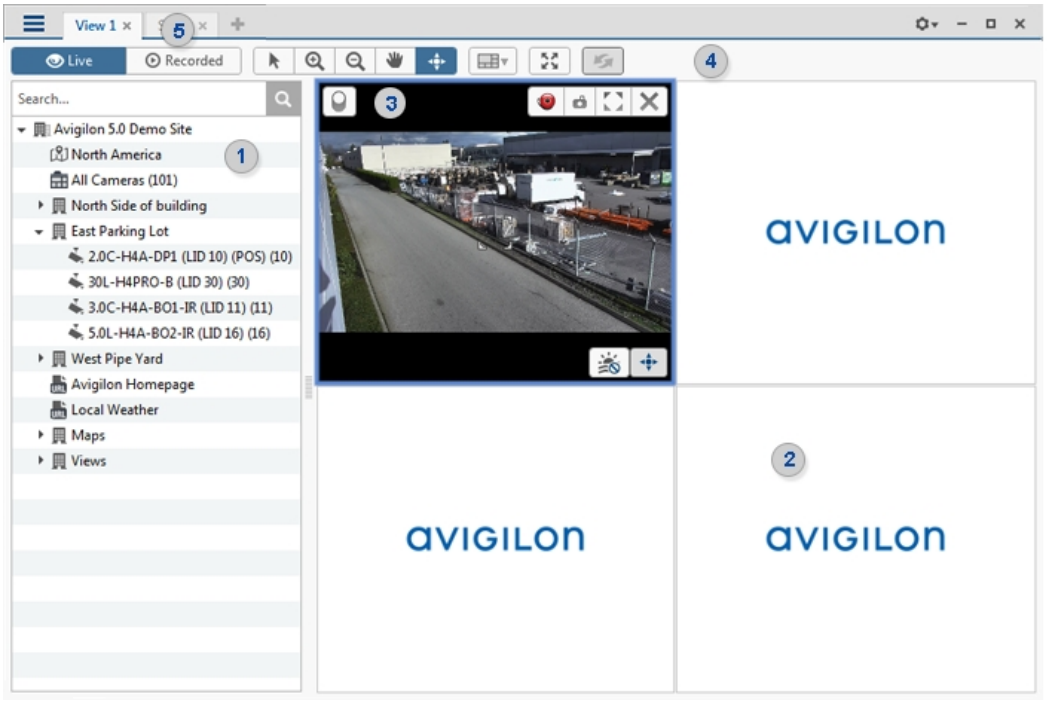


Figure 1: The Avigilon Control Center Client application window

Application Window Features

	Area	Description
1	System Explorer	Displays all the elements in your surveillance system. Use the **Search...** bar to quickly locate anything that is available in the System Explorer. You can search for items by name, and devices can also be searched for by location, logical ID, serial number and IP address. **Tip:** The content of the System Explorer changes depending on the tab you have open. For example, servers are not listed in the View tab.
2	View tab	Allows you to monitor video and organize image panels. You can have multiple Views open at once. Click + to open a new View tab.
3	Image panel	Displays live or recorded video from a camera. The video control buttons are displayed when you move your mouse into the image panel.
4	Toolbar	Provides quick access to commonly used tools.
5	Task tabs	Displays all the tabs that are currently open.
☰	New Task menu	Opens the New Task menu so you can select and open new task tabs. You can access advanced tools like Search and Export, or system administrative features like Site Setup.

	Area	Description
	The Application Menu menu	This menu gives you access to local application settings like Client Settings. You can also open a new window from this menu.
	System message list	The highlighted number shows the number of system messages that need your attention. Click the number to display the list of messages. The highlight color indicates the severity of the most recent message. • **Red** = Error • **Yellow** = Warning • **Green** = Information

System Explorer Icons

Icon	Description
	A site. Listed under a site are all the connected devices and linked features in the system.
	A virtual folder. Used to group and organize items in the View tab.
	A server. Only visible from system administration tabs and dialogs.
	A fixed camera.
	A PTZ camera.
	An Avigilon Presence Detector sensor.
	An encoder.
	An Access Control Manager (ACM) appliance. Only visible when an ACM appliance is connected to a site.
	An ACM panel.
	An ACM subpanel.
	An ACM input.
	An analytic channel (requires a Rialto device).
	A Virtual Matrix monitor.
	A saved View.

Icon	Description
	A map.
	A web page.

Initial System Setup

To ensure that you have set up the ACC system correctly, it is highly recommended that you review and complete the recommended procedures in the *Initial ACC™ System Setup and Workflow Guide*. The guide is available on the Avigilon website: **avigilon.com/support-and-downloads/**.

System Administration

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

In Avigilon Control Center software, servers are maintained in clusters called sites. Each site can contain multiple ACC servers that share configuration settings across the entire site. Optionally, a site can also connect to a single Access Control Manager™ appliance.

At the site level, you can manage your server and device connections, as well as set up site-wide system events.

At the server level, you can manage the recording and bandwidth for each of the server's connected cameras.

At the device level, you can edit the camera image quality and other device-specific features.

All the site, server and device settings can be configured from the Setup tab.

Monitoring Site Health

To help you monitor the health of your site, you can access a quick overview in the Site Health tab.

1. In the New Task menu, click .

   The Site Health tab is displayed.

2. In the System Explorer, select a site.

   The status of the connected servers and appliances is displayed.

If your sites are configured into a family, you will be able to see the status of all child sites if you are logged into the parent site. If you are only logged into a child site, the parent site status is displayed as unknown.

The following status icons identify the status of each component in the ACC software:

 The component is functioning normally.

 The component requires your attention.

 The component is unavailable or offline.

 The component status is unknown.

The status icons beside each site name identifies the overall health of the site.

By default, all server and appliance information is displayed.

To view a specific server in a site:

- In the search bar, enter the name of the server.

  Servers matching the description are displayed.

To show or hide the information displayed:

- Below the Site Information: box, click an icon to show or hide:

  - General information about your server or appliance.
  - Network adapter information.
  - Server hardware information.
  - Device information.
  - Access Control Manager appliance information.
  - Information about servers with warnings and errors.

  The selected information is displayed or hidden.

To export a report:

1. In the bottom-right corner, click **Export Site Report to PDF**.
2. Enter a report name and select a file location.

   A PDF report is downloaded.

Site Information:

At the top of the tab are details about the site. This information is not displayed if the ACC ES HD Recorder or ACC ES Analytics Appliance is functioning as an independent site.

Name	Description
License Id:	The site identifier used in the Avigilon licensing server.
Site License Usage:	The number of connected cameras over the total number of licenses available in the site. For example, 3/16 would indicate the site currently has 3 camera connections but is licensed for 16. **NOTE:** Cameras connected directly to an ACC ES HD Recorder or ACC ES Analytics Appliance are not listed in this count.

Server Name

At the top of each pane is the name of the individual server in the site. Beside the name is the server status.

General Information:

Information about the server in the site.

Name	Description
Server Version:	The ACC Server version number.
Server IP:	The server's IP address.

Name	Description
Model Name:	The server's model name. Only available if the server's SNMP service is enabled.
System Name:	The server's user-configurable name. Only available if the server's SNMP service is enabled.
Service Tag:	The server's service tag. Only available if the server's SNMP service is enabled.
CPU Load:	The percentage of server processing power that is used by the ACC Server software.
Memory usage:	The amount of memory used by the ACC Server software.
System Available Memory:	The amount of storage available for video recording.
Up Time:	The amount of time the server has been running since it was last rebooted.
Server License Usage:	The number of cameras currently connected to the server over the total number of licenses available in the site. **NOTE:** Devices that do not generate video streams do not use camera licenses.
LPR Service:	An icon displays the LPR service status: ✔ The LPR service is running correctly. ✖ The LPR service is unavailable.
Analytics Service:	An icon displays the ACC Analytics Service status: ✔ The ACC Analytics Service is online. ⚠ The ACC Analytics Service was overloaded at some point in the last 3 days. Reduce the Total Appearance Search Load by disabling the Avigilon Appearance Search feature on some cameras. ✖ The ACC Analytics Service is offline.
Peak Load (Last 3 Days):	The highest percent usage of the analytics service over the last 3 days.

Network Adapters:

The networks that the server is connected to, including the IP address of the network connection, the network speed and the amount of data passing through the connection.

Name	Description
Adapter Name	The name of the network adapter that is connected to the server.
Status	The operational status of the network adapter. Only available for Windows servers running ACC Server version 6.14 or later.
Link Speed	The maximum speed supported by the network adapter.
IP	The IP address of the network adapter. Appears empty for netowrk adapters that are

Name	Description
	disconnected.
Incoming	The speed of incoming data. This includes recording video.
Outgoing	The speed of outgoing data. This includes video streaming to the Client software.

Hard Drives:

Information about each hard drive in the server, including the serial number, status, and alerts. Only available if the server's SNMP service is enabled.

Name	Description
Disk Name	The hard disk name.
Product ID	The hard disk product number.
Serial No	The hard disk serial number.
State	The physical state of the hard disk.
Rollup Status	The overall (worst) status of the hard disk. Statuses include: • Other • Unknown • OK • Non-critical • Critical • Non-recoverable
SMART Alert	If there is a Self-Monitoring, Analysis, and Reporting Technology (SMART) Alert for the disk reliability or imminent failure, it will appear in this column.

Power Supplies:

Information about the server's power supply, including the location, power supply type, and state. Only available if the server's SNMP service is enabled.

Name	Description
Location Name	The power supply location in the chassis.
Status	The power supply status.
Type	The power supply type.
Sensor State	Additional information about the power supply provided by the sensor..

Cooling Devices:

Information about the server's cooling devices, including the location, status, and type. Only available if the server's SNMP service is enabled.

Name	Description
Location Name	The cooling device location in the chassis.
Status	The cooling device status.
Type	The cooling device type.
State Settings	The cooling device state.

Temperature Probes:

Information about the server's temperature probes, including information about the probe's location, status, and type. Only available if the server's SNMP service is enabled.

Name	Description
Location Name	The temperature probe location in the chassis.
Status	The temperature probe status.
Type	The temperature probe type.
State Settings	The temperature probe state.

Devices:

Information about the devices that are connected to this server.

NOTE: If the device is disconnected, the device's details may still be displayed but the Compression column will be empty because there is no video streaming.

Name	Description
General	The name, model number and location of the device. An icon displays the device connection status: ✔ The device is connected. ⚠ The device has disconnected for less than 5 minutes. ✖ The device has disconnected for more than 5 minutes.
Network	The IP and MAC addresses of the device.
Hardware	The serial number of the device.
Compression	The video compression rate, resolution, quality and images per second (ips) of video streamed from the device.
Retained Video	The age of the oldest recorded video that is not bookmarked with a protected bookmark.

Access Control Manager Appliance

Information about the Access Control Manager (ACM) appliance that is connected to this site.

Feature	Description
Appliance Name:	The name of the ACM appliance.
IP:	The IP address of the ACM appliance.

Managing User Connections

If you find that too many users are logged in through the same username, or inactive users are preventing active users from accessing a site, you can force specific users to log out.

1. In the New Task menu, click . The User Connections tab is displayed.
2. Select a site from the System Explorer to display a list of all the current users on the right.
    - The users are listed by User Name and Machine Name so that users that share a login are displayed separately.
    - The Login Duration column lets you know how long that user has been logged in to the site.
3. To force a user to log out of a site, select a user then click **Log Users Out**.

Accessing the Setup Tab

The Setup tab is where you configure your system.

In the Setup tab, the System Explorer is displayed on the left and the settings are displayed on the right. The Setup options change depending on the site, server, or device that is selected in the System Explorer.

To open the Setup tab, do one of the following:

- At the top-left corner of the application window, click  to open the New Task menu and then click  **Site Setup**.
- In the System Explorer, right-click the site or device you want to configure and then click **Setup**.

  NOTE: Server settings are only available after the site or device Setup tab is open. In the System Explorer, select the server you want to configure.

Site Settings

The settings stored at the site level impact all users and devices within the site.

These settings include user account information and email notifications. This is also where you can set up how the System Explorer is laid out, and where you can add or remove devices in a site.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Naming a Site

Give the site a meaningful name so that it can be easily identified in the System Explorer. Otherwise, the site uses the name assigned to the server it was originally discovered with.



1. In the site Setup tab, click .
2. In the following dialog box, enter a name for the site.
3. Click **OK**.

Corporate Hierarchy

You can set up a Corporate Hierarchy in the system to reflect your organization's structure.

Groups are given ranks to help define what they have access to. Users cannot see groups of equal or higher rank than the group they belong to. If users belong to multiple groups of different ranks, they will be able to view all ranks below the highest rank they belong to.

Sites can also be connected together, into families, and given ranks in the Corporate Hierarchy. This further defines what devices and events users can control.

Managing Users and Groups Across Multiple Sites

When you have a large organization, you need detailed user access permissions to manage how the system is used each day.

The Avigilon Control Center system offers several features to help you manage large organizations:

- **Active Directory Support:** The system can synchronize with Windows Active Directory to quickly import large number of users. For more information, see *Importing Active Directory Groups and Users* on page 41.
- **Group Privileges:** Users must be added to at least one group that defines what they can access within the system. This includes system features and specific devices. Only users with **Setup user and group settings** permission are able to edit other users and groups at all. For more information, see *Adding Groups* on page 39.

  To help you manage groups across the system, here are some features to help you maintain secure group access:

  - **Corporate Hierarchy:** Create a Corporate Hierarchy to determine which groups have control over other groups. For more information, see *Corporate Hierarchy* above.
  - **Site Families:** You can connect multiple child sites to an Enterprise parent site. You can then control group settings for all of the sites from the parent site. For more information, see *Connecting Site Families* on page 21.

Best Practices

Listed here are some recommendations for maintaining an efficient and secure system:

- Use a strong administrator password. The default administrator user has control over all aspects of the system, so adding a strong password to the account is highly recommended.
- Create a secondary user for the Administrator group. It is recommended that you do not use the default administrator user account, instead create a secondary user account with the same privileges so that the default administrator user can still be used in the rare event that the system becomes compromised.

Tip: If you forget your administrator user password, the alternate administrator user can be used to reset the password. This will avoid the need for a system-wide reset to restore the default administrator user password.

- Assign a rank to all groups. Unranked groups have access over all other groups, so it is recommended that any groups with users be assigned a rank to further define their access privileges. The default Administrators group is Unranked by default, but you can create a new group with same permissions and assign a rank to the new group. For more information, see *Corporate Hierarchy* on the previous page.
- Limit the number of users in the default Administrator group. The Administrator group is the oversight group that should only be used for system maintenance. For example, users in the default Administrator group are the only ones who can see or remove private bookmarks made by all users.
- Always check that the device access permissions are correct after a child site has been connected to a parent site. Ranked groups from the parent site whose rank is above or equal to the child site retain their permissions on the child site. These groups automatically gain access to all devices, maps, saved Views, and web pages on the child site.
- Always check group access permissions after a new server has been merged into the site.
    - If groups have the same name, the site settings are used and the users from both the site and the server are added to the group.
    - Groups that are new to the site automatically get access to all the devices in the site.
    - Groups that are new to the server automatically get access to all the devices that are connected to the server.
- Always check group access permissions after new users and groups settings are imported into the site.
    - If groups have the same name, the import settings are used and the users from both the import file and the current site are added to the group.
    - Groups added from the import file automatically gain access to all the new devices that were added since the settings were exported.

Setting Up a Corporate Hierarchy

Corporate hierarchy is set up by assigning ranks to different access permission groups. This includes user permission groups and sites that are organized into families. For more information about ranks, see *Ranks* on the next page.

You can assign ranks to permission groups through the Users and Groups dialog box. For more information about adding groups, see *Adding Groups* on page 39.

You can assign ranks to sites when they are organized into families. For more information about site families, see *Connecting Site Families* on page 21.

When you see the **Rank** option, you can select an existing rank or create a new one.

- To use an existing rank, select an option from the drop-down list. The default option is *Unranked*.
- To add a rank, click  . When you see the Edit Corporate Hierarchy dialog box, complete the following steps:

  If you have not yet created a Corporate Hierarchy, a message will appear prompting you to create a new one. Click **Yes**.

  The default rank is **Global**. It is the highest rank in the Corporate Hierarchy.

  NOTE: The Global rank cannot be deleted. It can only be renamed.

  1. Select **Global** then click . A new rank is added.
  2. To rename the rank, double-click the name and enter a new one in the text field. Click anywhere outside the text field to save the new name.
  3. Select a rank then click  to add a new rank immediately below the rank you selected.

     NOTE: Ranks can only be added or deleted. They cannot be moved within the Corporate Hierarchy.

  4. To delete a rank, select the rank then click . All subordinate ranks will also be deleted.

     NOTE: Make sure there are no members in the rank before you delete it. Members of a deleted rank are automatically assigned the lowest position in the Corporate Hierarchy and may lose required permissions.

  5. Click **OK** to save your changes.

Now that you've set up the Corporate Hierarchy, you can assign ranks to permission groups to define what users can access within the system. For more information, see *Users and Groups* on page 37.

You can also organize your sites and servers to mirror their physical location or reference their relationship in the Corporate Hierarchy. For more information, see *Connecting Site Families* on page 21.

Ranks

Ranks in the Corporate Hierarchy feature represent the different levels that may exist in your organization. Each rank can have different permissions and be responsible for subordinate ranks.

The default rank is **Global**. It is the highest rank in the Corporate Hierarchy and can configure all ranks that are added below it.

When you add ranks, be aware that users assigned to a rank can only edit other ranks that are subordinate in the Corporate Hierarchy. Any ranks that are above or parallel will not be accessible.

The following image is an example of a Corporate Hierarchy with multiple ranks. **Canada** is the highest, Global rank. **West Coast** and **East Coast** are of equal rank to each other, and one rank below **Canada**. Users belonging to **East Coast** cannot edit ranks below **West Coast** and vice versa.

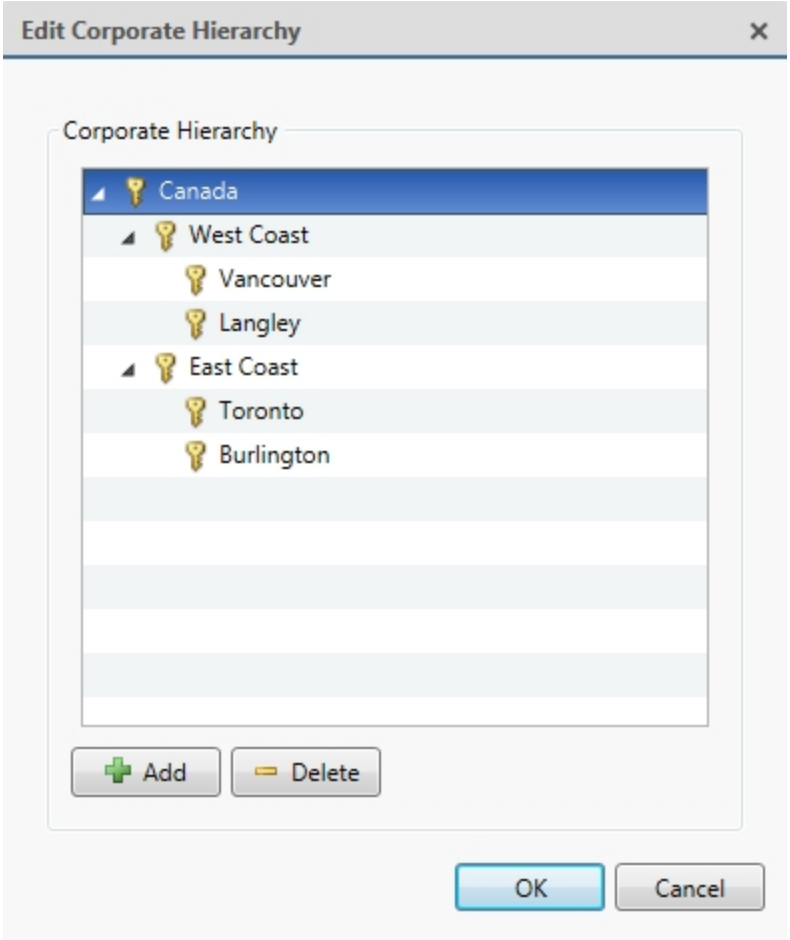


Figure 2: An example Corporate Hierarchy.

Unranked Groups

The Unranked groups are above the Corporate Hierarchy and cannot be deleted or edited.

Users belonging to Unranked groups are able to create and edit any ranked or Unranked groups and users if they have the **Setup user and group settings** privilege.

The default groups Administrators, Power Users, Restricted Users, and Standard Users are Unranked.

Deleted Ranks

If a rank is deleted, groups in this rank are removed from the hierarchy and assigned an orphaned rank. An orphaned rank is the lowest rank possible and is only visible to Unranked and Global users.

Unranked and Global users can reassign group ranks at any time. Members of the orphaned rank have no Setup user and group settings privileges but still retain other privileges, e.g. viewing live video.

Deleting a rank will also delete all the ranks below it in the Corporate Hierarchy. Remotely synchronized users and groups may become inaccessible.

Ranked Site Families

Ranks can also be applied to sites that have been organized into families. Once a site has been assigned a rank, all groups, users and device access are subject to the site's rank in the hierarchy.

The Corporate Hierarchy is configured through the parent site and the Global rank is associated with the parent site. For more information, see *Connecting Site Families* on page 21.

Managing Servers in a Site

A site can contain multiple servers to share settings and tasks across all the servers. For example, users and groups that are added to the site will automatically have access to all linked servers.

If you need users and groups to have more detailed access permissions, you can also organize each site into families to better reflect your corporate hierarchy.

By default, when a server is first discovered on the network, it is added to the System Explorer as a server in a site of the same name. You can move the server to a different site to share resources.

Tip: It is recommended that you plan how your system should be configured before you implement the features described in this section. This will help you avoid unnecessary cleanup and prepare for potential issues.

Connecting Servers to Sites

By default, each site only has one server but you can add multiple servers to a site so that they can be managed together. All servers within the site share settings and are represented as one unit in the System Explorer.

Tip: It is recommended that you only add new servers to an existing site to avoid managing a large number of duplicate settings, and more easily configure device connections across the combined site.

This procedure is primarily for grouping a number of servers in the same local area network to work together and share settings. If you're using the Avigilon Artificial Intelligence (AI) Appliance, connect the appliance to an NVR server and connect that server to your site.

If the servers are installed a wide distance apart but only need to share users and group information — you can join the sites together into a site family instead. For more information, see *Connecting Site Families* on page 21.

1. In the site Setup tab, click  .

   The Site Management tab lists all the sites that you can access and all the servers that are connected to each site.

   If you do not see the site or server you want to configure, you may need to add the site. For more information, see *Discovering Sites* on page 117.

2. When you select a  server, you will see the available options at the bottom of the application window.

3. To move a server:
    - Select the  server and drag it to a different site.
    - Or, select the  server then click **Connect to Site...** at the bottom-right corner of the tab. In the following dialog box, select the site you want the server to connect to.

    NOTE: Sites without any servers are automatically removed from the list.
4. After the server has joined the new site, reactivate the site licenses. For more information, see *Reactivating a License* on page 56.

Once the server is connected to the site, the settings are merged.

- Unique settings from the server are added to the site.
- If the settings are identical, only the site version is kept.
- If a server setting and a site setting have the same name but are configured differently, the server setting is added to the site and renamed in this format: *<setting name> (server name),* e.g. Email1 (Server2F).
    - In the rules engine, the *Notify users (default)* rule is always added and renamed, even if the settings are the same. The site version remains enabled but the added rule is disabled by default.
- The two site Views are combined.
    - The site settings take precedence.

      For example, a map from the site was copied to the server in the past. In the server, the map was placed at the top of the site View. But in the site, the same map is placed at the bottom. After the server is connected to the site, the map takes the position used by the site at the bottom.
    - New, unorganized elements from the server are listed at the bottom of the site View.
- User permission groups are merged.
    - If groups have the same name, the site settings are used and the users from both the site and the server are added to the group.
    - Groups that are new to the site automatically get access to all the devices in the site.
    - Groups that are new to the server automatically get access to all the devices that are connected to the server.
- Users with the same name will use the settings configured in the site (including passwords), and gain group permissions from the server.
- If the site is connected to a Windows Active Directory, the server must be connected to the same Active Directory domain or the connection will fail. For more information, see *Importing Active Directory Groups and Users* on page 41.

Disconnecting a Server from a Site

If the site has multiple servers, you can choose to disconnect a server from the current site and re-assign the server to its own site.

1. In the site Setup tab, click  .

   The Site Management tab lists all the sites that you can access and all the servers that are connected to each site.

2. Select a server from the site then click **Disconnect from Site...**.
3. After the server has disconnected from the site, reactivate the site licenses. For more information, see *Reactivating a License* on page 56.

When a server is disconnected, it retains all the settings it received from its previous site but becomes unlicensed.

You can purchase new licenses for the disconnected server, or you can deactivate the required licenses from the previous site and activate them on the disconnected server's own site. For more information about deactivating licenses, see *Deactivating a License* on page 55.

Connecting Site Families

Site families are sites that are connected together into a hierarchy. Sites are still managed independently, but user and group information is centrally managed by the parent site.

Child sites are connected to a parent site to create a site family. Once set up, all ranked user and group privileges on the parent site are applied to the child sites and controlled from the parent site. The child site can still define local users and groups.

For more information about the Corporate Hierarchy feature, see *Corporate Hierarchy* on page 15.

NOTE: A parent site can have multiple child sites, but a child site can only have one parent site. You must be logged in to both potential parent and child sites before you can connect them.

Only Enterprise sites can be parent sites. Each parent site can have up to 1 Core site, 24 Standard sites and unlimited Enterprise sites as child sites.

1. In the site Setup tab, click  .

   The Site Management tab is displayed.

2. Select the  site you want to connect as a child site.
3. In the bottom-right corner of the tab, click **Connect to Parent Site**.

   Tip: If you selected a  server instead of a site in the previous step, you will only have the option to Connect to Site....

4. In the following dialog box, select the parent site from the **Connect to:** drop-down list.
5. In the **Rank:** drop-down list, select a rank for the child site. To edit or view the entire Corporate Hierarchy,

click  . For more information, see *Setting Up a Corporate Hierarchy* on page 16.

6. Click **OK**.
7. In the confirmation dialog box, click **Yes**.

Disconnecting Site Families

If a child site needs to be moved or removed from the Corporate Hierarchy, you can disconnect it from the parent site. The child site can then function independently, be reconnected to the parent site or be connected to a new parent site.

Depending on your access permissions, you may only be able to perform one of the following:

- To disconnect the parent site from the child site:
    1. In the Site Management tab, select the child site you want to disconnect.
    2. In the bottom-right corner of the tab, click **Disconnect from Parent Site...**.
    3. When the confirmation dialog box appears, click **OK**.

    NOTE: If a network issue occurs while you are disconnecting the child site, you need to also revoke access from the parent site.
- To disconnect a child from the parent site:
    1. In the Site Management tab, select the parent site whose child site you want to disconnect.
    2. In the bottom-right corner of the tab, click **Disconnect Child Site...**.
    3. From the drop-down list, select the child site you want to disconnect.
    4. When the confirmation dialog box appears, click **OK**.

Upgrading Servers in a Site

NOTE: To use this feature:

- All NVR servers in the site must be running ACC Server version 5.6 or later.
- All ACC ES HD Recorders in the site must be running ACC Server version 5.8 or later.
- All Avigilon video analytics appliances in the site must be running ACC Server version 6.0 or later.

If you have multiple servers in your site, you can choose to upgrade all servers through the Client software rather than update each server manually at their physical location. This feature is especially helpful when you have an Enterprise system with up to 100 servers in a site.

Tip: To avoid losing video connection, set up failover connections before you perform an upgrade. This allows cameras to connect to a Secondary or Tertiary server when the Primary server is required to restart as part of the upgrade process. For more information, see *Failover Connections* on page 27.

Tip: After you perform each step in the Site Upgrade dialog box, you can close the dialog box and continue regular operations. Be aware that cameras will briefly disconnect from the system when the server restarts as part of the upgrade process.

1. Download the latest version of the Avigilon Control Center Server software or Avigilon video analytics appliance firmware from the Avigilon website: **avigilon.com.**
2. In the Client software, log in to the site.
3. In the site Setup tab, click  .

   The Site Upgrade dialog box is displayed. The dialog box lists all the servers that are in the site.

   If the site contains an ES camera, recorder, or an Avigilon video analytics appliance, the Platform column is displayed. The column displays the device model number to help you identify which upgrade package you should use.
4. In the top-right corner of the dialog box, click **Upload**.
5. In the Open dialog box, locate the installer that you downloaded from the Avigilon website.
6. In the Confirm Selected Installer dialog box, confirm that you've selected the correct installer then click **OK**.

   The dialog box displays the installer details in the Installer Info area and lists the servers that can be upgraded by the selected installer.

   The new installer is uploaded to one server then distributed to the other affected servers in the site. It may take several moments before the installer is fully uploaded.

   When the installer has been distributed to each server in the system, the **Upgrade** button is displayed beside the servers that can be upgraded by the new installer. The button is disabled until the installer has been distributed to all servers.
7. Click **Upgrade** beside a server.
   a. When the confirmation dialog box is displayed, click **OK** to allow the server to reboot as part of the upgrade process.

      When the server restarts, it will disappear from the list then reappear after it reconnects with the system.

      To facilitate the failover connections, it is recommended that you wait for each server to complete the upgrade process before upgrading the next server.

   b. Repeat this step for each server in the site.

Removing an Upgrade Installer

If you discover that you've uploaded the wrong installer to the site, you can choose to remove the installer before it is installed on a server.

1. In the site Setup tab, click  .
2. In the following dialog box, click **Remove**.
3. When the confirmation dialog box appears, click **OK**.

The upgrade installer is deleted from the system.

To upload a new upgrade installer to the site, see *Upgrading Servers in a Site* on page 22.

Connecting/Disconnecting Cameras and Devices

Cameras and other devices are connected to a site through the linked servers. The server manages and stores the camera's recorded video, while the site manages the events that are generated from the camera's video or by a connected device (such as an Avigilon Presence Detector sensor).

You can connect and disconnect cameras and devices through the Connect/Disconnect Devices... tab.

A connected camera or device appears with an icon next to its name in the System Explorer. When the connection to the device is not in its normal state, the connection status is indicated by an overlay on its icon. The status overlays may appear over any camera or device icon in the System Explorer. The status icons are shown in the following table.

Status Icon	
	The device is connected to the server and is currently upgrading its firmware.
	The device cannot connect to a server.
	Applies only to cameras. The camera is disconnected but recorded video from the camera remains on the server.

The status icons as they appear for a fixed camera are shown in the following table.

Icon	Definition
 **Camera Connected**	The camera is connected to the server.
 **Camera Upgrading**	The camera is connected to the server and is currently upgrading its firmware.
 **Camera Connection Error**	The camera cannot connect to a server. This may be because the camera is no longer on the network or there is a network conflict.
 **Camera Disconnected**	The camera is disconnected but recorded video from the camera remains on the server.
No Icon	The camera is disconnected and no recorded video from the camera remains on the server.

Discovering a Device

Avigilon and ONVIF® compliant devices that are connected to the same network as the Avigilon Control Center Server are automatically detected and added to the Discovered Devices list.

If a device is not automatically discovered, it may be on a different subnet or is a third party camera that needs to be manually discovered.

1. In the site Setup tab, click  .

   The Connect/Disconnect Devices... tab is displayed.

2. In the top-left corner, click **Find Device...**.
3. In the Find Device dialog box, complete the following fields to find the device:
   - **Search From Server:** select the server that you want the device to connect to.
   - **Search Type:** select a search type:
     - **IP Address** — select this option to discover a device by its IP address or hostname. The device and server's gateway IP address must be set correctly for the device to be found.
     - **IP Address Range** — select this option to discover a device by IP address range. Only devices with IP addresses in that range will be discovered.
   - **Device Type:** select the device's brand name.

     Tip: Select ONVIF to discover devices that are ONVIF compliant.
   - **Control Port:** enter the device control port. The default port number is 55080.
   - **Apply credentials to all uninitialized devices** check box — Enter the password for the administrator username, or create a username and set a new password.

     NOTE: If you forget the login credentials for an added device, refer to factory reset instructions in the device manual and repeat these steps to reset its password.
4. Click **OK**.

If the device is discovered, it is automatically added to the Discovered Devices list. You can now connect the device to a server.

Connecting a Device to a Server

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

To access a device from a site, it must be connected to a server within the site. The server manages and stores the camera's recorded video, while the site manages the events that are generated by a connected device (such as an Avigilon Presence Detector sensor) or from the camera's video .

After a device has been discovered on the network, it can be connected to the server. If you do not see a device you want to connect, see *Discovering a Device* on the previous page.

1. In the site Setup tab, click  .

   The Connect/Disconnect Devices... tab is displayed.

2. To display only devices in uninitialized state, select the **Uninitialized devices** check box. The devices are displayed in the Discovered Devices area.
3. In the Discovered Devices area, select one or more devices then click **Connect...**.

   Tip: You can also drag the device to a server on the Connected Devices list.

4. In the Connect Device dialog box, select the server you want the device to connect to.

   NOTE: If you are connecting multiple devices, all the cameras must use the same connection settings.

5. If you are connecting a third-party device, you may choose to connect the device by its native driver. In the **Device Type:** drop-down list, select the device's brand name. If there is only one option in the drop-down list, the system only supports one type of driver from the device.
6. In the **Connection Type:** drop-down list, select **Primary**. The device will automatically connect to this server if they are in the same network.

   If you are creating a failover connection, select Secondary or Tertiary.

7. In the **License Priority:** drop-down list, select the appropriate license priority. The highest priority is **1** and the lowest priority is **5**.

   NOTE: This option is only available if you are connecting to a Secondary or Tertiary server.

   The License Priority: setting decides the order that devices are connected to the server. The server will try to connect cameras with a higher priority before cameras with lower priority. If the server does not have enough camera channel licenses, low priority devices may not be connected. A camera channel license is only used when the device actually connects to the server.

8. If the camera supports a secure connection, the **Device Control:** drop-down list is displayed. Select one of the following options:

   NOTE: The setting may not be displayed if the camera only supports one of the options.

   - **Secure** — The system will protect and secure the camera's configuration and login details. This option is selected by default.
   - **Unsecure** — The camera's configuration and login details will not be secured and may be accessible to users with unauthorized access.

     Cameras with a secure connection are identified with the icon in the Status column.

9. To connect the devices to the ACC Server, enter the password for the `administrator` username, or create a username and set a new password.

   NOTE: If you forget the login credentials for a device, refer to factory reset instructions in the device manual and repeat these steps to reset its password.

10. If it is not displayed, click  to display the Site View Editor and choose where the device appears in the System Explorer.
    - In the  site directory, drag devices up and down the right pane to set where it is displayed.
    - If your site includes  folders, select a location for the device in the left pane. The right pane updates to show what is stored in that directory.
    - If you are connecting multiple devices at the same time, the selected devices must be assigned to the same location.

    Tip: If the site you want is not listed, you may need to connect the device to a different server. Make sure the selected server is connected to the site you want.
11. Click **OK**.
12. If the device is password protected, the Device Authentication dialog box appears. Enter the device's username and password, then click **OK**.

Related Tasks

Failover Connections.....27

Editing the Device Connection to a Server



1. In the site Setup tab, click .

   The Connect/Disconnect Devices... tab is displayed.
2. Select the device connections you want to edit from the Connected Devices list.
3. To edit the device connection details, click **Edit...**. For details about the editable options, see *Connecting a Device to a Server* on page 25.

   If you selected multiple cameras, only the settings that are identical are displayed.
4. To change the camera password, click **Change Password...** then enter a new password in the following dialog box.
5. If the camera has an authentication error, click **Login to Device...** then enter the correct password.
6. Click **OK**.

Failover Connections

You can set up failover connections so that if a server fails, the devices connected to it will automatically connect to a backup server and continue recording.

NOTE: Failover connections can only be made between servers within the same site.

Failover connections are set up in the Connect/Disconnect Devices... tab and are defined by the Connection Type: setting and the License Priority: setting.

The Connection Type: determines when the device will connect to a server:

- **Primary:** the device will automatically connect to this server if they are in the same network.
- **Secondary:** if the Primary server is not available, the device will try to connect to this server.
- **Tertiary:** if the Primary and Secondary servers are not available, the device will try to connect to this server.

The License Priority: setting decides the order that devices are connected to the server — **1** is the highest and **5** is the lowest. The server will try to connect devices with a higher priority before devices with lower priority. If the server does not have enough camera failover licenses, low priority devices may not be connected. A camera failover license is only used when the device actually connects to the server.

Camera failover licenses are only required for Secondary and Tertiary connections.

Setting Up a Failover Connection

1. In the Connect/Disconnect Devices... tab, select a device that is currently connected to its Primary server.
2. At the bottom of the application window, click **Connect...**.
3. When you see the Connect Device dialog box, select a different server within the same site and set the Connection Type: as either **Secondary** or **Tertiary**.
4. Select a **License Priority:** for the failover connection.
5. Click **OK**.
6. Repeat this procedure until all the required failover connections have been made.

The following is an examples of how failover will work in the event of server failure.

Example

Cameras A, B, C, D, E and F have failover connections set up to two different servers in the site. Assume the site has 6 camera channel licenses and 4 failover licenses, and the license priority is set to 1 for each connection. The camera failover licenses are only required for Secondary and Tertiary connections.



Figure 3: Primary connections

When the server NVR 1 fails, cameras A and B from NVR 1 automatically connect to their Secondary server, NVR 2.

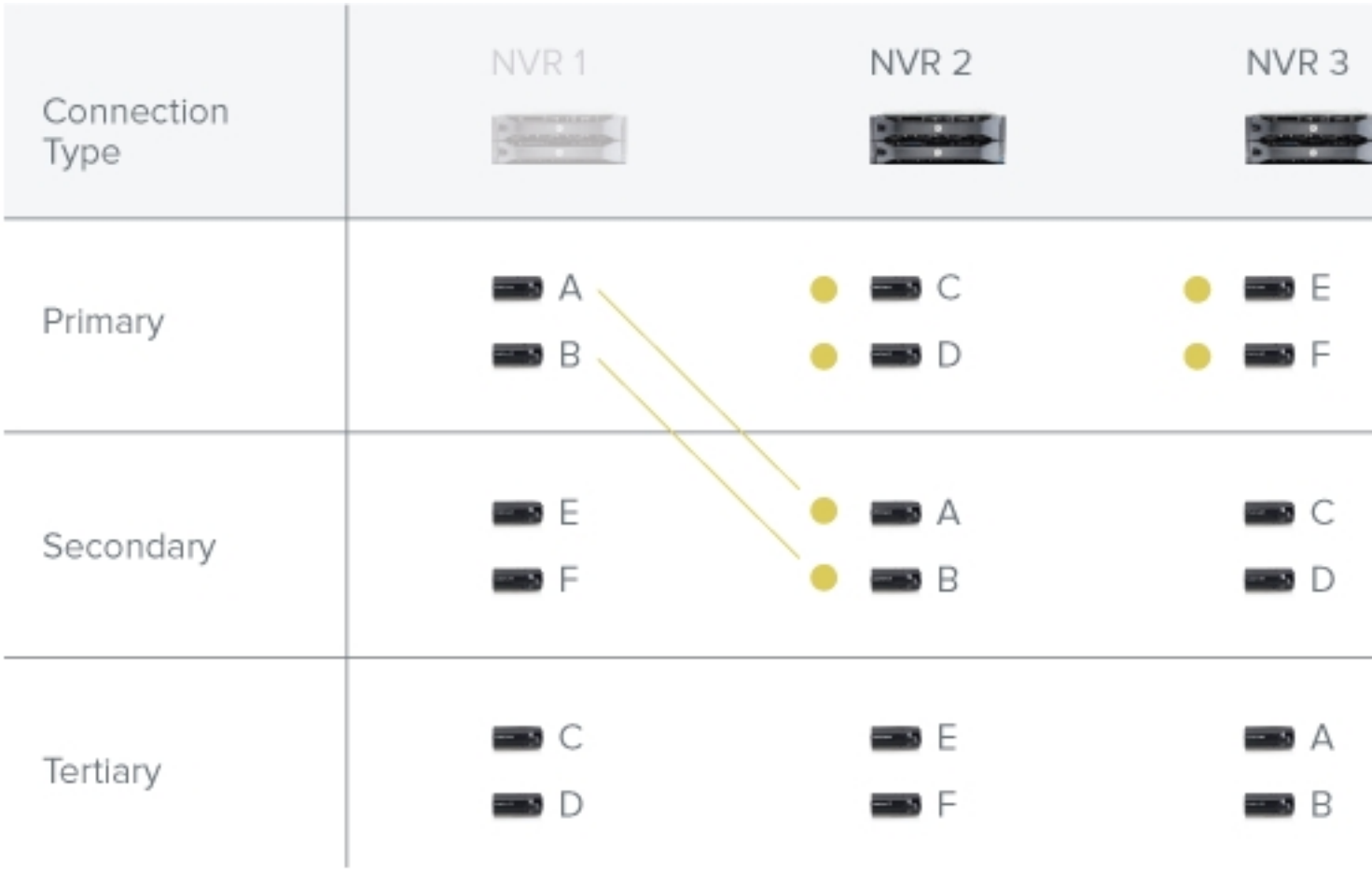


Figure 4: NVR 1 fails

When the server NVR 3 fails, cameras E and F automatically connect to their Tertiary server, NVR 2.

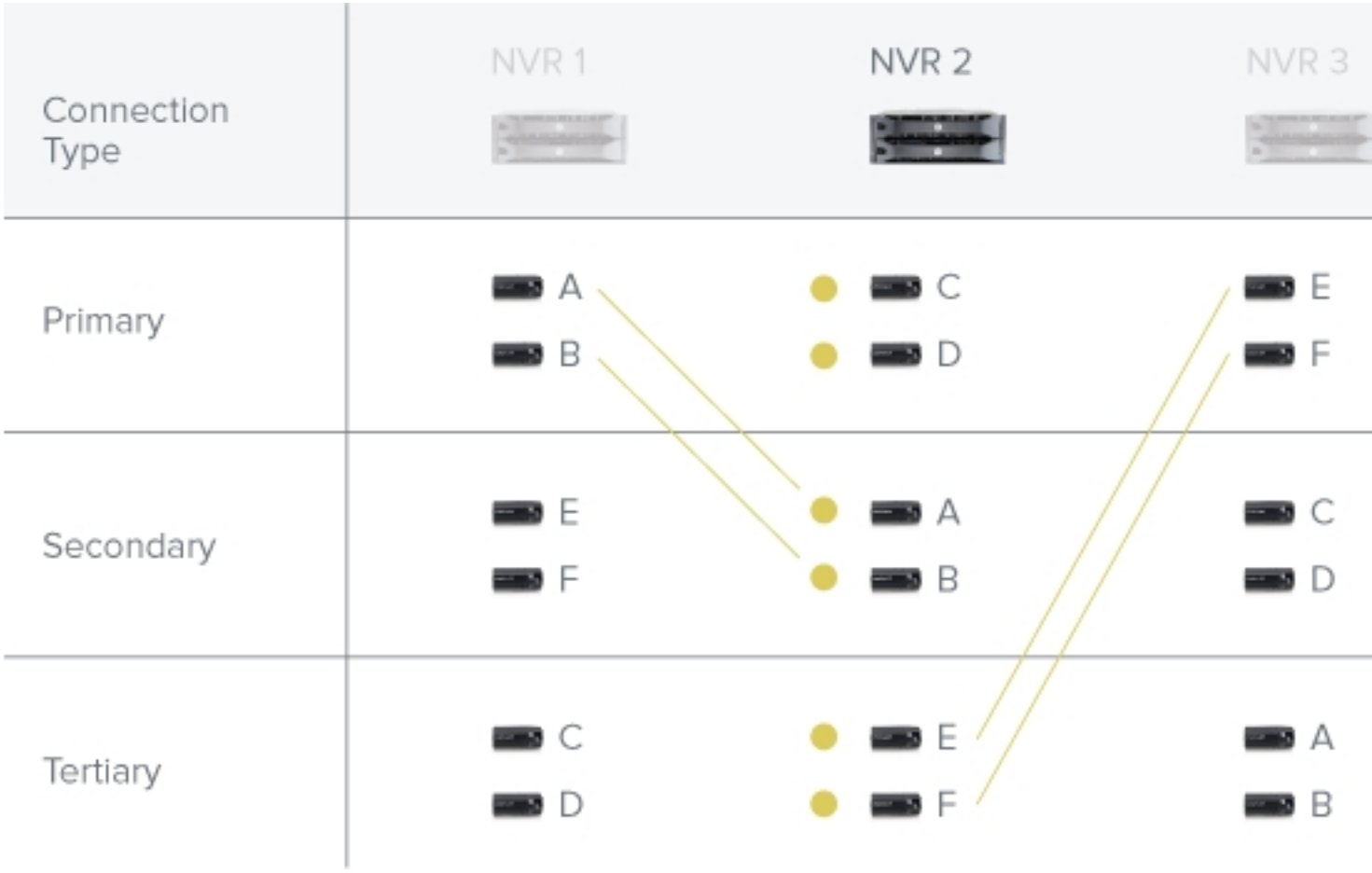


Figure 5: NVR 3 fails

Disconnecting a Device from a Server

1. In the site Setup tab, click  . The Connect/Disconnect Devices... tab is displayed.
2. Select the device you want to disconnect from the Connected Devices list, then do one of the following:
    - Click **Disconnect**. The device will be disconnected from the server and moved to the Discovered Devices list.
    - Drag the device into the **Discovered Devices** list.

Upgrading Camera Firmware

Camera firmware updates are typically included with the ACC Server update packages. Camera firmware updates are automatically downloaded and installed to the camera.

When the camera firmware is being upgraded, video from that camera cannot be displayed and the System Explorer will display  beside the camera name.

When the firmware upgrade is complete, the System Explorer will display  again and video from the camera will display.

Replacing a Device

Important: Only replace a device if it is defective or permanently damaged.

If a device is defective or permanently damaged, you can replace it with a similar device in the ACC system and transfer its recorded video to the new device.

To ensure proper functionality, devices should be replaced with those with similar capabilities. For example, if a fisheye camera malfunctioned, you could install a new fisheye camera in its place. Once you replace the device in the ACC system, the replacement device will automatically sync with the original device's recorded video. However, if a video analytics camera is replaced with a fisheye camera, previously recorded video may appear warped.

NOTE: For regularly scheduled maintenance, do not replace the device in the ACC system. Instead, disconnect the original device and connect a temporary replacement device. For more information, see *Disconnecting a Device from a Server* on the previous page and *Connecting a Device to a Server* on page 25.

The replacement device will maintain the following settings:

- Recorded and archived video
- Rules
- Alarms
- Events
- Bookmarks
- Maps

You may need to reconfigure the device's image rate and compression settings or update its motion detection area. If the replacement device has self-learning video analytics, is linked to ACM doors, or is used for Point of Sale (POS) transactions or License Plate Recognition (LPR), reconfigure those settings.

1. Uninstall the original device and install the replacement device.
2. In the site Setup tab, click  .

   The Connect/Disconnect Devices... tab is displayed.
3. In the Discovered Devices area or below a connected server, select the replacement device then click **Replace**.

   The Replace Device dialog box is displayed.
4. Select the disconnected device you want to replace.
5. Click **OK**.

   The replacement device syncs with the original device's recorded video and settings.

   NOTE: For devices with failover connections, the replacement device must replace the original device on each failover server. For example, if you have a device with 3 failover connections, you will have to replace that device 3 times. The failover level and license priority are maintained.

Always uninstall the original device before replacing it in the ACC system. If you replace a device in the ACC system but did not disconnect the original device from the network, you may receive a connection error if the original device comes online. If this happens:

1. Disconnect both the replacement and original devices from the ACC system.
2. Perform a factory reset on each device.
3. Connect each device to the ACC system as described in *Connecting a Device to a Server* on page 25.

Adding an ACM™ Appliance to Your Site

Add an Access Control Manager appliance to your ACC site so that you can link ACM door events to ACC rules and trigger actions — such as activating a specific camera when certain door events occur.

Before Adding ACM to ACC

Before an ACM appliance can be added to your ACC site, there are several configuration steps required in the ACM appliance.

For more information about any of the following settings, see the ACM help files.

NOTE: If you are using an ACM appliance version 5.10.10 SR1 or later, an ACC Administrator delegation and role have already been created. Double-check that the delegation has all rights listed in step 1 below, and that the role is set up as described in step 3.

1. Create a delegation for integrating with the ACC software. This delegation must have the following rights:
    - Appliance Listing
    - Delegations Listing
    - Door Grants
    - Doors Listing
    - Identities Listing
    - Identities Login - Remote
    - Identities Photo Render
    - Inputs Listing
    - Panels Listing
    - Partitions List
    - Roles Listing
    - Subpanels Listing
    - System Summary Listing
2. Create a routing group to define events sent from the ACM appliance to the ACC software.
    a. Specify the following for the group:
        - **Schedule**: 24 Hours Active
        - **Schedule Qualifier**: Appliance
        - The **Installed** box must be checked

b. Add the following event types to the routing group:
    - Door held open
    - Forced Door
    - Intrusion
    - Invalid Credential
    - Maintenance
    - System
    - Tamper
    - Valid Credential

3. Create a role that allows the ACC software to communicate with the ACM appliance:
    a. Keep the default **Parent** value (none).
    b. Keep the default **Start Date** value (the current date).
    c. In the **Stop Date** box, enter an appropriate date for this role to expire. By default, the role will stop working 1 year from its creation date.
    d. Select the **Installed** check box and click **Save**.

       Additional tabs will appear.

    e. In the role's **Delegate** tab, assign only the delegation that was created in the preceding steps.
    f. In the **Routing** tab, assign only the routing group that was created in the preceding steps.
4. If you plan to import Active Directory identities to the ACM appliance or the ACC software, configure an LDAP Collaboration. For Active Directory Remote Authentication, configure remote authentication from external domains.
5. Create a dedicated identity for interacting with the ACC software.

   NOTE: To protect the security of the connection between the ACM appliance and the ACC software, the dedicated identity should have only the permissions outlined in this procedure. Operators should not have access to this account.

    - Assign a Last Name, Login, and Password for the identity.
    - The password should meet the minimum password strength requirements for your ACC site.

      The password strength is defined by how easy it is for an unauthorized user to guess. It is highly recommended that you select a password that uses a series of words that is easy for you to remember but difficult for others to guess.

    - Under the identity's **Roles** tab, assign only the role that was created in the preceding step.
6. If your ACM appliance uses partitions, add the identity as a member of the partitions they will need to access from the ACC Client.
7. Configure ACM to use the same NTP Time Server as the ACC Server.

   For Windows systems, the ACC Server gets its time from the operating system. For ACC ES recorders and appliances, the NTP Time Server can be configured through the device's web interface.

a. In the top-right corner, click the gear icon to open the Setup & Settings menu and select **Appliance**.

b. In the **Time Server** box, enter the Time Server IP address.

Once these settings are applied, you can connect to the ACM appliance from the ACC Client.

Connecting ACC to an ACM Appliance

Connect an ACM appliance to your ACC site and you can link doors controlled by the appliance to cameras controlled by the ACC software. After doors and cameras are linked, you can configure rules that are triggered by doors in the ACC software.

Before you begin, make sure you have the following:

- The hostname or IP address of the ACM appliance.
- The ACM port number if different from the default port (443).
- The username and password for the identity that was created to add the ACM appliance to the ACC software.

1. In the site Setup tab, click  .

   The Access Control dialog box is displayed.

2. Enter the required credentials.
3. Click **OK**.

   The Untrusted New Site dialog box is displayed. Confirm that the listed SHA-256 fingerprint ID is the same.

   The fingerprint information is typically listed on the Appliance:Edit page, under the SSL Certificate tab.

4. If the fingerprints are the same, click **Trust**.

   If the fingerprints do not match, contact your system administrator.

The ACM appliance is now listed under the site as AC *Hostname* in the Setup tab.

Linking Doors to Cameras

You can link each door to any number of cameras in your site. Once a link has been created, authorized users can grant door access or perform identity verification while monitoring live video from the linked cameras. You will also be able to configure rules that are triggered by doors in the ACC software.

You can link doors that are installed and connected to installed panels or subpanels.

Contact your ACM administrator to configure the door you want to link to a camera.

NOTE: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. For more information, see *Importing ACM Roles* on page 43. Contact your ACM administrator to update your permissions.

To add or edit links:

1. In the ACM appliance Setup tab, click  .

   The **Cameras and Doors** dialog box is displayed.

2. To add a link, click **Create Link**.
   a. In the following dialog box, click the **Select a door** drop-down list then select the check box beside a door.

      NOTE: The available doors and your ability to view badge photos depend on your permissions in the ACM appliance. Contact your ACM administrator to update your permissions.

   b. In the **Select one or more cameras** drop-down list, check the box beside all the cameras that you want to link with the selected door.
   c. Click **OK**.
3. To edit a link, select a link then click **Edit Link**.

   You can only change the cameras that are linked to the door.

4. To delete a link, select a link then click **Delete Link**.

   When the confirmation dialog is displayed, click **Yes**.

5. Click **OK** to close the Cameras and Doors dialog box.

Authorized users can now grant access to doors or perform identity verification while monitoring live video from the linked cameras. For more information, see *Granting Door Access* on page 135 or *Identity Verification* on page 135.

You can also create rules triggered by doors. For more information, see *Adding a Rule for an ACM Appliance Event* below.

Adding a Rule for an ACM Appliance Event

After you have connected an ACM appliance to your site, you can create rules in the ACC software that are triggered by ACM appliance events.

ACM appliance events can include door or installed input events. For example, you can create a rule that immediately displays live video on all users' screens when a door is either forced or held open.

For a complete list of rules, actions, and conditions for access control events, see *Rule Event and Action Descriptions* on page 189.

NOTE: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. For more information, see *Importing ACM Roles* on page 43. Contact your ACM administrator to update your permissions.

1. In the site Setup tab, click  .

   The Rules dialog box is displayed.

2. Click .
3. On the Select Rule Event(s) page, select all the events that will trigger the rule.

   If there is blue underlined text in the rule description, click on the text to further define the event.

   When the trigger event is defined, click .
4. On the Select Rule Action(s) page, select all the actions that will occur in response to the triggers.

   If there is blue underlined text in the rule description, click on the text to further define the action.

   When the action is defined, click .
5. On the Select Rule Condition(s) page, select one or more conditions that will cause the rule to run. To always run the rule, clear all conditions.

   If there is blue underlined text in the rule description, click on the text to further define the condition.

   When the condition is defined, click .
6. On the Select Rule Properties page, complete the following:
   a. Enter a **Rule Name:** and a **Rule Description:**.
   b. Select a **Schedule:** for the rule. For more information, see *Scheduling Site Events* on page 61.
   c. Select the **Rule is enabled** check box to enable the rule once the wizard is finished. Clear the check box if you do not want to enable the rule once the wizard is finished.
   d. Confirm the rule description in the bottom part of the dialog box.
7. Click to save the new rule.

Users and Groups

When users are added to the ACC system, they are assigned to a group that defines their access permissions in a site. Use the Users and Groups dialog box to create and manage users and groups.

Adding a User

NOTE: This procedure describes adding individual users to the system. If you are managing users through Windows Active Directory, add new users directly through Active Directory. For more information, see *Importing Active Directory Groups and Users* on page 41.

1. In the site Setup tab, click  .
2. In the Users tab, click **Add User**.
3. When the Add/Edit User dialog box appears, complete the User Information area.
4. If you don't want this user to be active yet, select the **Disable user** check box. Disabled users are in the system but cannot access the site.
5. In the Login Timeout area, select the **Enable login timeout** check box to set the maximum amount of time the Avigilon Control Center Client software can be idle before the user is automatically logged out of the application.
6. Select the **Member Of** tab to assign the user to a group.
    a. Select the check box beside each access group the user belongs to.

       The other columns display the permissions that are included in the selected groups.

    b. Return to the **General** tab.
7. In the Password area, complete the following fields:
    - **Password:** — enter a password for the user.
    - **Confirm Password:** — re-enter the password.
    - **Strength:** — indicates the strength of the password. The strength is defined by the group the user is assigned to. If the user is a member of more than one group, the user must meet the strongest password requirement.

      The password must meet the minimum strength requirements.

        - ✔ — password meets the strength requirements.
        - ✘ — password does not meet the strength requirements, enter a new password.

      The password strength is defined by how easy it is for an unauthorized user to guess. If your password does not meet the strength requirements, try entering a series of words that is easy for you to remember but difficult for others to guess.
    - **Require password change on next login** — select this check box if the user must replace the password after the first login.
    - **Password Expiry (Days):** — specify the number of days before the password must be changed.
    - **Password never expires** — select this check box if the password never needs to be changed.
8. Click **OK**. The user is added to the site.

Editing and Deleting a User

You can edit and delete users as needed.

NOTE: Be aware that you cannot edit or delete users that belong to the same ranked group as you or higher. This also means that you cannot edit your own user account unless you are part of an Unranked group.

Tip: If a user has access to more than one site, the changes to the user need to be made on each site.

1. In the site Setup tab, click  .
2. In the Users tab, select a user then perform one of the following:
    - To edit the user's information, click **Edit User**. For details about the editable options, see *Adding a User* on page 37.

      NOTE: If you want to edit a user that was imported through the External Directory tab, you can only disable the user or change their Login Timeout setting. All other settings are maintained by the External Directory.
    - If Two-Factor Authentication is enabled, and a user has lost access to their verification code, click **Reset Two-Factor Key**. The next time the user logs in, they will see a new QR code that they can scan.
    - To delete the user, click **Delete User**.

      NOTE: Users imported through the External Directory tab cannot be deleted, only disabled.

Adding Groups

Groups define what features users have access to. Create new groups to change what users can access.

Groups can be given a rank in the Corporate Hierarchy to further define what the members of the group can access. For more information about the Corporate Hierarchy feature, see *Corporate Hierarchy* on page 15.

1. In the site Setup tab, click  .
2. In the following dialog box, select the Groups tab and click **Add Group**.
3. In the pop-up dialog box, select an existing group to use as a template for your new group, then click **OK**.
4. In the Edit Group dialog box, complete the following:
    a. Give the new group a name.
    b. Select a rank for the group from the **Rank:** drop-down list. To edit or view the entire Corporate Hierarchy, click  .
    c. Move the **Min Password Strength:** slider to define how strong the password used by each user in the group must be.

       The password strength is defined by an algorithm that anticipates how easy a password is to guess. There is no defined character minimum, but the stronger the setting, the harder it should be for an unauthorized user to crack the password.

       Tip: If users are expected to change their passwords frequently, you may want to select a weaker setting to ensure users do not have difficulty choosing new passwords.
    d. To enable Two-Factor Authentication, select the **Required** check box.

The next time users in this group log in, they will need to download an authenticator app on their mobile device and scan a QR code to log in to a site.

For proper use, ensure your servers sync to a real-time source. Verification codes are only valid within +/- 5 minutes of the server's time. If this does not match the time on the user's mobile device, the user will not be able to log in.

NOTE: The default administrator will be able to log in to a site without Two-Factor Authentication, even if it is enabled for their group.

Important: Two-Factor Authentication is not supported on the ACC Mobile 2 or ACC Mobile 3 Preview apps, the ACC Virtual Matrix software, or the ACC Gateway Web Client. Users with Two-Factor Authentication enabled will not have access to these programs.

e. Select the required **Group Privileges:** and **Access Rights:** for the group. Clear the check box of any feature or device that you do not want the group to have access to.

5. To enable the Dual Authorization feature, click **Enable Dual Authorization**.

   When you enable Dual Authorization, users in this group cannot review recorded video without permission from a user in the authorizing group.

   a. In the following dialog box, click the toggle to enable Dual Authorization.
   b. Select the groups that can grant authorization to users in this group.
   c. To disable the feature, click the toggle at the top of the dialog box.
   d. Click **OK**.

6. Select the Members tab to add users to the group.

   If a user is added to the group through the Add/Edit User dialog box, the user is automatically added to the group's Members list.

   a. Click .
   b. Select the users that should be part of this new group. Only users that have been added to the site are displayed.

      Tip: Enter the name of a user in the **Search...** field to locate specific users.

   c. Click **Add**. The users are added to the Members list.

7. Click **OK** to save the new group.

Editing and Deleting a Group

You can change the access permissions for a set of users by editing their access group.



1. In the site Setup tab, click .
2. Select the Groups tab.
3. Select a group and do one of the following:
   - To edit the group, click . For details about the configurable options, see *Adding Groups* on page 39.
   - To delete the group, click .

     NOTE: Default groups cannot be deleted.

Importing Active Directory Groups and Users

You can import Windows Active Directory groups and users to a site so users can log in with their Windows credentials. Members of an imported Active Directory group are automatically added as users to the site.

Changes to user accounts in the Active Directory are automatically synchronized with user accounts in the ACC software.

NOTE: Imported user information, including login credentials, is maintained by the Active Directory. In the ACC software, you can only disable an imported user, assign the user to a group, or configure the user's Login Timeout settings.

Enabling the Active Directory

To import groups and users, Active Directory must be enabled.



1. In the site Setup tab, click .

   The Users and Groups dialog box is displayed.
2. Select the **External Directory** tab.
3. Select the **Enable External Directory** check box.
4. If your site is connected to an ACM appliance, select **Active Directory** from the drop-down list.

   NOTE: If your site was previously using Avigilon's Access Control Manager system as the external directory, the previously imported Identities are automatically disabled. You will no longer be able to control doors from the ACC Client.
5. Click **Edit**.
6. In the following dialog box, enter your username and password for the network domain, then click **OK**.

Back in the External Directory tab, you can now import groups and users.

Importing a Group



1. In the site Setup tab, click .

   The Users and Groups dialog box is displayed.

2. In the External Directory tab, click **Add Group**.
3. In the following dialog box, select an existing group to use as a template, then click **OK**. You can edit the permissions for the group later.
4. In the Select Groups dialog box, locate the Windows group you want to import by doing one of the following:
   - Enter the name of the Windows group in the **Enter the object names to select** field and click **OK**.
   - Click the **Advanced** button and search for the group.

The group is automatically added to the External Directory list and the Groups list. All the users in the group are imported into the Users list.

The imported Active Directory group can now be edited like any existing group in the ACC software. You can assign the group a rank, feature privileges, and device access rights.

Members of an imported Active Directory group can be assigned to any existing group in addition to the group they were imported with. For more information, see *Assigning an Imported User to a Group* below.

Importing a User

NOTE: To import a user, your ACC Client and Server must run version 6.8 or later.



1. In the site Setup tab, click .

   The Users and Groups dialog box is displayed.

2. In the External Directory tab, click **Add User**.
3. In the Select Users dialog box, locate the Windows user you want to import by doing one of the following:
   - Enter the name of the Windows user in the **Enter the object names to select** field and click **OK**.
   - Click the **Advanced** button and search for the Windows user.

The user is automatically added to the External Directory list and the Users list. The user can now be assigned to a group. For more information, see *Assigning an Imported User to a Group* below.

Assigning an Imported User to a Group

To use the ACC system, an imported user must be assigned to a group.

NOTE: If the user was imported as part of a Windows group, they will automatically be assigned to that group.

1. In the Users tab, click **Edit User**.

   The Add/Edit User dialog box is displayed.

2. Select the **Member Of** tab.
3. Select the check box beside each access group the user belongs to.

   The other columns display the permissions that are included in the selected groups.

4. Click **OK**.

The imported user is assigned to the selected groups.

Importing ACM Roles

NOTE: This feature is only available to sites that are connected to an ACM appliance.

To provide users with control over doors, you must import Roles from the ACM appliance. When you import a role, you are also importing all the identities that are assigned to the role.

Only identities with a username and password in the ACM appliance will be imported.

Important: Usernames in the ACC software and ACM appliance must be unique. Duplicated usernames will not be imported.

If your ACM appliance is partitioned, ensure identities are members of the appropriate partitions so they can access unification features in the ACC Client.

NOTE: Importing ACM Roles to a site will disable all Active Directory users in the ACC software.

1. In the site Setup tab, click  .

   The Users and Groups dialog box is displayed.

2. Int the External Directory tab, select the **Enable External Directory** check box. From the drop-down list, select **Avigilon Access Control Manager**.

   Tip: If you previously imported Active Directory users, you can still do so by configuring remote authentication from external domains in the ACM application first. For more information, see the ACM help files.

3. Click **Add Group**.
4. In the following dialog box, select an existing group to use as a template then click **OK**. You can edit the permissions for the group later.
5. In the following dialog box, select all the roles that you want to import.

   You can use the search bar to find specific roles.

6. Click **OK** to add the roles.

Once imported, the roles are added to the External Directory list and the Groups list. All the identities assigned to the role are imported into the Users list.

Imported roles can be edited like any existing group in the ACC Client software. You can assign a rank, feature privileges, and device access rights to the imported role. However, you cannot assign ACC users to an ACM role from the ACC Client software.

Imported identities can be added to existing groups in addition to the role they were imported with.

Imported identity information, including login credentials, is maintained by the ACM appliance.

External Notifications

You can configure the site to send external notifications in response to specific events. You can set up an SMTP server for the site and choose what events require external notifications.

If you use a central station monitoring service, you can set up external notifications to be sent between your site and the monitoring station. You can configure your site to send either SMTP notifications or Security Industry Association (SIA) notifications.

Setting Up the Email Server

To send email notifications, the site must be given access to an email server.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.
2. Select the Email Server tab.
3. In the Email Server Settings: area, complete the following:
   a. **Sender Name:** enter a name to represent the site in all email notifications.
   b. **Sender Email Address:** enter an email address for the site.
   c. **Subject Line:** enter a subject line for all emails sent from the site. The default subject is *Avigilon Control Center System Event*.
   d. **SMTP Server:** enter the SMTP server address used by the site.
   e. **Port:** enter the SMTP port.
   f. **Timeout (seconds):** enter the maximum amount of time the server will try to send an email before it quits.
4. (Optional) If the email server uses encryption, select the **Use secure connection (TLS/SSL)** check box.
5. (Optional) If the email account has a username and password, select the **Server requires authentication** check box.
   - Enter the **User Name:** and **Password:** for the email account.
6. Click **OK**.

Configuring Email Notifications

In the Email Notifications dialog box, you can create email notification groups to specify who will receive email notifications when certain events occur.

Be aware that you cannot send any email notifications until you've set up an email server for the site. For more information, see *Setting Up the Email Server* on the previous page.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.

2. Make sure the Email Notifications tab is selected.
3. Click .
4. Enter an **Email Group Name:**.
5. In the **Email Recipients:** area, add all the user, group and individual emails that are part of this email group. Do any of the following:

   - Click  to add a site user or access group. In the dialog box, select all the required users and groups then click **OK**.
   - Click  to add individual emails. In the dialog box, enter the email address then click **OK**.

   Tip: Make sure the site users in the Email Recipients: list have a valid email in their user account.

6. Click  to send a test email to everyone on the Email Recipients: list.
7. In the **Email Trigger:** area, select all the events that will trigger an email for this email group. Click the blue underlined text to define the event requirements.

   Tip: If you require other events or more specific requirements, you can also configure email notification in the rules engine. For more information, see *Rules* on page 53.

8. To attach a snapshot of the email notification event, select the **Attach images from device(s) linked to the event** check box.

   NOTE: This option is disabled if *Motion Detect* is not selected because there are no images associated with system events, digital inputs, or POS transaction exceptions.

9. In the **Email Schedule:** area, select a schedule for the email notification. For more information, see *Scheduling Site Events* on page 61.
10. To limit the number of emails sent, enter the minimum amount of time between each email in the **Send email at most every:** field.
11. Click **OK**.

The new email notification is saved and added to the Email Groups: list.

Editing and Deleting an Email Notification

You can edit or delete email notifications as needed.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.

2. In the Email Notifications tab, do one of the following:
   - To edit an email notification, select the notification from the **Email Groups:** list then make the required changes. For more information about the editable options, see *Configuring Email Notifications* on page 44.
   - To delete an email notification, select the notification from the **Email Groups:** list then click .

Central Station Monitoring

Central station monitoring notifications allow an ACC site to notify a third-party central monitoring company when an event of interest occurs. This feature works through the external notification feature and the rules engine. You need to enable the ACC site to send notifications, then create all the rules that would cause a notification to be sent to the central monitoring station.

Enabling Central Station Monitoring

If you use a central station monitoring service, you can set up the ACC site to communicate with your central monitoring service via:

- XML over SMTP notifications
- SIA over IP notifications

Consult with your central monitoring service for their preferred notification type.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.

2. In the Central Station Monitoring tab, select the **Enable Central Station Monitoring** check box.
3. In the Central Monitoring System: drop-down list, select which type of notification the ACC software should send:
   - **XML over SMTP** — external notifications will be sent to the central station monitoring service using SMTP.
   - **SIA over IP** — Security Industry Association (SIA) notifications will be sent to the central station monitoring service using IP.

You can now configure the notification options.

Configuring Notification Options

Consult with your central monitoring service for the correct settings for each field.

1. In the Options area, complete the fields with the information provided by your central monitoring service.
    - If you selected XML over SMTP notifications, the central monitoring service will typically provide you with a specific name, email address, and SMTP details to identify you in their system.
    - If you selected SIA over IP notifications, the central monitoring service will typically provide you with an Account Number, Site Receiver Numbe, primary and secondary server IP addresses and port numbers.
2. To periodically check the state of the connection to the central monitoring service, select a time interval from the **Minimum Heartbeat Interval:** drop-down list.
    - The selected amount of time must pass before a confirmation message is sent. The confirmation message is only sent if no other notifications are sent during the set time period.
    - This feature allows the system to automatically send a message to the central monitoring service to confirm that the systems are still connected and no issues have occurred.
    - If the central monitoring service requires the system to send a heartbeat test message at specific intervals, select the option that is equal to half the requested interval. For example, if the central monitoring service requires a confirmation message be sent once a day, assign the system to send a message every 12 hours.
3. Click **OK** to save your changes.

You can now create rules to send the central monitoring service notifications when specific events occur.

Create Central Station Monitoring Rules

Create rules that will notify the central monitoring service of specific events. For more information about creating rules, see *Adding a Rule* on page 53.

- On the Select Rule Action(s) page, make sure the **Send notification to Central Monitoring Station** option is selected. This ensures the central monitoring service is notified of the rule event.

  Tip: The system Email Notifications feature works separately from the Central Station Monitoring feature, but you can configure the rules to send you the same notifications as the central monitoring service. When you create rules for the central monitoring service, include the **Send email** option on the Select Rule Action(s) page. You can configure the rule to send you details that are not included in the central monitoring notification.

For XML over SMTP notifications only, you can customize the notification by clicking the blue link text in the rule description.

1. Click **no media** to select the type of attachment included with the notification.
    - In the Select Attachment dialog box, select the **Image** or **Video** check box.
    - For Video attachments, select the quality:

      low The attached video resolution is 4CIF with a fixed frame rate of 5 fps. The attached video size is typically under 1 MB.

      high The attached video resolution is 720p with a fixed frame rate of 10 fps. The attached video size is typically under 3 MB, depending on the camera's image and compression settings and the amount of motion in the scene.
2. Click **no media source** to select which cameras to export from.
    - In the Select Cameras dialog box, you can choose to include attachments from cameras linked to the trigger event or other cameras in the system.

      NOTE: Only select cameras that are connected to the same server as the triggering device. Attachments from other servers are not currently supported.

To arm or disarm event notifications from the site, the ACC software also supports rule conditions — the requirement that a condition be met before a rule is executed. Digital input device events can be used to condition a rule and effectively arm or disarm the rule.

License Plate Recognition

License Plate Recognition (LPR) is a licensed feature that allows users to read and store vehicle license plates from any video streamed through the ACC software.

You must have the LPR feature licensed and installed on your server. For more information about adding an LPR license to your site, see *Licensing the Site* on page 54. For more information about configuring your LPR server settings, see *Setting Up License Plate Recognition* on page 69.

If your site is licensed, you can add an LPR Watch List to detect license plates across all servers in your site that have the LPR feature installed.

A Watch List identifies license plates that are of interest. When a license plate on a Watch List is detected, operators will be notified with an event. You can trigger an action in the Rules engine for each Watch List. For example, you could create a Watch List of black-listed license plates and add a rule to alert you when one of those license plate is detected in your surveillance video.

Adding a Watch List

When you add a new Watch List to your site, you can import or manually add each license plate that needs to be detected. Each license plate has a Minimum Confidence setting that determines how similar the detected license plate number must be before it is considered a match.

For ACC software version 6.12 or later, the Minimum Confidence is the probability that the detected license plate matches a license plate in the Watch List.

For earlier software versions, the Minimum Confidence is the percent difference between the detected license plate and the license plate in the Watch List.

Tip: If you receive too many false alarms for a license plate, increase the license plate's Minimum Confidence. If you are missing alarms for a license plate, decrease the license plate's Minimum Confidence.

1. In the site Setup tab, click .
2. In the following dialog box, click **Add**.

   The Add Watch List dialog box is displayed.
3. Enter a **Watch List Name:** and **Watch List Description:**.
4. Add license plates:
   - **To import a list of licenses plates:**
     - Click **Import** and select a comma-separated values (CSV) file.

       The CSV file must include a column for the **License Plate** and a column for the **Minimum Confidence**.

       The license plates are added to the Watch List.
   - **To add a license plate:**
     1. Click **Add**.

        The Add License Plate dialog box is displayed.
     2. Enter the license plate and select the **Minimum Confidence** using the slider.
     3. Click **OK**.

        The license plate is added to the Watch List.
   - **To edit a license plate:**
     1. Select the license plate then click **Edit**.

        The Edit License Plate dialog box is displayed.

        Update the license plate or the **Minimum Confidence** using the slider.
     2. Click **OK**.

        The license plate is updated.
   - **To delete a license plate:**
     - Select the license plate then click **Delete**.

       The license plate is deleted from the Watch List.
5. Click **OK**.

   The Watch List is saved.

Editing a Watch List

You can add, remove, or update license plates in an existing Watch List.

1. In the site Setup tab, click .
2. In the following dialog box, select a Watch List and click **Edit**.

   The Edit Watch List dialog box is displayed.

   For details about the editable options, see *Adding a Watch List* on page 48.

   NOTE: If you import a list containing license plates that are already in the Watch List, the import will replace the existing entries.

Exporting a Watch List

You can export an existing Watch List as a text file or a comma-separated values (CSV) file.

Tip: Export an existing Watch List and make updates to the CSV file. Then import it as a new Watch List that can be used to create different rules.

1. In the site Setup tab, click .
2. In the following dialog box, select a Watch List and click **Edit**.

   The Edit Watch List dialog box is displayed.
3. Click **Export**.

   A CSV file is downloaded.

Deleting a Watch List

You can delete a Watch List if it is no longer useful.

NOTE: Consider exporting the license plates before deleting a Watch List. For more information, see *Exporting a Watch List* above.

1. In the site Setup tab, click .
2. In the following dialog box, select a Watch List and click **Delete**.

Alarms

Use the Alarms dialog box to create and manage alarms. You can monitor alarms from the Alarms tab, the ACC Mobile 2 app, or the ACC Mobile 3 Preview app. For more information about the Alarms tab, see *Monitoring Alarms* on page 152.

The ACC Mobile 2 app and the ACC Mobile 3 Preview app are available for free on the App Store and Google Play™ store. The app allows you to acknowledge, assign and purge alarms from your mobile device. For more information, see the *ACC Mobile User Guide*.

Adding a New Alarm

Alarms need to be added to the site before they can be monitored.

1. In the site Setup tab, click  .

   The Alarms dialog box is displayed.

2. Click .

   The Add Alarm wizard is displayed.

3. On the Select Alarm Trigger Source page, select an **Alarm Trigger Source:** then choose the trigger requirements for this alarm. Click  to continue.

   The alarm trigger options are:

   - **Motion Detection** — the alarm is triggered when movement is detected in the selected camera's field of view.
   - **Video Analytics Event** — the alarm is triggered when a video analytics event is detected in the selected camera's field of view.

     NOTE: You must select a video analytics camera or appliance camera channel to use this alarm trigger.

   - **Digital Input Activation** — the alarm is triggered when the selected digital input is activated.
   - **License Plate Watch list Match** — the alarm is triggered when a license plate on the selected Watch List has been detected.

     For more information about setting up a license plate Watch List, see *Adding a Watch List* on page 48.

   - **POS Transaction Exception** — the alarm is triggered when a transaction exception is detected from the selected POS transaction source.

     For more information about configuring a transaction exception, see *Adding a Transaction Exception* on page 68.

   - **Device Error** — the alarm is triggered when an error occurs in the selected camera.
   - **System Error** — the alarm is triggered when a system error occurs. For a list of system errors, see *Alarm Trigger Source Descriptions* on page 197.
   - **External Software Event** — the alarm is triggered by an event generated by a third-party integration software.

4. On the following Select Linked Devices page, select the cameras that will record the alarm event then complete the following:

   a. Set the **Pre-Alarm Record Time:** and the **Recording Duration:**.

   b. Select the **View linked devices when alarm is triggered** check box to automatically display the alarm video in a View tab in the ACC Client when the alarm is triggered.

   c. Click  to continue.

5. On the Select Alarm Recipients page, select the groups and users that need to be notified of this alarm. You can create an escalation workflow to determine who is notified next if the alarm is not acknowledged.
    a. Click  to add the users or groups that will be notified of this alarm. By default, the list is empty and you must add at least one user to continue.
    b. In the following dialog box, select all the required users () and groups (). Use the search bar at the top of the window to quickly find specific users and groups.
    c. Click **Add**.
    d. Assign each user a **Wait Time**. The Wait Time determines when the user or group will be notified of the alarm.

       If a user is assigned a Wait Time of 0h 0m, the user will be notified immediately after the alarm occurs. If the next user is assigned a Wait Time of 1h 0m, that user is not notified until one hour after the alarm occurs but only if the alarm remains active. If the first user acknowledges the alarm within one hour, the second user is never notified of the alarm.

       In the Alarms tab, only users who are notified will see the live alarm trigger. All potential alarm recipients will see the alarm once it has been acknowledged.
6. Select the **Play sound when alarm is triggered:** check box to play a sound when the alarm is triggered. You can choose an alarm sound from the drop-down list.

   The sound is played in the Client software only, and will be used to notify the selected users.
7. Click  to continue.
8. (Optional) On the Select Alarm Acknowledgment Action page, set the actions that must occur when an alarm is acknowledged then click  to continue.
    - If the user must add comments about the alarm, select the **Require a comment when acknowledging alarm** check box.
    - If a digital output must be activated when the alarm is acknowledged, select the **Activate selected digital output(s) on alarm acknowledgment** check box. Then, select the digital outputs that must be activated.
    - If the digital output should only be activated when confirmed by a user, select the **Require user confirmation before activating digital output(s)** check box.
9. On the Select Alarm Properties page, complete the following:
    a. Enter a name for the alarm.
    b. Select a **Priority:** for the alarm. **1** is the highest alarm priority.
    c. Select a **Schedule:** for the alarm. For more information, see *Scheduling Site Events* on page 61.
    d. Make sure the **Enable alarm** check box is selected to set the alarm.
10. Click  to save the new alarm.

Editing and Deleting Alarms

1. In the site Setup tab, click  .

   The Alarms dialog box is displayed.

2. Select an alarm then do one of the following:

   - To edit the alarm, click .

     Go through the Add Alarm wizard and make the required changes on each page. On the last page, click  to save your changes.

     For details about the editable options, see *Adding a New Alarm* on page 50.

   - To delete the alarm, click .

Rules

The Rules engine allows you to trigger specific actions when a certain event, or set of events, occurs.

For example, you can create a rule that starts a live stream when the back door is opened, or a rule that triggers an alarm when an Avigilon Presence Detector sensor detects that it is likely that a person has been present for an excessive amount of time.

If the default email notification options are insufficient for your needs, you can use the Rules engine to set up more specific trigger events.

Adding a Rule

When you create a rule, you can define:

- The events that trigger the rule.
- The actions that occur when the rule is triggered.
- The conditions that effect when the rule is triggered.

For a complete list of rule events, actions, and conditions, see *Rule Event and Action Descriptions* on page 189.

1. In the site Setup tab, click  .

   The Rules dialog box is displayed.

2. Click .
3. On the Select Rule Event(s) page, select all the events that will trigger the rule.

   If there is blue underlined text in the rule description, click on the text to further define the event.

When the trigger event is defined, click .

4. On the Select Rule Action(s) page, select all the actions that will occur in response to the triggers.

   If there is blue underlined text in the rule description, click on the text to further define the action.

   When the action is defined, click .

5. On the Select Rule Condition(s) page, select one or more conditions that will cause the rule to run. To always run the rule, clear all conditions.

   If there is blue underlined text in the rule description, click on the text to further define the condition.

   When the condition is defined, click .

6. On the Select Rule Properties page, complete the following:
   a. Enter a **Rule Name:** and a **Rule Description:**.
   b. Select a **Schedule:** for the rule. For more information, see *Scheduling Site Events* on page 61.
   c. Select the **Rule is enabled** check box to enable the rule once the wizard is finished. Clear the check box if you do not want to enable the rule once the wizard is finished.
   d. Confirm the rule description in the bottom part of the dialog box.
7. Click to save the new rule.

Editing and Deleting a Rule

1. In the site Setup tab, click . The Rules dialog box is displayed.
2. Select a rule, then do one of the following:
   - To edit the rule, click . Go through the **Rule Setup** wizard and make the required changes on each page. On the last page, click to save your changes.

     For details about the editable options, see *Adding a Rule* on the previous page.
   - To delete a rule, click . When the confirmation dialog box appears, click **OK**.

Licensing the Site

The License Management dialog box gives you access to all the licenses in a site.

You can activate licenses to begin using your ACC system for normal operations, or activate new licensed features in your working ACC system.

If you ever need to perform a server hardware upgrade, you will need to deactivate your ACC Server license then activate the license again on the new server.

If you ever need to modify your system architecture by joining or removing servers from a site, you will need to reactivate your licenses to confirm the system changes.

For more information about any of the licensing features, see the following procedures.

Activating a License

You can activate a license for a new ACC system, or activate new licensed features for an operating ACC system. Once activated, you can immediately use the new licensed features.

1. At the top-left corner of the application window, click to open the New Task menu then click .
2. In the site Setup tab, click  .
3. In the License Management dialog box, click **Add License...**.
4. In the following dialog box, select one of the following tabs:
   - If you have internet access, select the **Automatic** tab.

     To complete activating the license through this tab, see *Automatic Licensing* on the next page.
   - If you do not have internet access, select the **Manual** tab.

     To complete activating the license through this tab, see *Manual Licensing* on page 57.

When you are prompted to enter the product key, be aware of the following:

- A check mark will appear if the product key is valid.
- If you have multiple product keys, click **Add Key** and enter the next product key.

  If you have multiple product keys listed in a text file, you can copy and paste them into the product key field. If invalid product keys are pasted, the number of invalid product keys are displayed. To view the invalid product keys, click **Copy To Clipboard** and paste the product keys into a text file.

  Tip: You can also copy and paste the product keys into a text file to save a copy for future reference.
- If you need to remove the last product key, click **Remove Last Key**.
- To clear all the product keys, click **Clear**.

Deactivating a License

You can deactivate individual licenses and activate them on a different site. For example if you are upgrading your server hardware, you can deactivate the license on the older server then activate the same license on the new server.

NOTE: There is a limit to the number of times a license can be deactivated. If you encounter an error while activating a previously deactivated license, this may be the issue. Contact Avigilon Technical Support for help.

1. In the site Setup tab, click  .
2. In the License Management dialog box, select the license you want to deactivate.

   You can select multiple licenses to deactivate them at the same time.
3. Click **Remove License...**.
4. In the following dialog box, save a copy of the product keys.
   a. Click **Copy to Clipboard**.
   b. Paste the product keys in to a text file.
   c. Save the text file.
5. Select one of the following tabs:
   - If you have internet access, select the **Automatic** tab.

     To complete deactivating the license through this tab, see *Automatic Licensing* below.
   - If you do not have internet access, select the **Manual** tab.

     To complete deactivating the license through this tab, see *Manual Licensing* on the next page.

Once a license has been deactivated, you can activate the license on a new site. For more information, see *Activating a License* on the previous page.

Reactivating a License

When servers are added to or removed from a site, the site licenses are made inactive. The licenses need to be reactivated to confirm system changes and resume normal operations.

The site will continue to function normally for a limited amount of time, but eventually the site will stop normal operations if you do not reactivate the affected licenses.

1. In the site Setup tab, click  .

   The License Management dialog box is displayed.
2. Click **Reactivate Licenses...**.
3. In the following dialog box, select one of the following tabs:
   - If you have internet access, select the **Automatic** tab.

     To complete activating the license through this tab, see *Automatic Licensing* below.
   - If you do not have internet access, select the **Manual** tab.

     To complete activating the license through this tab, see *Manual Licensing* on the next page.

Automatic Licensing

NOTE: You must have internet access to use this method.

1. Open the License Management dialog box then initiate the licensing task that you want to perform.
2. At the top of the following dialog box, select the **Automatic** tab.
3. If you are activating a license, you will be prompted to enter a license key or select the preferred demo license edition.
4. Click the button that will immediately apply your license changes.

Manual Licensing

1. Open the License Management dialog box then initiate the licensing task that you want to perform.
2. At the top of the following dialog box, select the **Manual** tab.
3. If you are activating a license, you will be prompted to enter a license key or select the preferred demo license edition.
4. Click **Save File...** .
5. From the Save As window, choose where you want to save the `.key` file that is generated by the system. You can rename the file as required.
6. Click **Save**.
7. Copy the `.key` file to a computer with internet access.
8. Open a web browser and go to **http://activate.avigilon.com**.

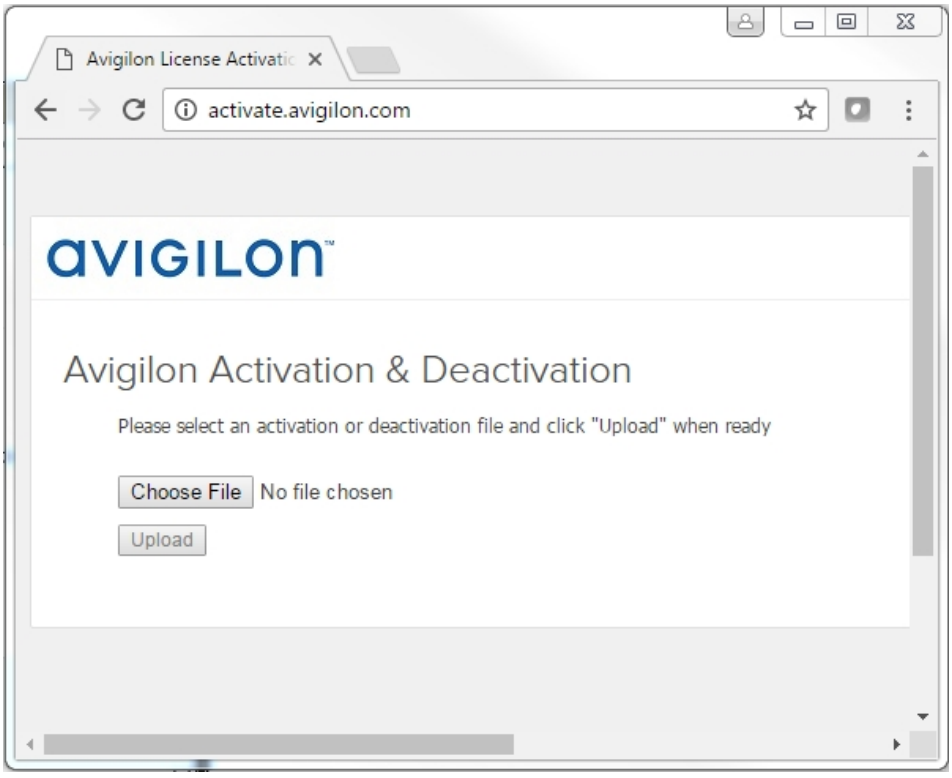


Figure 6: The Avigilon License Activation web page

9. Browse to the location of the `.key` file then click **Upload**.

   The generated license file (`.lic`) should download automatically. If it does not, allow the download to occur when you are prompted.

10. Copy the downloaded `.lic` file to a location that would be accessible to the ACC Client software.
11. Complete the product registration page to receive product updates from Avigilon, then click **Register**.

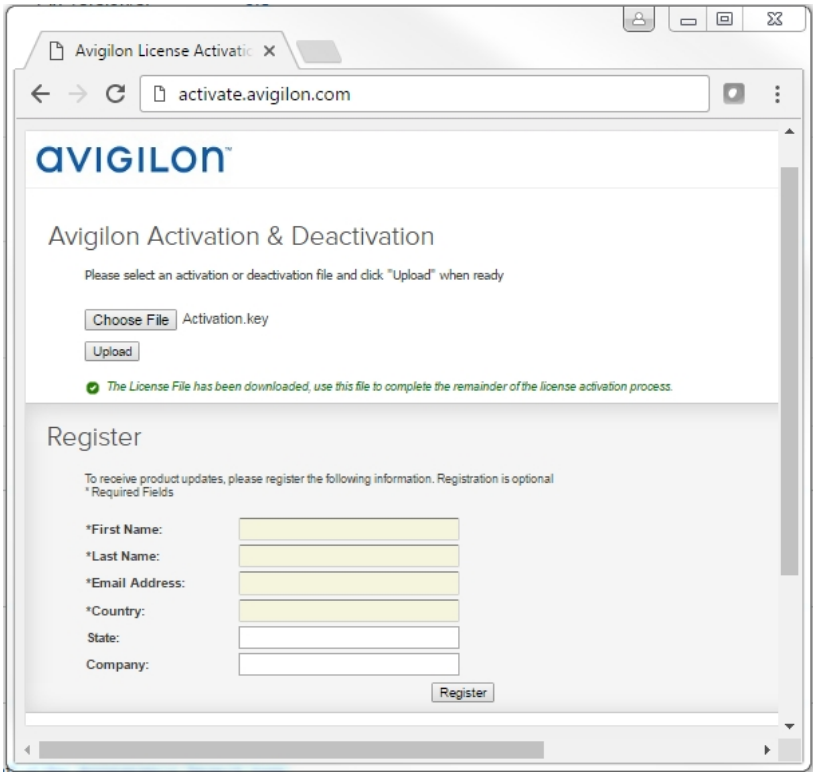


Figure 7: The product registration web page

12. If you are deactivating a license, you can now activate the deactivated license on a different site. For more information, see *Activating a License* on page 55.

    Otherwise, complete the remaining steps.

13. Return to the ACC Client and click **Apply...**.
14. Locate the downloaded `.lic` file and click **Open**.
15. When the Confirm Licenses dialog box is displayed, click **OK**.

Backing Up System Settings

You can back up site and server configuration settings so that they can be restored after an unexpected system failure or used on a different site.

If you want to back up or archive recorded video, see *Storage Management* on page 70.

1. In the site Setup tab, click  .
2. In the following dialog box, select the server that you want to back up. The site settings are automatically included in the backup file.
3. If you want to encrypt the backup file, select the **Encrypt the backup file.** check box then enter a password.

   The password is required when the backup file is used to restore the system settings. Be aware that if you lose the encryption password, the file can no longer be used.

   NOTE: It is highly recommended that you enable the encryption option because the settings file may contain sensitive system information.
4. Click **OK**.
5. In the Save As dialog box, name and save the file.

   The backup file is saved in Avigilon Settings File (`.avs`) format.

NOTE: Backup files can only be restored to servers that are running the same or more recent version of the Avigilon Control Center Server software.

Restoring System Settings

NOTE: You cannot restore settings from a 5.2.2 or earlier server through this version of the Avigilon Control Center Client software.

If you have a backup Avigilon Settings File (`.avs`), you can restore the settings as needed. You would typically restore settings after a server has been replaced in the site, or when setting up several independent sites that require similar settings.

NOTE: Make sure the new site is licensed to run the same features as the server that generated the backup file. If not, you will lose access to features that were included in the backup file but are not supported by the new site.

Be aware that when you restore server settings, all existing settings are overwritten by the restored settings. When you restore site settings, the restored settings are merged with any existing settings.

1. In the site Setup tab, click  .
2. In the following dialog box, find and select the `.avs` file that you want to restore.
3. If the backup file is encrypted, enter the required password in the following dialog box. You will not be asked to provide a password if the file is not encrypted.
4. Select the settings you want to restore.

   By default, the system will select the recommended option for you.

- **Restore site and server settings** — select this option to restore all settings in the site and the selected server.

  NOTE: If the server is part of a multi-server site, do not select this option because the site settings are maintained by the other connected servers.

- **Restore server settings** — select this option to restore all settings to the selected server.
- **Use custom settings** — click **Choose Settings** to specify the settings that you want to restore.

  Be careful when selecting the custom settings because some settings have dependencies that may cause unexpected issues if they are not supported by the server.

5. Select the server that you want to restore the settings to.

   It is recommended that you only select servers in the Recommended Servers list. Servers in this list do not have any existing device connections. Restoring settings to a server that is not in this list may overwrite existing device connection details or cause the system to exceed its license and processing limits.

6. Click **OK**.

If you restored the site settings, the settings are merged:

- Unique settings are added to the site.
- If the settings are identical, only the current site version is kept.
- If an import setting and a site setting have the same name but are configured differently, the import setting is added to the site and renamed in this format: *<setting name>* (Import), like Email1 (Import).
  - In the rules engine, the Notify users (default) rule is always added and renamed, even if the settings are the same. The import version is enabled and the site version is disabled by default.
- The two site Views are combined.
  - The import settings take precedence.

    For example, a map from the import file is already used in the site. Currently, the map is stored at the top of the site View. But in the import file, the map is kept at the bottom. After the import settings are merged with the current site settings, the map is moved to the bottom.

  - Unorganized elements from the import file are listed at the bottom of the site View.
- User permission groups are merged.
  - If groups have the same name, the import settings are used and the users from both the import file and the current site are added to the group.
  - If the site supports new permissions not available in the import file, the new permissions are disabled by default for the imported group.
  - Default group settings (i.e. Administrators, Power Users, Restricted Users, Standard Users) will use the default site settings for permissions not available in the import file.
  - Groups added from the import file automatically gain access to all the new devices that were added since the settings were exported.
- Users with the same name will use the import settings, including passwords.

Scheduling Site Events

Site events are actions that can affect the entire site, like email notifications. When you configure a site event, you are given the option to assign a schedule to the event. Schedules control when events can occur — at specific times during a day, or only on specific days.

When you see the **Schedule** option while configuring an event, you can select an existing schedule or create a new schedule.

- To use a preconfigured schedule, select an option from the drop-down list. The default option is *Always*, which allows the event to run constantly.
- To change a schedule, select the schedule then click  >  .
- To delete a schedule, select the schedule then click  > . In the following confirmation dialog box, click **OK**.
- To create a schedule, click  then select  . When the Edit... dialog box is displayed, complete the following steps:
    1. Give the new schedule a name.
    2. Give the first recurrence a name.

       You can add multiple recurrences to create a detailed schedule. For example, you could create one recurrence to cover every weekend, plus extra recurrences to cover public holidays.

        - To add extra recurrences, click  .
        - To delete a recurrence, select the recurrence then click  .
    3. For each recurrence, define the duration by entering a **Start:** and **End:** time.

       Be aware that if you enter an End: time that is earlier than the Start: time, the event will span two days. For example, if the schedule is set to start at 12:00 pm and end at 11:59 am, the event is automatically enabled from 12:00 pm on day 1 and will end at 11:59 am on day 2.
    4. In the **Start Date:** field, enter when the recurrence should begin.

5. In the Recurrence pattern area, select the frequency of the recurrence.

Option	Description
Daily	The event is enabled during the same time every day. • Select the number of days between each schedule recurrence.
Weekly	The event is enabled during the same day and time every week. • Select the day(s) of the week, then select the number of weeks between each schedule recurrence.
Monthly	The event is enabled during the same day and time every month. • Select the specific day or weekday, then select the number of months between each schedule recurrence.
Yearly	The event is enabled during the same day and time every year. • Select the specific day or weekday and month, then select the number of years between each schedule recurrence.

6. Add and complete any other recurrences that need to be part of the schedule.
7. Click **OK** to save the new schedule.

Server Settings

Server settings are related to video recording on each server in the system. This includes configuring the recording schedule, data aging, and bandwidth usage.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Naming a Server

Give the server a meaningful name so that it can be easily identified in the System Explorer. Otherwise, the server uses the name that is assigned by Windows.



1. In the server Setup tab, click .
2. In the following dialog box, enter a name for the server.
3. Click **OK**.

Recording Schedule

The ACC system uses a recording schedule to set when each connected camera should be recording video. By default, the server is set to record motion and configured events when they occur.

Once the recording schedule is set, video is recorded automatically.

Adding and Editing a Recording Schedule Template

The recording schedule is set by using templates that tell cameras when and what to record. For example, you can create one recording schedule template for weekdays and another for weekends.

NOTE: Recording templates are shared across a site.



1. In the server Setup tab, click . The Recording Schedule dialog box is displayed.
2. Click **Add Template** below the Templates: list.
3. Enter a name for the **New Template**.
4. Click the **Set Area** button, then click or drag the cursor across the **Recording Mode:** timeline to set the types of events that the cameras will record throughout the day. Individual rectangles on the Recording Mode: timeline are colored when they have been selected.

   The **Recording Mode:** options include:

   - **Continuous** — record video constantly.
   - **Motion** — only record video when motion is detected.
   - **Digital Inputs** — only record video when a digital input is activated.
   - **Alarms** — only record video when an alarm is activated.
   - **POS Transactions** — only record video when a point of sale (POS) transaction is made.
   - **License Plates** — only record video when a license plate is detected.
5. To disable recording in parts of the template, click the **Clear Area** button, then click or drag the cursor across the timeline to remove the set recording areas.
6. If cameras are *not* recording in Continuous mode all day, you can set cameras to record reference images between events in the recording schedule.

   - Select the **Record a reference image every:** check box, then set the time between each reference image.

Editing and Deleting a Template



1. In the Setup tab, select the server you want to edit then click .
2. In the Recording Schedule dialog box, select a template from the Templates: pane and do one of the following:
   - To edit a template, modify the schedule.
   - To rename a template, click **Rename Template** and enter a new name.
   - To delete a template, click **Delete Template**.
3. Click **OK** to save your changes.

Setting Up a Weekly Recording Schedule

You can set up a weekly recording schedule by applying templates to cameras for each day of the week.



1. In the server Setup tab, click . The Recording Schedule dialog box is displayed.
2. Select a template from the Templates: list.
3. In the Default Week area, click the days of the week this template applies to for each camera.

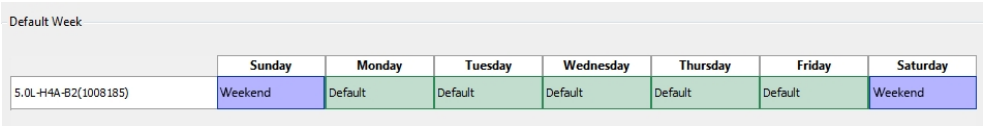


Figure 8: The Recording Schedule dialog box: Default Week

4. Click **OK**.

Recording and Bandwidth

While the Recording Schedule dialog box sets when and what cameras record, the Recording and Bandwidth dialog box sets how long recorded video is stored.

In the Recording and Bandwidth dialog box, you can change the data aging settings and set the maximum record time for each connected camera. The amount of data aging that is available depends on the camera that is connected to the system.

- For JPEG2000 or JPEG compression cameras, data aging is available at three rates:
  - **High Bandwidth** keeps recordings at their original quality.
  - **Half Image Rate** discards half of the recorded data to make room for new recordings.
  - **Quarter Image Rate** keeps 1/4 of the original recorded data so that you can still see older video.
- For H.265 and H.264 cameras that support data aging, data aging is available at two rates:
  - **High Bandwidth** keeps the original high quality video and the secondary stream of low resolution video.
  - **Low Bandwidth** only keeps the secondary stream of low resolution video.

  NOTE: The data aging can only occur when the secondary stream is enabled.
- For H.265 and H.264 cameras that *do not* support data aging, only the **High Bandwidth** video is kept.

By default, the system is set to keep recorded video for the maximum amount of time based on the available storage.

At the bottom of the Recording and Bandwidth dialog is the following statement:

Total record time estimate is based on constant recording

The retention time is determined by the **Max. Record Time** setting and the average camera data rate. Since the system can only provide an estimate of the data rate for the full retention period, the actual retention time may exceed the Max. Record Time setting by 5 minutes.

1. In the server Setup tab, click  .

   The Recording and Bandwidth dialog box is displayed.

   The Data Aging column shows an estimate of the recording time that is available at each image rate, given the amount of space on the recording device.

2. In the Data Aging column, move the sliders to adjust the amount of time video is stored at each image rate.
   - To change the data aging settings for all linked cameras, move the slider for one linked camera and all linked cameras will be updated.
   - To change the data aging setting for one camera, break the camera's link to other cameras by clicking the icon to the left of its name, then make your changes.
3. In the **Max. Record Time** column, manually enter a maximum record time or select one of the options from the drop-down list for each camera.

   NOTE: If the time estimated in the Total Record Time column is significantly shorter than what is set in the Max. Record Time column, the camera's actual recording time will be closer to the Total Record Time estimate.

4. Click **OK**.

NOTE: If you are setting up data aging to work with the Storage Management Continuous Archive feature, keep note of the lowest data aging setting. To work together, the value of the data aging setting must be greater than the value configured for the Archive video older than: parameter on the Storage Management dialog box. This ensures that archiving starts before data is deleted on the local ACC Server.

POS Transactions

The Point of Sale (POS) Transaction Engine is a licensed feature that records raw data from POS transaction sources. You can link cameras to specific POS transaction sources, and set up the system to make note of transaction exceptions.

Once POS transactions have been set up, you can see live and recorded POS transaction data in the View tab while watching any linked video.

To monitor live POS transactions, see *Monitoring Live POS Transactions* on page 136.

To review recorded POS transactions, see *Reviewing Recorded POS Transactions* on page 152.

Adding a POS Transaction Source

1. In the server Setup tab, click  . The POS Transactions dialog box is displayed.
2. Click . The POS Transactions Setup wizard is displayed.
3. On the Set Transaction Source Device page, enter the **Hostname/IP Address:** and the **Port:** of the POS transaction source device, then click **Next**.
4. On the Set Transaction Source Data Format page, select a data format, then click **Next**.

   To add or edit a data format, click **Add** or **Edit**. Alternatively, click **Copy From** to duplicate then edit the selected data format.

   For more information about adding a new data format, see *Adding a Transaction Source Data Format* below.
5. On the Set Transaction Exceptions page, select any exceptions that need be monitored, then click **Next**. If you do not need to monitor for exceptions, you can skip this page.

   To add or edit a transaction exception, click **Add** or **Edit**. For more information, see *Adding a Transaction Exception* on page 68.
6. On the Set Transaction Source Device page, select the cameras you want to link to the transaction source.

   You can also set the amount of time video needs to be recorded before and after each transaction. The default value is 5 seconds.

   When you are ready to continue, click **Next**.
7. On the Set Transaction Source Name and Description page, enter a name and description for the transaction source. Select **Enable transaction source** to start receiving data from the transaction source.
8. Click to save the new transaction source.

Adding a Transaction Source Data Format

NOTE: POS transaction source data formats are shared across a site.

When you add a new POS transaction source, be aware that the transaction source must have a source data format.

1. In the POS Transactions Setup wizard, click when you arrive on the Set Transaction Source Data Format page. The Configure Data Format dialog box is displayed.

   For information about accessing this dialog box, see *Adding a POS Transaction Source* above.
2. In the Properties area, define the following:
   - **Name:** enter a name for the data format.
   - **Description:** enter a description of the data format.
   - **Transaction Start Text:** (required) enter the text that identifies the start of each transaction from

the POS transaction source.

- **Transaction End Text:** (optional) enter the text that identifies the end of each transaction.
- **Encoding:** Select the encoding used by the POS transaction source.

3. Capture data from the transaction source. Perform any of the following to capture raw data of the source data format:

   The following figure shows raw transaction data on the left and filtered transaction data on the right.

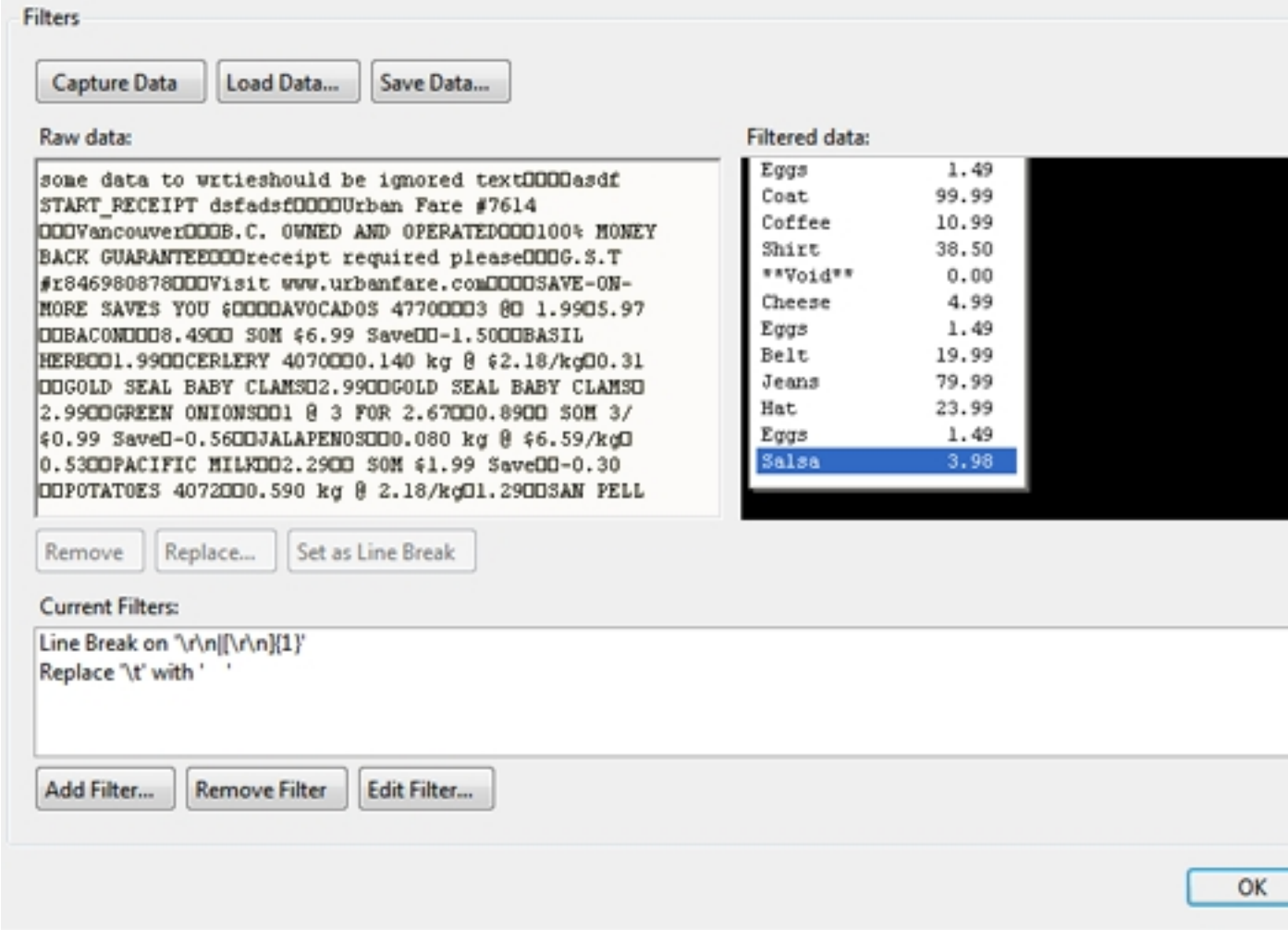


Figure 9: The Configure Data Format dialog box

- Click **Capture Data** to start capturing a raw transaction data sample.
- Click **Stop Capture** to stop capturing transaction data.
- Click **Load Data...** to load raw transaction data from a file.
- Click **Save Data...** to save a copy of the transaction data that has been captured.

4. To create a new filter for the raw transaction data file, click **Add Filter...**. The Configure Filter dialog box is displayed.

   There are two default filters in the Current Filters: area — one to create line breaks and the other to delete extra white space at the beginning of each line. If you do not need extra filters, skip this step.

a. In the **Text:** field, enter text for the filter to search for.
b. Select the **Match case** and/or **Match whole word** check box to focus the text filter to only find text with the same capitalization or an exact match.
c. In the **Method:** drop-down list, select a search method. You can choose to filter text found through a **Normal** search, **Wildcards** search, or **Regular expressions** search.
d. In the **Action to Take:** area, select the action the system will take when the filter finds a match to your text criteria.
e. Click **OK**.

5. On the Configure Data Format screen, click **OK** to add the new data format to the data format list.

Adding a Transaction Exception

NOTE: POS transaction exceptions are shared across a site.

To help monitor unusual transactions, you can set up transaction exceptions. Transaction exceptions can help you identify unauthorized discounts, fake returns, and manual price overrides.

1. In the POS Transactions Setup wizard, click  when you arrive on the Set Transaction Exceptions page.

   For information about accessing this page, see *Adding a POS Transaction Source* on page 66.

2. In the Configure Exception dialog box, enter a name for the exception.
3. Select one of the Text to Match options:
   - **Match Text** — Enter text that will be monitored as a transaction exception.

     The system will monitor all transactions for the text entered in the **Text to Match** field.

   - **Match Value** — Enter the value that triggers the transaction exception. You can use the relational operators from the drop-down list, and further define the value by entering any text that may appear before or after the value.

     The exception will monitor all transactions for values that match what you enter in the **Text Before Value:**, **Match when value:**, and **Text After Value:** fields.

4. Click **OK**.

The new transaction exception is added to the Set Transaction Exceptions page.

Repeat this procedure until all the required transaction exceptions have been added to the transaction source.

Editing and Deleting a POS Transaction Source

1. In the server Setup tab, click  .

   The POS Transactions dialog box is displayed.

2. In the POS Transactions dialog box, select a POS transaction source, then do one of the following:

   - To edit the POS transaction source, click . Go through the POS Transactions Setup wizard and make the required changes on each page. On the last page, click to save your changes.

     For details about the editable options, see *Adding a POS Transaction Source* on page 66.

   - To delete the POS transaction source, click .

     When the confirmation dialog box is displayed, click **Yes**.

Setting Up License Plate Recognition

The License Plate Recognition (LPR) settings are only available if you have the feature licensed for your site and installed on the server.

There are two types of licenses: LPR5 and LPR6. A site can have both LPR5 and LPR6 licenses, but only one type of license can be used per server. For more information about adding an LPR license to your site, see *Licensing the Site* on page 54.

1. In the server Setup tab, click  .

   The License Plate Recognition dialog box is displayed.

2. Select a lane from the License Plate Lane list.

   The number of lanes listed is determined by the number of License Plate Recognition (LPR) channels that are available on the server.

3. Complete the following fields:

   - **Name:** enter a name for the lane.
   - **Camera:** select the camera that will perform LPR. One camera can be used for multiple lanes.
   - **License Plate Configuration:** select the regional license plate format that needs to be recognized by the camera. For more information, see *Supported License Plates* on page 199.
   - **Pre-Event Record Time:** enter the amount of time that video is recorded before the license plate is recognized.
   - **Post-Event Record Time:** enter the amount of time that video is recorded after the license plate is recognized.

- **Minimum Confidence:** move the slider to set the minimum confidence required for a detected license plate to be recognized. The default value is 80%.
- Select the **Enable this lane** check box to enable LPR on this lane.
- **Max Image Analysis Rate:** enter an image rate between 1 – 60 ips. This specifies the maximum frame rate analyzed by the LPR service. The default value is **15**.
    - If this setting is higher than the camera's image rate, the LPR service will analyze all frames from the camera, increasing the processing time.
    - If this setting is lower than the camera's image rate, the system will reduce the number of frames it analyzes, reducing the processing time.

4. Move and adjust the green overlay until it spans the width of the traffic lane in the camera's field of view. LPR is only performed in the green area.

   NOTE: If the overlay is red, the license plate detection area is too large and cannot be used.

5. Click **OK**.

LPR is now configured for your site and you can add and update your Watch Lists. For more information, see *Adding a Watch List* on page 48.

Storage Management

To maintain a copy of the video recorded in your system, you can archive the video into Avigilon Backup (AVK) format. AVK files can be opened in the Avigilon Control Center Player and re-exported as needed.

Video archiving can be configured to occur continuously or on demand.

If you are running the ACC Server software on a network video recorder, you need to enable the Storage Management feature in the Avigilon Control Center Admin Tool. The Admin Tool is also where you manually set the video archive location. For more information, see *The Avigilon Control Center Server User Guide*.

If you are running an Avigilon Edge Solution device, like the H4 ES camera, you would enable archiving through the product web interface.

If you only want to archive an individual event, it is recommended that you export the video instead. For more information, see *Export* on page 173.

Enabling Continuous Archive

You can enable the Storage Management Continuous Archive feature to automatically archive video to the archive directory in hourly blocks during the configured time frame.

Archived video is accessible when you playback recorded video from the ACC Client software. For more information, see *Playing Recorded Video with the Timeline* on page 145.

Archived video is stored in Avigilon Backup (AVK) format, so you can also review archived video in the ACC Player software.

It is highly recommended that you set up the Storage Management Continuous Archive feature to work with video data aging. By configuring the two features together, you can create a tiered storage configuration to help manage the amount of video retained on the local ACC Server. Review your video data aging settings in the Recording and Bandwidth dialog box, and set up the Storage Management Continuous Archive feature to begin archiving before data aging starts. This helps ensure that you always have high bandwidth quality video of important events, while the ACC Server continues to have space for new recordings.

NOTE: Ensure that the Archive video older than: parameter is set so that archiving to the archive directory starts and completes before data is deleted on the local ACC Server. Best practice is to set the Archive video older than: parameter to at least one day less than the value set for video data aging to account for retries if the network connection is restricted or degraded.

For more information about data aging, see *Recording and Bandwidth* on page 64.

NOTE: The configured archiving schedule occurs in the server's local time and not the client's local time.

1. In the server Setup tab, click .

   The Storage Management dialog box is displayed.

   NOTE: If you see an error message, the Storage Management feature must be enabled in the Avigilon Control Center Admin Tool or Edge Solution device web interface first. That is also where you select the preferred archive directory.

   If you are running the ACC Server software on a network video recorder, see *The Avigilon Control Center Server User Guide* for more information.

   If you are running an Edge Solution device, refer to the device user guide for more information.

2. Select the **Enable Continuous Archive** check box.
3. In the Camera(s) to Archive: list, select the device video to include in the archive.
4. In the Options area, define the following:
   - **Archiving permitted:** specify the time frame when Continuous Archive is permitted.

     If you want archiving operations to occur 24 hours each day (including retries), specify the time frame to be **00:00** to **23:59**.

     The time specified is in the server's local time. If you are physically located in a different time zone from the server, remember to consider the time difference.

   - **Archive video older than:** the minimum age of recorded video before it is archived (in days).

     Ensure the minimum age specified here is less than the age specified in the Recording and Bandwidth dialog box for deleting High Bandwidth video on the local ACC Server. A one day difference is sufficient to account for retries if the network connection is restricted or degraded. For example, if the Recording and Bandwidth dialog box marks that the system will maintain 10 days of High Bandwidth video on the local ACC Server, enter **9** or less.

     Tip: Recorded video remains in the site until it is removed by data aging.

     For more information, see *Recording and Bandwidth* on page 64.

   - **Delete oldest archives when disk full:** check this box to automatically delete the oldest archive files when the archive storage location is full.

     NOTE: Disable this setting if your storage is managed by a disk system.

5. Click **OK**.

   The Status area displays when the next archive will occur.

Each video archive is saved in a subfolder within the configured archive directory, and is named after the archive start date and time.

If an error occurs during the archiving process, or if a network issue makes the destination folder temporarily unavailable, the ACC system will automatically retry archiving.

Resetting Continuous Archive

If you disabled continuous archive for longer than the Archive video older than: setting and want to re-enable continuous archive, the ACC system will start archiving video from the last successful archive date. To archive video starting from the hour before the Archive video older than: setting, reset the continuous archive feature.

1. In the server Setup tab, click .

   The Storage Management dialog box is displayed.

2. Click **Reset Continuous Archive**.
3. A dialog box displays the date video will be archived from. Click **OK**.

   The continuous archive feature is reset.

Archiving Recorded Video On Demand

Storage Management must be enabled in the Avigilon Control Center Admin Tool or Edge Solution device web interface before you can archive video from the ACC Client.

Files are always archived in Avigilon Backup (AVK) format. You can review archived video in the Avigilon Control Center Player.

Once Storage Management is enabled, you can trigger the system to archive video as required. You can archive video from any number of cameras in your system, and for an extended time range.

1. In the New Task menu, click .

   The Archive tab is displayed.

2. In the System Explorer, select all the cameras you want to archive.

   NOTE: You can only archive video from one server at a time.

3. In the **Archive Options** area, set the time range of the archive.

   The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to change the time range.

4. Select the **Delete oldest archives when disk full** check box to allow the application to automatically overwrite old archive files when the archive folder is full.

   NOTE: If this check box is selected, both on-demand and continuous archives may be overwritten — even if the **Delete oldest archives when disk full** setting is disabled in the Server Storage Management Continuous Archive settings.

5. Click **Start Archiving**.
6. When the archive is complete, click **OK**.

Each video archive is saved in a subfolder that is named after the archive time range.

Enabling Server-Based Analytics

Server-based analytics is a feature that enables Classified Object video analytics for cameras without analytics capabilities. To use this feature, you need an Avigilon video analytics appliance.

1. In the server Setup tab, click  .
2. In the following dialog box, a list of connected cameras are displayed.

   Only cameras without the Classified Object video analytics mode enabled are displayed.

   If you do not have access rights for a camera, it will not be shown in this list.
3. To enable Classified Object video analytics, select the check box beside the connected camera. If you have an Avigilon Artificial Intelligence (AI) Appliance, enabling video analytics also enables the Avigilon Appearance Search feature.

   The Total Analytic Load bar displays the appliance's video analytics capacity. The percentage is based on the enabled camera's current Compression and Image Rate settings. You cannot exceed a Total Analytic Load of 100%.
4. Click **OK**.

   Your settings are now saved.

Classified Object events can now be set up for the enabled cameras from the camera's Setup tab.

Enabling the Avigilon Appearance Search™ Feature

With the Avigilon Appearance Search feature, operators can find all instances of a person or vehicle in recorded video quickly and easily. To use the Avigilon Appearance Search feature, you need one of the following:

a. An NVR with a GPU for use with cameras that support the Avigilon Appearance Search feature.

b. An NVR connected to an Avigilon Artificial Intelligence (AI) Appliance for use with cameras without Classified Object video analytics.

If you have an Avigilon Artificial Intelligence (AI) Appliance, the Avigilon Appearance Search feature is automatically enabled when server-based video analytics are applied to a camera. For more information, see *Enabling Server-Based Analytics* above.

If you have cameras that support the Avigilon Appearance Search feature, do the following:



1. In the server Setup tab, click .

   The Appearance Search dialog box displays a list of connected cameras that support the Avigilon Appearance Search feature.

   If you do not have access rights for a camera, it will not be shown in this list.

2. To enable the Avigilon Appearance Search feature, select the check box beside the camera. The Load for each camera is proportional to the amount of activity in the camera's field of view.

   The Total Appearance Search Load bar displays an estimate of the server's analytics service load based on the amount of data that each enabled camera may generate. When the load exceeds 100%, search results might be missed.

   You can view the status of your analytics service in the Site Health tab. For more information, see *Monitoring Site Health* on page 9.

3. Click **Apply** or **OK**.

   Your settings are saved.

Tip: You can also enable and disable the Avigilon Appearance Search feature for an individual camera in the device's Analytics settings.

Device Settings

Device settings are used to adjust video quality and set up devices that can be connected to cameras and Avigilon video analytics appliances. These settings include adjusting camera display quality, video compression and image rate.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

General

Use the device General dialog box to set a device's identity, select the analytics mode, and configure device PTZ settings. You can also reboot the device through the General dialog box.

Setting a Device's Identity

In a device's General dialog box, you can give the device a name, describe the device's location and give the device a Logical ID. The Logical ID is needed to control the device through keyboard and joystick commands.

1. In the device Setup tab, click  .

   The General dialog box is displayed.

   NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

2. In the **Device Name:** field, give the device a meaningful name to help you identify it. By default, the device model number is used as the device's name.
3. In the **Device Location:** field, describe the device's location.
4. In the **Logical ID:** field, enter a unique number to allow the Client software and integrations to identify this device. By default, the device's Logical ID: is not set and must be manually added.

   Tip: If **Display LogicalIDs** is enabled in Client Settings, the device's Logical ID will appear beside the device's name in the System Explorer.

5. (Cameras only) To disable the LEDs on a device, select the **Disable device status LEDs**. This may be required if the device is installed in a covert location.
6. Click **OK**.

Analytics Mode

If you have a self-learning video analytics device, you can select which analytics mode you want to enable.

The **Classified Object** mode detects and classifies objects such as a person or a vehicle. You can set up rules and alarms based on this detection.

The **Unusual Motion** mode detects motion and compares the speed, direction, and location of movement with what is typical for a scene. It displays anomalies and lets users view activity that would not otherwise be seen using traditional pixel-based motion detection.

To use Unusual Motion mode, you need:

- A camera with Unusual Motion Detection video analytics.
- The ACC Client software version 6.8 or later.
- The ACC Server software version 6.8 or later.

Tip: If you have an ACC ES Analytics Appliance, you can enable both analytics modes. In the device Setup tab enable Unusual Motion mode and in the server Setup tab enable server-based analytics. For more information, see *Enabling Server-Based Analytics* on page 73.

Enabling an Analytics Mode

Enable Classified Object or Unusual Motion mode for a video analytics device.

1. In the device Setup tab, click .

   The General dialog box is displayed.

2. In the Video Analytics Mode: drop-down list, select one of the following:
   - To enable Classified Object Detection, click **Classified Object**.
   - To enable Unusual Motion Detection, click **Unusual Motion**.
   - To disable analytics for cameras that only support Unusual Motion mode, click **None**.
3. Click **OK**.

   The analytics mode is enabled.

Configuring PTZ

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

Use the camera General dialog box to enable and configure the motorized pan, tilt, zoom (PTZ) devices that may be connected to Avigilon cameras. PTZ devices are connected to Avigilon cameras through the RS-485 inputs.

Third-party PTZ camera controls cannot be configured through the Avigilon Control Center software.



1. In the camera Setup tab, click .

   The General dialog box is displayed.

2. In the PTZ area, select the **Enable PTZ controls** check box.

   NOTE: If the features described in the following steps are not displayed, the camera only has a motorized zoom and focus lens. You will be able to control the zoom and focus settings through the PTZ Controls pane but other PTZ controls will not be available.

3. In the **Protocol:** drop-down list, select the appropriate PTZ protocol. The available protocols include:
   - AD Sensormatic
   - AXSYS
   - AXSYS DCU
   - Ernitec ERNA
   - Honeywell Diamond
   - Kalatel ASCII
   - Pelco D
   - Pelco P

- TEB Ligne
- Videotec MACRO
- Videotec Legacy
- Vicon extended
- Vicon normal
- JVC JCBP

4. Enter the **Dip Switch Address:**, **Baud Rate:**, and **Parity:** for the PTZ device.
5. Click **OK**.

Once PTZ has been configured, you can use the camera's PTZ Controls while you watch the camera's live video stream. For more information, see *Controlling PTZ Cameras* on page 129.

Changing the Camera Operating Priority

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

Depending on the scene, you may want the camera to maintain a specific frame rate rather than use all the available features. Or the reverse.

Choose what the camera should prioritize during normal operations.

1. In the device Setup tab, click  .

   The General dialog box is displayed.
2. From the **Mode:** drop-down list, select one of the following:
   - **High Framerate** — the camera will hold the preferred image rate as the priority.

     The camera will stream at the configured image rate even if it is unable to use other features supported by the camera. Depending on the camera model, disabled features may include self-learning video analytics, WDR and edge storage.
   - **Full Feature** — the camera will maintain the function of all supported features as the priority.

     The camera will dedicate more processing power towards maintaining the function of its key features, and use an optimized image rate. Depending on the camera feature, the image rate may be capped down to less than half the configured image rate.
3. Click **OK**.

Rebooting a Device

You can restart all Avigilon devices through the device's General dialog box. This feature is not available for third party devices.

1. In the device Setup tab, click  .

   The General dialog box is displayed.

2. Click **Reboot Device...**.

The device will disconnect from the Avigilon Control Center system and shut down. When the device starts up again, the device should automatically reconnect with the server it was previously connected to.

Network

Use the device Network dialog box to change how a device connects to the server network.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

1. In the device Setup tab, click  .

   The Network dialog box is displayed.

2. Select how the device obtains an IP address:
   - **Obtain an IP address automatically:** select this option for the device to connect to the network through an automatically assigned IP address.

     The device will attempt to obtain an address from a DHCP server. If this fails, the device will obtain an address through Zero Configuration Networking (Zeroconf) and select an address in the 169.254.0.0/16 subnet.

   - **Use the following IP address:** select this option to manually assign a static IP address to the device.

     Enter the **IP Address:**, **Subnet Mask:**, and **Gateway:** you want the device to use.

3. Select the **Control Port:** for connecting to the device. This port is also used for manually discovering the device on the network.
4. (Cameras only) Select the **Enable Multicast** check box to enable multicast streaming from the device. You must Enable Multicast to set up redundant recording to multiple servers.

   Use the default generated **IP Address:**, **TTL:**, and **Base Port:**, or enter your own values.

5. Click **OK**.
6. (Rialto Video analytics appliance only) When prompted, allow the system to restart the device.

Image and Display

Use the Image and Display dialog box to control a camera's display settings for live and recorded video.

An image histogram is provided at the bottom of the window to help you configure your settings.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

Changing Image and Display Settings



1. In the camera Setup tab, click .

   The Image and Display dialog box is displayed.

   NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

2. Use the focus controls to focus the camera. For more information, see *Zooming and Focusing the Camera Lens* on page 81.

3. Click to toggle the Auto Contrast Adjustment.

   This setting changes the contrast of the video displayed in this dialog box. It does not affect recorded video or video displayed in other views. By default, Auto Contrast Adjustment is off.

4. If the camera supports day/night control, select one of the following options from the **Day/Night Mode:** drop-down list:
   - **Automatic** — allow the camera to control the infrared cut filter based on the amount of light in the scene.

     If available, move the **Day/Night Threshold:** slider to set the exposure value (EV) when the camera changes from day to night mode.
   - **Day Mode** — the camera will only stream in color and the IR cut filter is disabled.
   - **Night Mode** — the camera will only stream in monochrome and the IR cut filter is enabled.

5. Adjust the camera's image settings to best capture the scene. A preview of your changes are displayed in the image panel and the histogram.

   Tip: Use the **Maximum Exposure:**, **Maximum Gain:**, and **Priority:** options to control low light behavior.

Option	Description
Synchronize Image Settings with All Heads (Avigilon HD Multisensor Dome Cameras Only)	You can apply the same image settings to all camera heads by selecting this check box. **NOTE:** Zoom and focus settings must be set individually.
Exposure:	You can allow the camera to control the exposure by selecting **Automatic**, or you can set a specific exposure rate. **NOTE:** Increasing the manual exposure time may affect the image rate.
Iris:	You can allow the camera to control the iris by selecting **Automatic**, or you can manually set it to **Open** or **Closed**.

Option	Description
Maximum Exposure:	You can limit the automatic exposure setting by selecting a **Maximum Exposure:** level. By setting a **Maximum Exposure:** level for low light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images.
Maximum Gain:	You can limit the automatic gain setting by selecting a **Maximum Gain:** level. By setting a **Maximum Gain:** level for low light situations, you can maximize the detail of an image without creating excessive noise in the images.
Color Palette:	You can change how information captured from thermal cameras is represented by selecting a **Color Palette:**. **WhiteHot** – Grayscale. White represents hot, black represents cold. **BlackHot** – Grayscale. Black represents hot, white represents cold. **Rainbow** – Multicolor. Red represents hot, blue represents cold.
Priority:	You can select **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera will maintain the set image rate as the priority, and will not adjust the exposure beyond what can be recorded for the set image rate. When set to **Exposure,** the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible.
Flicker Control:	If your video image flickers because of the fluorescent lights around the camera, you can reduce the effects of the flicker by setting the **Flicker Control:** to the same frequency as your lights. Generally, Europe is **50 Hz** and North America is **60 Hz**.
Backlight Compensation:	If your scene has areas of intense light that cause the overall image to be too dark, move the **Backlight Compensation:** slider until you achieve a well exposed image.
Enable Wide Dynamic Range	Select this box to enable automatic color adjustments through Wide Dynamic Range (WDR). This allows the camera to adjust the video image to accommodate scenes where bright light and dark shadow are clearly visible.
Enable Adaptive IR Compensation	Select this box to enable automatic infrared adjustments through Adaptive IR Compensation. This allows the camera to automatically adjust the video image for saturation caused by IR illumination.
Saturation:	You can adjust the video's color intensity by moving the **Saturation:** slider until the video image meets your requirements.

Option	Description
Sharpening:	You can adjust the video sharpness to make the edges of objects more visible. Move the **Sharpening:** slider until the video image meets your requirements.
Image Rotation:	You can change the rotation of captured video. You can rotate the video 90, 180, or 270 degrees clockwise.
White Balance	You can control white balance settings to adjust for differences in light. You can allow the camera to control the white balance by selecting **Automatic White Balance**, or select **Custom White Balance** and manually set the **Red:** and **Blue:** settings.

Click **Apply to Devices...** to apply the same settings to other cameras of the same model.

6. Click **OK**.

Zooming and Focusing the Camera Lens

If the camera has remote zoom and focus capabilities, you can control the camera's zoom and focus through the Image and Display dialog box.

1. In the camera Setup tab, click  .

   The Image and Display dialog box is displayed.

2. If the camera has a built-in auto-focus feature, you can choose one of the following:
   - **Continuous Focus** — the camera will automatically focus itself whenever the scene changes. Skip the following steps.
   - **Manual Focus** — you can manually focus the camera through the **Focus:** buttons. Once the focus is manually set, it will not change.
3. While you watch the preview in the image panel, complete the following steps to zoom and focus the camera:

   Tip: For Avigilon HD Pro Cameras, the lens must be set to auto-focus (AF) mode on the camera. If the camera does not detect the lens, the Focus: buttons are not displayed.

   a. Use the **Zoom:** buttons to zoom in to the distance you want to focus.
4. In the **Iris:** drop-down list, select **Open**. When the iris is fully open, the camera's depth of field is the shortest.

5. Use the **Focus:** buttons until the image becomes clear.

Button	Description
Auto Focus	The camera will automatically focus one time.
	The camera will focus as close to zero as possible.
	Large step toward zero.
	Small step toward zero.
	Small step toward infinity.
	Large step toward infinity.
	Infinity.

   Click **Apply to Devices...** to apply the same settings to other cameras of the same model.

6. Click **OK**.

Measuring Pixels in the Field of View

When setting up a camera for video analytics or License Plate Recognition (LPR), it is important to have a minimum number of pixels in the target area to improve detection results. For example, you may want to ensure that there are enough pixels to detect a person's face or a license plate in the field of view (FoV).

For cameras that have video analytics or LPR enabled, you can measure the number of pixels in a target area using the ACC Client.

For pixel guidelines, refer to the following documents on **avigilon.com**:

- *Designing a Site with Avigilon Video Analytics Guide*
- *H4 LPC Camera Kit and ACC 6 License Plate Reader Engine Site Design Guide*

NOTE: This feature is only available for:

- Video analytics cameras. Fisheye cameras and cameras connected to a video analytics appliance are not supported.
- Cameras associated to a lane with the **Enable this lane** check box selected.

To measure pixels:

1. In the camera Setup tab, click  .

   The Image and Display dialog box is displayed.

2. In the toolbar, click .

   A purple overlay appears over the camera's FoV. The live video is paused so you can measure the number of pixels an object of interest covers within the FoV.

3. To resize the overlay, click and drag the corners.
4. To move the overlay, click and drag within the overlay.

   The number of pixels used for video analytics, LPR, or both applications is displayed. The number of pixels may differ for each application depending on the camera resolution.

   NOTE: While using the pixel measuring tool, you cannot edit other Image and Display settings.

5. Click  to hide the pixel measuring overlay and continue streaming live video.

Dewarping a Fisheye Lens

If your camera uses a supported fisheye or panomorph lens, you may choose to dewarp the image through the Avigilon Control Center software.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.



1. In the camera Setup tab, click .
2. In the **View Perspective:** drop-down list, select one of the following options:
   - **Floor:** select this option if the camera is installed to look up.
   - **Ceiling:** select this option if the camera is installed to look down.
   - **Wall:** select this option if the camera is installed to look at the horizon.
3. If available, edit the Image and Display settings.
4. Click **OK**.

The system dewarps the lens image based on the way it is installed. You will be able to control how video is displayed in an image panel through the PTZ controls.

Configuring Infrared LEDs

You can enable or disable infrared (IR) LEDs on the H4 Multisensor camera's exterior from the ACC Client software. Disable IR LEDs to prevent reflections off nearby objects like walls or posts from compromising a camera's image.

1. In a View tab, open the camera in an image panel.
2. Right-click the image panel and select **Infrared LEDs...**.
3. In the following popover:
    - Select the IR LEDs you want to enable.
    - Clear the IR LEDs you want to disable.
4. Click **Apply**.

    The selected LEDs are enabled.

Compression and Image Rate

Use the camera Compression and Image Rate dialog box to modify the camera's frame rate and image quality settings for sending image data over the network.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the camera Setup tab, click 

.

    The Compression and Image Rate dialog box is displayed.

    The Total Camera Bandwidth: area gives an estimate of the bandwidth used by the camera with the current settings. Adjust the settings as required.

    NOTE: For cameras capable of maintaining multiple streams, the settings in this dialog box only affect the primary stream.
2. In the **Format:** drop-down list, select the preferred streaming format.
3. In the **Image Rate:** bar, move the slider to select the number of images per second (ips) you want the camera to stream over the network.

    For H.265 and H.264 cameras and encoders, the image rate setting must be divisible by the maximum image rate. If you set the slider between two image rate settings, the application will round to the closest whole number.
4. In the **Image Quality:** drop-down list, select an image quality setting. An image quality setting of **1** will produce the highest quality video and require the most bandwidth. The default setting is **6**.
5. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in kilobits per second (kbps).
6. In the **Resolution:** drop-down list, select the preferred image resolution.
    NOTE: For thermal cameras, use the default resolution for enhanced video quality.
7. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe.

    To help you determine how frequently keyframes are recorded, the Keyframe Period: area tells you the amount of time that passes between each recorded keyframe.

    It is recommended that you have at least one keyframe per second.

8. If your camera supports multiple video streams, you can select the **Enable Low Bandwidth Stream** check box. Depending on your version of the software, the check box may also be called "Enable secondary stream".

   When enabled, the lower resolution video stream is used by the HDSM™ feature to enhance bandwidth and storage efficiencies.

9. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
10. Click **OK**.

Manually Adjusting Recorded Video Streams

Avigilon and third party ONVIF compliant cameras support the configuration of secondary stream compression settings.

If you have a 1-3 megapixel Avigilon H4 HD camera, you also have the option of manually adjusting the primary and secondary video stream, or allowing the system to automatically use HDSM technology. HDSM technology allows ACC software to automatically record both the primary and secondary stream so that the system can intelligently adjust video bandwidth and storage efficiencies to meet your requirements.

If your local regulations require that a specific video stream be recorded or be a certain resolution, you have the option of manually adjusting the settings to meet the requirements.

NOTE: If the camera is connected to multiple servers (including for failover), the following settings must be the same at each server connection. Otherwise, the settings may constantly overwrite each other and the camera is unable to record the correct video stream settings.

1. In the Compression and Image Rate dialog box, select the preferred bandwidth you want the camera to record from the Recording Profile: drop-down list. From the Recording Profile: drop-down list, select Record High Bandwidth or Record Low Bandwidth. Selecting Record High Bandwidth enables streaming and the recording of the High Bandwidth Stream, while viewing the live low profile stream.

   NOTE: The option for selecting Record High Bandwidth or Record Low Bandwidth is applicable to third party ONVIF compliant cameras only.

   The High Bandwidth Stream is automatically disabled for recorded video but the settings are still available for you to configure the live video stream. The Low Bandwidth Stream settings are enabled.

2. The default HDSM Auto option allows the system to use the HDSM feature for viewing live and recorded video. Be aware that if you are using the Manual setting, HDSM technology is disabled for recorded video but is still used for live video streams. If you are using the Flexible setting, HDSM technology is enabled for recorded video and can still be used for live video streams. Selecting the Flexible setting only enables the control in the **Max Bit Rate:** field and the **Resolution:** drop-down list.
3. If you need to adjust the live video stream, change the High Bandwidth Stream settings first.

   The High Bandwidth Stream settings are used to optimize the Low Bandwidth Stream settings, so some of the settings may change depending on your settings for the High Bandwidth Stream.

4. If it is not displayed, click  to display the Low Bandwidth Stream settings.

   If you prefer to record a higher resolution video, clear the **Enable Low Bandwidth Stream** check box and adjust the High Bandwidth Stream settings.

5. In the **Resolution:** drop-down list, select the preferred image resolution.

6. In the **Image Rate:** bar, move the slider to select the number of images per second (ips) you want the camera to stream over the network.
7. In the **Image Quality:** drop-down list, select an image quality setting. An image quality setting of **1** will produce the highest quality video and require the most bandwidth. The default setting is **6**.
8. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in kilobits per second (kbps).
9. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe.

   To help you determine how frequently keyframes are recorded, the Keyframe Period: area tells you the amount of time that passes between each recorded keyframe.

   It is recommended that you have at least one keyframe per second.
10. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
11. Click **OK**.

The changes immediately take effect. The ACC Client software will continue to use HDSM technology to manage the display of live video, but recorded video will only display the configured video stream.

The data aging settings in the Recording and Bandwidth dialog box update to reflect the new recording profile settings.

Enabling Idle Scene Mode

NOTE: Only available to cameras that support this feature.

Idle scene mode offers the option to record video at a different frame rate and quality if there are no motion events detected in the scene.

A motion event is when the camera uses its Pixel Motion Detection or Classified Object Motion Detection ability to identify significant events in the scene. For more information, see *Motion Detection* on page 102.

Idle scene mode is typically used to set the camera to stream at a lower image rate and reduced quality to lower the bandwidth and storage used when the scene is idle.

NOTE: If the camera setting is updated to stream in MJPEG format, you may have to close and re-open the Compression and Image Rate dialog box to view the Idle Scene Mode options.

1. In the Compression and Image Rate dialog box, select the **Enable Idle Scene Mode** check box.

   The Idle Scene Mode settings are displayed. If the settings do not automatically display, click  to reveal the settings.
2. In the **Post-Motion Delay:** field, enter the amount of time in seconds the scene must be idle before it switches to idle scene mode.
3. In the following **Image Rate:** bar, move the slider to select the number of images per second (ips) you want the camera to stream while the scene is idle.
4. In the **Image Quality:** drop-down list, select the video image quality when the camera is in idle scene mode.
5. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in this mode.

6. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe.

   To help you determine how frequently keyframes are recorded, the Keyframe Period: area tells you the amount of time that passes between each recorded keyframe.

7. Click **OK** to save your settings.

Next time the camera's field of view becomes quiet or idle, the camera will automatically switch to idle scene mode. The camera will automatically switch back to standard streaming mode when motion events are detected in the scene.

Enabling HDSM SmartCodec™ Technology Settings

NOTE: Only available to cameras that support this feature.

HDSM SmartCodec technology operates by separating foreground objects from the background image, then reduces bandwidth by increasing compression to the background image. In this way, higher quality image is retained for objects of interest in the foreground while reducing bandwidth for static backgrounds. When there is no motion in the scene, HDSM SmartCodec feature switches the camera into idle scene mode to increase bandwidth savings when there are no objects of interest.

HDSM SmartCodec feature uses the camera's motion detection area to help define when it should switch to idle scene mode. You can configure the motion detection area from the Motion Detection dialog box. For more information, see *Motion Detection* on page 102.

1. In the Compression and Image Rate dialog box, select the **Enable HDSM SmartCodec** check box.

   The HDSM SmartCodec settings are displayed. If the settings do not automatically display, click  to reveal the settings.

2. In the **Bandwidth Reduction:** drop-down list, select one of the following options:
   - **Low**
   - **Medium**
   - **High**
   - **Custom**

   If the scene background does not provide any valuable information, for example a white hallway, choose **High** to enhance bandwidth savings. If the scene background may cause objects of interest to behave differently, for example a traffic intersection, choose **Low**. This setting provides you with some bandwidth savings, while maintaining enough background clarity to see events in full context.

3. In the **On Motion:** section, choose the preferred **Background Image Quality:** option.

   An image quality setting of **1** will produce the highest quality background image but require the most bandwidth.

   When motion activity is detected, the foreground areas of the video are streamed and recorded using the High Bandwidth Stream settings while the background areas use the Background Image Quality: setting.

4. In the **On Idle Scene:** section, enter the **Post-Motion Delay:** setting in seconds. This field defines how long the scene must be idle before it switches to idle scene mode.

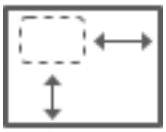
5. In the following **Image Rate:** bar, move the slider to select the number of images per second (ips) you want the camera to stream while the scene is idle.
6. In the **Image Quality:** drop-down list, select the video image quality when the camera is in idle scene mode. This setting is applied to the foreground and background image.
7. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in this mode.
8. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe.

   To help you determine how frequently keyframes are recorded, the **Keyframe Period:** area tells you the amount of time that passes between each recorded keyframe.
9. Click **OK** to save your settings.

Image Dimensions

Use the Image Dimensions dialog box to set the image dimensions for the camera. You can crop the video image to help reduce bandwidth and increase the maximum image rate.

NOTE: This feature is only available for JPEG2000 cameras.

1. In the camera Setup tab, click  .

   The Image Dimensions dialog box is displayed.
2. Adjust the image dimensions by doing one of the following:
   - Drag the edges of the image until the video is cropped to fit your requirements.
   - Change the values for the **Top:**, **Left:**, **Width:**, and **Height:** fields.
3. Click **OK**.

Teach By Example

For most scenes, the Avigilon self-learning feature is all that is required for the video analytics device to learn the scene and accurately classify objects of interest. In exceptional situations where self-learning should be disabled, the Teach By Example feature can be used to help refine classified object detection.

The Teach By Example feature lets you provide feedback on the accuracy of classified objects by reviewing recorded video and assigning Teach Markers to detected objects. Teach Markers can be assigned then applied to devices by different users. Users who assign markers typically monitor video on a regular basis. You must assign 30 True Teach Markers and 30 False Teach Markers before they can be applied to a device. Administrators, who may be less involved with day-to-day video monitoring, apply the Teach Markers to the device.

If new Teach Markers are applied to a device, any previously applied teach markers will be overwritten. To see when Teach Markers were last applied to a device, see *Viewing Teach Marker Status* on page 91.

For more information about when the self-learning feature should be enabled or disabled, see *Self-Learning on Video Analytics Devices* on page 98.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Teach By Example Recommendations

Teach By Example is a feature that allows users to provide feedback by validating the accuracy of classifications done by the system.

- Teach By Example is recommended if the system reports an undesirable number of false alarms after self-learning is complete or has been disabled.
- Teach By Example is not required, but can be used to help refine classification of people and vehicles to further reduce the number of false alarms.
- You can perform Teach By Example after self-learning is complete, or when self-learning is disabled.
- If you decide to disable self-learning after having executed a Teach By Example exercise, you may need to teach the system again to account for classified results that were previously filtered by self-learning.
- For changes in lighting, including the addition of infrared light, make sure you provide examples of true and false detections in the new lighting.
- Always restore the factory default Teach By Example settings after a camera is physically moved or adjusted, and if the focus or zoom level is changed. The change in the camera's field of view affects the video analytic results.

Assigning Teach Markers

Assign True or False Teach Markers to classified objects in recorded video to help increase a video analytics device's detection accuracy.

You need at least 30 True Teach Markers and 30 False Teach Markers per camera to teach a video analytics device. Each camera will accept a maximum of 200 True Teach Markers and 200 False Teach Markers.

You can assign Teach Markers to recorded video from Classified Object Motion search results.

NOTE: Assigned Teach Markers are local to a single server and are created for individual cameras. They are not shared between servers or cameras. Once applied, the Teach Markers are local to a camera and persist even if the camera changes servers.

1. Start a Classified Object Motion search in a region of interest (ROI) slightly larger than the ROI used for video analytics events from the same device. For more information, see *Performing a Motion Search* on page 166.
    - For True Teach Markers, use events that properly identify a person or vehicle without a specified duration or confidence level.
    - For False Teach Markers, use events that are longer than 2 seconds with a confidence level greater than 20%.
2. Click inside a Classified Object bounding box to display the Teach Markers menu and select whether the object is:
    - A **True Person**/**True Vehicle**.
    - A **False Person**/**False Vehicle**.
3. Assign at least 30 True Teach Markers and 30 False Teach Markers.

    To see how many Teach Markers have been assigned, go to the device's Setup page and click **Teach By Example**. A tally of the total assigned markers is displayed at the bottom of the Teach By Example tab.

Tip: For devices with minimal activity, if you cannot find 30 events to meet the minimum number of Teach Markers, increase the ROI for your search.

4. Review the Teach Markers and apply them to the device. For more information, see *Managing Teach Markers* below and *Applying Teach Markers to the Device* below.

You can also assign Teach Markers to a video analytics device by:

- Playing back recorded video in the Teach By Example tab until you encounter bounding boxes in the scene. For more information about controlling video playback, see *Playing Recorded Video with the Timeline* on page 145.
- Performing a , , or search, then selecting results that include bounding boxes. For more information about performing each of these searches, see *Search* on page 156.
- Locating an alarm linked to a video analytics device in the Alarms tab, then reviewing the Alarm Triggers until you identify one that includes bounding boxes. For more information about the Alarms tab, see *Monitoring Alarms* on page 152.

Managing Teach Markers

After you've assigned Teach Markers to a video analytics device, you can modify or delete them before they are applied to the device.



1. In the device Setup tab, click .

   The Teach By Example tab opens.

2. Review the assigned Teach Markers.
   - To edit Teach Markers:
     a. Select an item from the **Teach Markers** list.
     b. Click the related bounding box in the image panel then change the assigned object type.
   - To remove individual Teach Markers, click the related bounding box in the image panel then select **Not Used**.
   - To remove all Teach Markers, click **Clear All Markers**.

     This will delete all assigned Teach Markers, but not Teach Markers that were applied to the device.
   - To remove Teach Markers that were applied to the device, see *Removing Teach Markers from the Device* on the next page.
   - To see when Teach Markers were last applied to the device, see *Viewing Teach Marker Status* on the next page.

Applying Teach Markers to the Device

After the minimum number of Teach Markers have been assigned, you can apply the markers to the device. This sends the true and false detection details to the device. Once applied, the Teach Markers are local to a camera and persist even if the camera changes servers.

NOTE: This action will overwrite all previously applied Teach Markers on the device.



1. In the device Setup tab, click .

   The Teach By Example tab opens.

2. To apply all the Teach Markers to the video analytics device, click **Apply**.

   NOTE: You must have a minimum of 30 True Teach Markers and 30 False Teach Markers, or an error message is displayed.

   The Teach Markers are sent to the device, and the device will use these details to increase its detection accuracy.

The listed Teach Markers are removed from the list because they have been applied to the device. You can verify that the device was updated. For more information, see *Viewing Teach Marker Status* below.

Removing Teach Markers from the Device

If there are significant changes in the scene or if the camera is moved to a different location, you may want to remove the Teach Markers that have been applied to the device because the information is no longer accurate.



1. In the device Setup tab, click .

   The Teach By Example tab opens.

2. Click **Restore to Factory Default**.
3. When you are prompted, click **Yes**.

The device's teach data is restored to the factory default settings. To verify the settings were restored, see *Viewing Teach Marker Status* below.

If you have new Teach Markers assigned to the device, those markers are not deleted from the list. Only the markers that have already been applied to the device are removed.

Viewing Teach Marker Status

You can verify the last time Teach Markers were applied or restored to factory default from the device Setup tab.

1. In the device Setup tab, click  .

   The Settings dialog box opens.

2. In the Self Learning section, the **Teach Markers Applied:** field displays:
   - The date the Teach Markers were last applied.
   - If the Teach Markers are in the factory default state.

     NOTE: If your device is connected to a Rialto video analytics appliance or if you are using the ACC Server version 6.8 or earlier, the Teach Markers Applied: field displays **Unknown**.

Analytic Events

You can set up specific video analytics events on each Avigilon self-learning video analytics device. Devices can be configured to detect a variety of human and vehicle activity within a scene.

The configured events can be used to set up detailed rules. For more information, see *Rules* on page 53.

Adding Video Analytics Events

Before you can add video analytics events to rules and alarms, they must first be created for each video analytics device.

1. In the device Setup tab, click  .

   The Analytic Events dialog box opens.

2. Click . The Analytics Events: dialog box opens.
3. Enter a name for the video analytics event.
4. Select the **Enabled** check box. If the check box is clear, the video analytics event will not detect or trigger any events.
5. In the Activity: area, select one of the following options:

   NOTE: The option you select here will define the other settings that are displayed.

   - **Objects in area** – the video analytics event will be triggered when the selected object type moves into the region of interest.

     In the image panel, define the green region of interest. The green overlay can be configured like the Classified Object Motion Detection feature. For more information, see *Setting Up Classified Object Motion Detection* on page 104.

   - **Object loitering**– the video analytics event will be triggered when the selected object type stays within the region of interest for an extended amount of time.

     In the image panel, define the green region of interest.

- **Objects crossing beam** – the video analytics event will be triggered when the selected object type crosses the beam in the pointed direction.

  In the image panel, move or resize the green directional beam as needed:

  - To move the beam, click and drag the green beam in any direction.
  - To change the length or rotate the beam, click one end of the beam and stretch or rotate the beam.
  - To change the direction of the beam, click  .
  - To detect objects traveling in either direction of the beam, click  .

6. In the **Object Types:** area, select  and/or  .
7. Click **OK** to save your settings.

For more video analytic event options, click **Show Advanced Options**. For a description of the advanced options, see *Video Analytics Event Descriptions* on page 186.

Editing and Deleting Video Analytics Events

1. In the device Setup tab, click  .

   The Analytic Events dialog box opens.

2. Select an event from the Analytics Events: list and do one of the following:

   - To edit the video analytics event, click  . In the following dialog box, make the required changes. For more information, see *Adding Video Analytics Events* on the previous page.

     NOTE: If you change the name of the event, any rules or alarms linked to the event may no longer function.

   - To delete the video analytics event, click .

Privacy Zones

You can set privacy zones in the camera's field of view to block out areas that you do not want to see or record, like bathroom entrances and other private areas.

Adding a Privacy Zone

1. In the camera Setup tab, click .

   The Privacy Zones dialog box is displayed.

2. Click  and a green box will appear in the image panel.
3. Move and resize the green box until it covers the area you want to keep private.
4. Click **OK**.

Editing and Deleting a Privacy Zone

1. In the camera Setup tab, click .

   The Privacy Zones dialog box is displayed.

2. Select a privacy zone from the Privacy Zones: list and do one of the following:
   - To edit the privacy zone, adjust the green box in the image.
   - To delete the privacy zone, click .
3. Click **OK** to save your changes.

Manual Recording

When you trigger manual recording in an image panel, you are telling the camera to record video outside of its recording schedule. Manual recording continues until it is stopped, or until the maximum manual recording time is reached.

To set the maximum manual recording time, follow these steps:

1. In the camera Setup tab, click .

   The Manual Recording dialog box is displayed.

2. Define the following:
   - **Manual Recording Duration:** enter how long the camera should record if recording is not manually stopped.
   - **Pre-Trigger Record Time:** enter the amount of time video is recorded before manual recording is activated.

Click **Apply to Devices...** to apply the same settings to other cameras of the same model.

3. Click **OK**.

For more information on manually recording video, see *Triggering Manual Recording* on page 133.

Analytics Settings

The Analytics Settings dialog box is used for initial configuration for devices that include analytics capabilities, including Avigilon cameras with self-learning video analytics, Avigilon video analytics appliances, and devices with presence detection capabilities.

Configuring Classified Object Detection

Cameras with Classified Object Detection video analytics and cameras connected to ACC ES Analytics Appliances can be configured to better understand the scene where they are installed and improve classified object detection accuracy. This allows cameras to learn their surroundings and detect specific events.

To configure Classified Object Motion Detection for a video analytics camera, see *Setting Up Classified Object Motion Detection* on page 104.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the device Setup tab, click .

   The Settings dialog box opens.

2. From the **Analytics Scene Mode:** drop-down list, select the location that best describes where the camera is installed.

   The Analytics Scene Mode: setting helps the camera identify what it should be looking for.

   - **Outdoor** — this option is suitable for most outdoor environments. This setting optimizes the camera to identify vehicles and people.
   - **Outdoor High Sensitivity** — only use this option if you require the system to be more sensitive than the Outdoor setting. This option is optimized to run with higher sensitivity for detecting people and vehicles in challenging outdoor scenes. Be aware that this option will generate more false positives.
   - **Large Indoor Area** — this option only detects people and is optimized to detect people around obstructions, like chairs and desks, if the head and torso are visible.
   - **Indoor Overhead** — this option is optimized for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera FoV. Any movement is assumed to be human. It can be used in areas with limited space but with high ceilings, or to monitor doors. It should not be used with the Avigilon Appearance Search feature, or to detect people traveling against the crowd.

   NOTE: If you change the Analytics Scene Mode: setting after it has been set, the system will delete any data the device may have learned.

3. Select the **Display Classified Objects** check box to display bounding boxes around classified objects in live and recorded video.
4. In the Self Learning section:
    1. Check the **Enable Self Learning** box to enable self-learning.
    2. Clear the check box to disable self-learning. After self-learning is disabled, the camera stops self-learning and no longer utilizes any learned information.

        NOTE: Disabling self-learning may result in more classified objects being falsely detected.

    3. The Progress: status in the dialog box tells you the progress made so far.
    4. To reset self-learning, click **Reset**.
        - In the confirmation dialog box that appears, click **Yes**.

        NOTE: When self-learning is reset, all previous self-learning data for the device is deleted.
5. In the **Camera Type:** drop-down list, select the type of camera that has been connected to this camera channel.

    This helps the video analytics determine what type of image it should expect from the camera.

    - **Day and Night** — select this option if the camera can stream video in color or black and white. This type of camera typically displays color video during the day and black and white video at night to capture as much detail as it can of the scene.
    - **Color** — select this option if the camera can only stream video in color.
    - **Black and White** — select this option if the camera can only stream video in black and white.
    - **Thermal** — select this option if the camera can stream forward looking infrared (FLIR) video.
6. Move the **Sensitivity:** slider to define how sensitive the camera is to sudden changes in the scene.

    Tampering is defined as a sudden change in the camera field of view, usually caused by someone unexpectedly moving the camera. Lower the setting if small changes in the scene, like moving shadows, cause tampering events. If the camera is installed indoors and the scene is unlikely to change, you can increase the setting to capture more unusual events.
7. Select the **Trigger Delay:** value to define how long the camera will wait for tampering events to be sent.

    Trigger delay is defined as a temporary change in the camera field of view that may generate a tampering event due to a change in the scene. If the tampering ends before the trigger delay time has elapsed, no tampering events will be sent. If the time elapses but the tampering has not stopped, the events will be sent by the camera. The default setting is **8** and is a value in seconds from **2** and **30**.
8. Select the **Enable Appearance Search** check box if you want to use this camera with the Avigilon Appearance Search feature.

    NOTE: This option is only displayed if the camera is connected to a network video recorder that supports the Avigilon Appearance Search feature.
9. If the camera is too sensitive and falsely detects motion as classified objects, select the **Enable Noise Filter** check box .

    Disable this option if the camera is not sensitive enough.
10. Click **Apply** to save your settings.

Next, you can enable self-learning and configure analytics events. For more information, see *Self-Learning on Video Analytics Devices* on the next page or *Analytic Events* on page 92.

Enabling or Disabling Video Analytics Display

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

If you are configuring an Avigilon self-learning video analytics device, you can enable or disable the device from displaying the bounding boxes that highlight video analytics activity.

By default, this setting is enabled.

Tip: If you want to change this setting for all cameras rather than for specific devices, change the Video Analytics Activity overlay option in the Client Settings dialog box. For more information, see *Video Display Settings* on page 113.

Enabling Video Analytics Display

Once enabled, bounding boxes are displayed for the camera's video stream in the View tab and for Classified Object Detection, in the camera's AVI video export.

1. In the device Setup tab, click  .

   The Settings dialog box opens.
2. Select the **Display Classified Objects** check box.
3. Click **OK**.

   Displaying video analytics activity is enabled.

Disabling Video Analytics Display

Once disabled, bounding boxes are no longer displayed in the camera's video stream in the View tab or for Classified Object Detection, in the camera's AVI video export.

The camera continues to detect video analytics data, so you will still be able to see bounding boxes while configuring video analytic events, Classified Object Motion Detection and Teach By Example. Bounding boxes will also be displayed when you perform a Motion or Classified Object Events search on the camera's video.

1. In the device Setup tab, click  .

   The Settings dialog box opens.

2. Clear the **Display Classified Objects** check box.
3. Click **OK**.

   Displaying video analytics activity is disabled.

Self-Learning on Video Analytics Devices

Self-learning is the ability of an Avigilon video analytics appliance or camera to perform self-adjustment of the scene. The video analytics device adjusts itself to the activity in its field of view. This can significantly improve the accuracy of classified object detection.

Self-learning can be enabled and disabled. It is highly recommended that you enable self-learning for all video analytic devices, except in the following circumstances:

- If you do not expect any people or vehicles in the device's field of view.
- Scenes where objects can be observed to be moving at different heights. For example, overhead pedestrian bridges, train platforms, hills and underpasses.

For more information, see *Configuring Classified Object Detection* on page 95.

For information on the learning progress for Unusual Motion Detection, see *Unusual Motion Learning Progress* on the next page.

Progress Bar

A progress bar is displayed in the device's Analytics Settings dialog box. The following table describes each phase of the learning progress.

Learning Progress (%)	Description
0 – 33	The device is in the initial learning stage where it begins to gather information on the scene.
34 – 66	The device is adjusting itself using the data it has gathered on the average objects in the scene.
67 – 100	The device has established a high level of classified object detection accuracy.

The learning progress depends on the amount of activity in the scene. Approximately 200 high-confidence detections are required for optimal self-learning calibration.

Resetting the Learning Progress

During installation, a camera is frequently adjusted. Once the camera is stable, we recommend that you reset the camera's learning progress.

When the learning progress is reset, all learning data is cleared. By allowing the video analytics device to re-learn the scene, you are able to prevent missed and false detections based on old data.

NOTE: Always reset the learning progress after a camera is physically moved or adjusted, and if the focus or zoom level is changed. The change in the camera's field of view affects the video analytic results.

1. In the device Setup tab, click  .

   The Settings dialog box opens.

2. Below the self-learning Progress bar, click **Reset**.

   A dialog box will ask you to confirm your decision.

3. Click **Yes**.

   The learning progress is reset.

Typically, the complete learning progress for a video analytic device is enough to learn the scene. However, if the device continues to produce a large number of false object classifications after the learning progress is complete, use the Teach By Example feature to refine the device's object classification capabilities. For more information, see *Teach By Example* on page 88.

Unusual Motion Learning Progress

The Unusual Motion algorithm analyzes motion-based activity and learns the scene to identify rare events.

The initial learning progress can take up to 2 weeks to reach 100%, but events can be reported while the device is learning. As soon as there is enough information about what is typical for a scene, you will see unusual motion events in your live and recorded video. For more information, see *Viewing Unusual Motion Events* on page 147.

As the learning cycle continues towards 100%, the system will increase its accuracy. The system continues to learn activity patterns over time, even after the learning progress reaches 100%.

Resetting the Learning Progress

During installation, a camera is frequently adjusted. Once the camera is stable, we recommend that you reset the camera's learning progress.

When the learning progress is reset, all learning data is cleared. By allowing the video analytics device to re-learn the scene, you are able to prevent missed and false detections based on old data.

NOTE: If a camera with video analytics or unusual motion detection is physically moved or adjusted, or if the focus or zoom level is changed, reset the learning progress to provide accurate results. If the camera's image rate and compression or display settings are updated, the learning progress may reset automatically.

1. In the device Setup tab, click  .

   The Settings dialog box opens.

2. Below the self-learning Progress bar, click **Reset**.

   A dialog box will ask you to confirm your decision.

3. Click **Yes**.

   The learning progress is reset.

Configuring Rialto™ Video Analytics Appliances

To use a Rialto video analytics appliance, configure each connected camera channel for video analytics detection.

If you are configuring an analog video analytics appliance, the cameras are physically connected to each camera channel before the appliance is connected to the system.

If you are configuring an IP video analytics appliance, any camera on the network can be digitally connected to the appliance camera channels. Before you complete this procedure, connect the required cameras first.

NOTE: Rialto video analytics appliances do not support the Avigilon Appearance Search feature. Cameras connected to Rialto appliances do not have the option to be enabled for the feature.

1. Open the Setup tab, then select one of the appliance camera channels.

2. In the device Setup tab, click  .

   The Analytic Events dialog box opens.

3. Assign a camera to the channel.

   Skip this step if you are configuring an analog appliance.

   - From the **Linked Camera:** drop-down list, select a camera for this camera channel.

     Only cameras connected to the same server are listed.

     NOTE: If the camera you link to has a resolution higher than 2.0 MP, the video analytics appliance will use the camera's secondary video stream. This does not affect the resolution of recorded video.

     After you select the camera, the dialog box expands to display the video analytic event settings.

4. From the **Analytics Scene Mode:** drop-down list, select the location that best describes where the camera is installed.

   The Analytics Scene Mode: setting helps the camera identify what it should be looking for.

- **Outdoor**— this option is suitable for most outdoor environments. This setting enhances the camera to identify vehicles and people.
- **Large Indoor Area** — this option only detects people and is enhanced to detect people around obstructions, like chairs and desks, if the head and torso are visible.
- **Indoor Overhead** — this option has enhanced value for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera FoV. Any movement is assumed to be human. It can be used in areas with limited space but with high ceilings, or to monitor doors.
- **Outdoor High Sensitivity** — only use this option if you require the system to be more sensitive than the Outdoor setting. This option is enhanced to run with higher sensitivity for detecting people and vehicles in challenging outdoor scenes. Be aware that this option will generate more false positives.

NOTE: If you change the Analytics Scene Mode: setting after it has been set, the system will delete any data the device may have learned.

5. In the **Camera Type:** drop-down list, select the type of camera that has been connected to this camera channel.

   This helps the video analytics appliance determine what type of image it should expect from the camera.

   - **Color** — select this option if the camera can only stream video in color.
   - **Black and White** — select this option if the camera can only stream video in black and white.
   - **Day and Night** — select this option if the camera can stream video in color or black and white. This type of camera typically displays color video during the day and black and white video at night to capture as much detail as it can of the scene.
   - **Thermal** — select this option if the camera can stream forward looking infrared (FLIR) video.
6. Check the **Enable Noise Filter** box if the camera is too sensitive and falsely detects motion as classified objects. Disable this option if the camera is not sensitive enough.
7. If you plan to enable self-learning or configure video analytic events, apply your changes now.

   Tip: Each time you choose to save or apply your settings, you may be prompted to reboot. To save time, enter all your video analytic settings before you click Apply or OK.

   For more information about self-learning, see *Self-Learning on Video Analytics Devices* on page 98.

   For more information about video analytic events, see *Analytic Events* on page 92.
8. Click **Apply** to save your settings.
9. If you are prompted, allow the device to reboot.

Configuring Avigilon Presence Detector™ Sensors

The Avigilon Presence Detector (APD) sensor is a short-range (9 meters or 30 feet) radar unit that can detect fine motion, such as breathing, in a small indoor area. It can complement cameras to detect activities such as loitering that a camera may not detect as reliably. It is also useful for locations where the use of a camera is impractical or not allowed, but where unusual motion can indicate an unwanted presence that needs to be investigated.

The APD™ sensor detects a person coming into its range and sends a "Presence Detected" notification, and presence is indicated in the event timeline. If the person moves out of range within a preconfigured amount of time called the Dwell Time, a Presence Ended event is sent. However, if the person lingers in range beyond the Dwell Time, a Presence Dwell Time Exceeded event notification is sent until the person lingering actually moves out of range. Then both a Presence Dwell Ended and a Presence Ended event notification are sent. To review these presence events, see *Performing an Event Search* on page 167.

An APD sensor only detects the presence of moving objects within its range. It cannot identify or quantify the objects detected.

1. In the device Setup tab, click  .

   The Settings dialog box opens.

2. Move the **Range:** slider to define the range within which motion can be detected. Enter the line of sight distance from the sensor to the outer edge of the floor area in which you want detection to occur. Accurate range setting is critical in an enclosed area where you do not want to detect motion on the other side of a wall or barrier, or in a large room or lobby space where you only want to detect motion within a specific distance.
3. Set the **Dwell Time:** to measure the amount of time that the APD sensor has to detect motion before a Presence Dwell Time Exceeded event is generated and forwarded to the server. Longer dwell times are suitable for detecting activities such as loitering, so that normal activities in range do not generate events. Shorter dwell times are suitable for detecting activity in an area where no activity is expected. Set the dwell time so that expected movement within range does not generate events.
4. Move the **Sensitivity:** slider to define how sensitive the APD sensor is to fine movement, such as breathing. Lower the sensitivity if you are seeing false detections.

Motion Detection

Depending on the type of camera you are configuring, there may be two types of motion detection available: Pixel Motion Detection and Classified Object Motion Detection.

Pixel Motion Detection observes the video stream as a whole and considers any change in pixel as motion in the scene. This option is available to most cameras that are connected to the system.

Classified Object Motion Detection analyzes the video and only reports the motion of vehicles or persons. This option is only available to Avigilon self-learning video analytics devices.

Setting Up Pixel Motion Detection

In the Motion Detection dialog box, use the Pixel Motion Detection tab to set up pixel motion detection. This allows you to define when the system will acknowledge motion in the scene.

1. In the device Setup tab, click  .

   The Motion Detection dialog box is displayed.

2. In the **Pixel Motion Detection** tab, define the green motion detection area in the camera's field of view:

   NOTE: Pixel motion detection is ignored in the areas that are not highlighted in green.

   Tip: Refer to the red motion activity overlay to help you define the green motion detection area. The motion detection area should avoid areas prone to continuous pixel motion — like TVs, computer monitors, trees and moving shadows. These areas tend to trigger motion recording even though the motion activity may be insignificant.

   -  — Click this button then draw green rectangles to define the pixel motion detection areas. You can draw multiple rectangles to create your pixel motion detection area.
   -  — Click this button and draw rectangles to erase sections from the pixel motion detection area.
   -  — Click this button and manually draw pixel motion detection areas with your mouse. This tool allows you to be very specific and highlight unusual shapes.
   -  — Click this button to highlight the entire image panel for pixel motion detection.
   -  — Click this button to clear the image panel of all pixel motion detection areas.

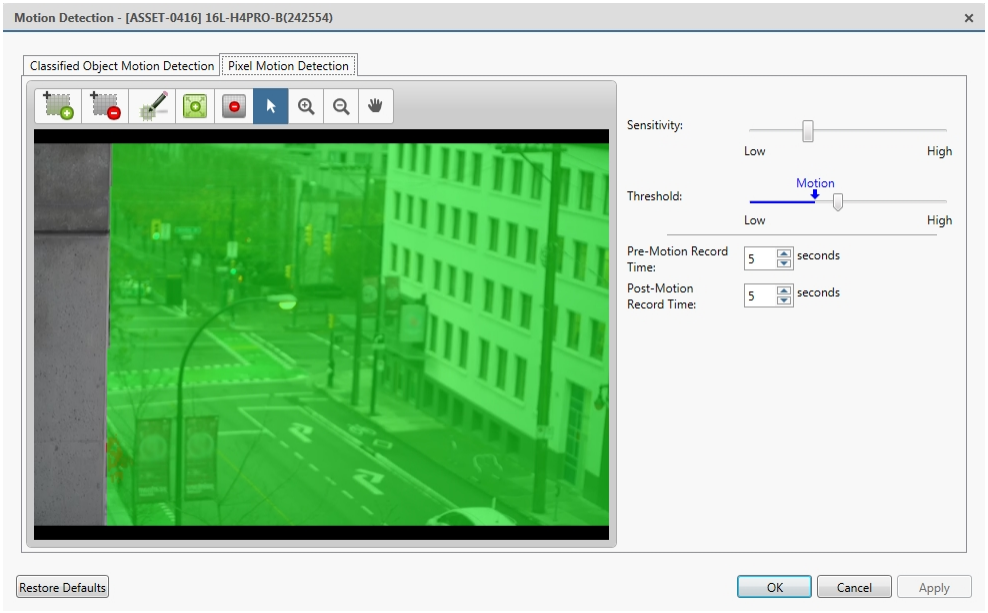


Figure 10: The Motion Detection dialog box: the Pixel Motion Detection tab

3. Define how sensitive the system should be to pixel motion.

    a. Move the **Sensitivity:** slider to adjust how much each pixel must change before it is considered in motion.

    When the sensitivity is High, even small movements are detected - like dust floating immediately before the camera lens.

    b. Move the **Threshold:** slider to adjust how many pixels must change before the image is considered to have pixel motion.

    When the threshold is High, only large motions are detected - like a truck driving across the scene.

    Tip: The **Motion** indicator above the Threshold: slider will move to indicate how much motion is occurring in the current scene. Only when the Motion indicator moves to the right of the Threshold: marker will the camera detect the pixel motion.

    c. In the **Pre-Motion Record Time:** and **Post-Motion Record Time:** fields, specify how long video is recorded before and after the pixel motion event.

4. Click **OK** to save your settings.

Setting Up Classified Object Motion Detection

In the Motion Detection dialog box, use the Classified Object Motion Detection tab to set up object motion detection. This allows you to define when the system will acknowledge a person or vehicle in the scene.

1. In the device Setup tab, click  .

   The Motion Detection dialog box is displayed.

2. In the **Classified Object Motion Detection** tab, define the green motion detection area in the camera's field of view:

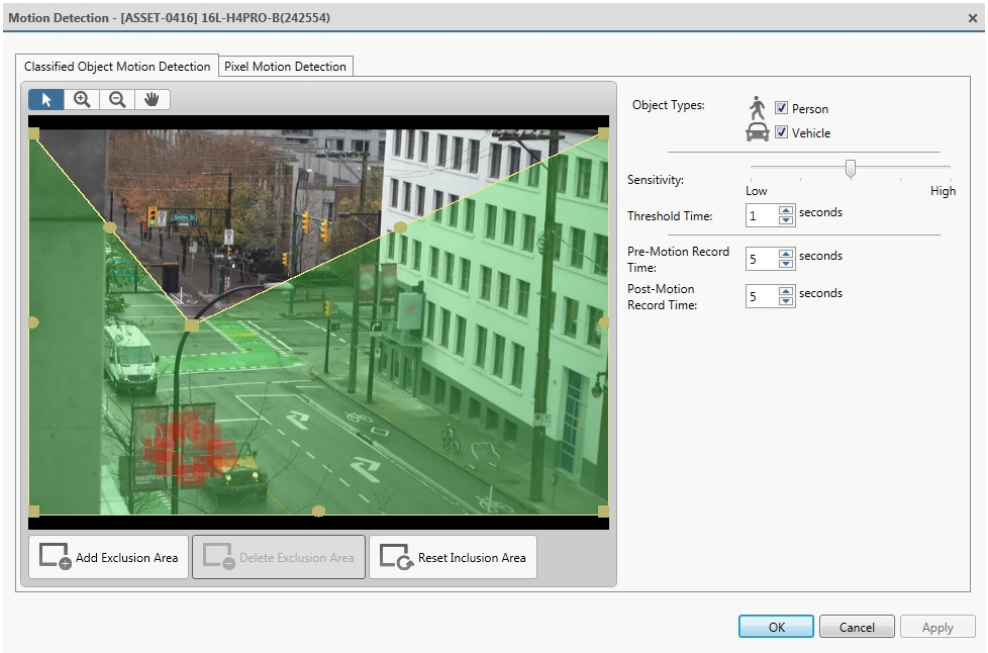


Figure 11: The Motion Detection dialog box: the Classified Object Motion Detection tab

- To change the shape or size of the green overlay, click and drag any of the yellow markers on the border. Extra markers are automatically added to help you fine tune the shape of the overlay.
- To move the green overlay, place the cursor over the green overlay until the cursor changes into a hand or the pan tool. Then, click and drag the green overlay to the desired location.
- Click  to add an exclusion area. The exclusion area is added inside the green overlay.

  Classified object motion is *not* detected in exclusion areas.

  - To set an exclusion area, move and resize the exclusion area as required then click anywhere on the green overlay.
  - To edit an exclusion area, double-click the exclusion area then modify as required.

- Select an exclusion area then click  to delete the exclusion area.
- Click  to restore the default green overlay.

3. Define the objects that are detected by the system.
    a. Check the **Person** box to detect people in the area.
    b. Check the **Vehicle** boxes to detect vehicles in the area.
    c. Move the **Sensitivity:** slider to adjust how sensitive the system is to the detection of classified objects.

        If you set the slider to **Low**, the video analytics device will detect fewer objects because the system must be highly confident that it has detected a person or vehicle before you are notified of an event.

        If you set the slider to **High**, the video analytics device will detect more objects because the system does not need to be as certain of the object classification before you are notified of a motion event.

        Be aware that if the slider is set too low, the system may miss classified object motion. If the slider is set too high, the system may generate a higher number of false classified object motion detections. Adjust the **Sensitivity:** slider to match the level of activity in the scene.

    d. In the **Threshold Time:** field, adjust how long an object must be moving before it is considered a moving object.
    e. In the **Pre-Motion Record Time:** and **Post-Motion Record Time:** fields, specify how long video is recorded before and after a classified object motion detection event.
4. Click **Apply** to save your settings.

Configuring the Video Intercom

Before a newly installed Avigilon Video Intercom device at your site can initiate a video intercom call session, you need to enable the microphone and speaker on the device in the ACC Client software. See *Microphone* on page 110 and *Speaker* on page 111.

Authorizing ACC Operators to Answer the Video Intercom

To authorize ACC operators to receive calls from a Video Intercom, you must configure a rule that connects the digital input event that occurs when the call button is pressed to an action that starts a call session between the Video Intercom device and an ACC operator. Rules are configured at the site setup level.

The following example is a basic rule which specifies that when the call button is pressed on any Avigilon Video Intercom device, a video intercom call is initiated to a number of ACC users, one of whom answers the call.

To specify the trigger event:

1. In the Select Rule Event(s) list, under Device Events, select the **Digital Input Activated** check box.
2. In the panel below the events list, click **any digital input**. The Select Digital Inputs dialog box is displayed.
3. Click **Any of the following digital inputs:** and for each Avigilon Video Intercom device at your site select

Call button.

4. Click **OK** to return to the Select Rule Event(s) list, then click .

To specify the action to take:

1. In the Select Rule Action(s) list, under Monitoring Actions, select the **Video intercom call** check box.
2. In the panel below the actions list, click **all users**. The Select Users dialog box is displayed.
3. Click **All of the following users and/or groups:** and then click to select any combination of groups and users that you want to answer video intercom calls.
4. Click **OK** to return to the Select Rule Action(s) list, then click and complete defining the rule.

Alternatively, you can set up one rule per Avigilon Video Intercom device. To do this:

1. Specify the **Call button** of only one device when you specify the trigger event.
2. Before you select the users to answer the call:
    a. In the panel below the actions list, click **the camera linked to the event**. The Select Camera dialog box is displayed.
    b. Click **All of the following cameras:**, then select the same Avigilon Video Intercom device that you specified for the trigger event.
    c. Click **OK** to return to the Select Rule Action(s) list, then specify the user and continue to complete defining the rule.

For instructions on how to add and edit rules, see *Rules* on page 53.

For instructions on how an operator answers a call from an Avigilon Video Intercom device, see *Answering a Video Intercom Call* on page 134.

Recording Video When the Call Button is Active

To conserve video storage, you can schedule the ACC software to record only when a visitor presses the call button on a Video Intercom. You need a recording schedule template to record video only when the digital output from a Video Intercom is activated, which happens when the call button is pressed and lasts until the visitor is granted access, or three minutes elapses with no response. You can also specify when during the day you want video recorded. Then you can specify the Video Intercoms that use this schedule, and specify the days of the week the schedule is active.

To define a recording schedule template for a Video Intercom call:

1. In the server Setup tab, click . The Recording Schedule dialog box is displayed.
2. Click **Add Template** below the Templates: list.
3. Enter a name for the **New Template**.
4. Click the **Clear Area** button to clear the default settings.
5. Click the **Set Area** button.

6. In the **Recording Mode:** area, click or drag the cursor across in the **Digital Inputs** timeline to specify the hours that you want to record video when the call button is pressed. The rectangles on the Recording Mode: timeline are colored when they have been selected.
7. Optionally, select any other events that you might want to trigger recording, and whether you want reference images recorded at a regular frequency between events in the recording schedule.

   For more information, see *Adding and Editing a Recording Schedule Template* on page 63.

To assign a Video Intercom to a schedule and set the days the schedule is active:

1. Ensure the template is selected in the Templates: list.
2. In the Default Week area, select the Video Intercom:
   - Click the name of the Video Intercom to use this template to record every day of the week.
   - Click to select the days of the week to use this template only on specific days.

   For more information, see *Setting Up a Weekly Recording Schedule* on page 64.
3. Click **OK**.

Digital Inputs and Outputs

Use the Digital Inputs and Outputs dialog box to set up external devices with digital inputs and outputs that are connected to a device or Avigilon video analytics appliance.

The external devices can be used to create alarms or trigger recording events and specific actions through the Rules engine. For more information, see *Rules* on page 53.

Setting Up Digital Inputs

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the device Setup tab, click  .

   The Digital Inputs and Outputs dialog box is displayed.
2. In the **Digital Inputs:** area, select an input.
3. Enter a **Name:** for the digital input.
4. In the **Recording Duration:** area, select one of the following:
   - Select **Follow event** to record the entire digital input event.
   - Select **Maximum time:** to limit the recording time.
5. Enter the **Pre-Event Record Time:** and **Post-Event Record Time:**.
6. Select the digital input's default **Circuit State:**.

7. Select cameras to link to this digital input.

   If the Recording Schedule is configured to record digital inputs, the cameras selected in the **Link to Camera(s):** area are used to record the events triggered by this digital input.

8. Click **OK**.

Setting Up Digital Outputs

Once a digital output is configured, you can manually trigger the digital output in an image panel. For more information, see *Triggering Digital Outputs* on page 133.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.



1. In the device Setup tab, click .

   The Digital Inputs and Outputs box is displayed.

2. In the **Digital Outputs:** area, select an output.
3. Enter a **Name:** for the digital output.
4. Select the digital output's default **Circuit State:**.
5. The **Output Mode:** options define what occurs when the digital output is activated.
   - Select **Hold** to enable the digital output in continuous mode.
   - Select **Pulse** to enable the digital output in pulse mode. If there is a **Repeat Count:** field, specify the number of repeat counts for the pulse. If there is a **Total Duration:** field, specify how long the digital output should be for the pulse.
6. If there is a **Pulse Duration:** field, specify the pulse duration in minutes and seconds.
7. In the Link to Camera(s): area, select the cameras that are permitted to trigger this digital output.

   By default, the system automatically selects the camera that this digital output is connected to.

8. Click **OK**.

Configuring Standby Mode

If a person does not agree to be under surveillance due to privacy concerns, ACC users can put a device on Standby by triggering a rule. When a device is on Standby, it does not stream or record video.

You can set up rules to enable and disable Standby mode. For example, you could set up a digital input rule to trigger Standby mode for a device until a digital output rule is triggered. You could also set up a rule that triggers Standby mode when two conditions are met using rule conditions. For example, you could set up a rule to trigger Standby more when motion is detected and a digital input is activated.

Add a rule to enable Standby mode:

1. In the site Setup tab, click  .

   The Rules dialog box is displayed.

2. Click and select the events that will trigger the rule. Click .
3. On the Select Rule Action(s) page, select **Pause device**. Click .
4. On the Select Rule Condition(s) page, select one or more conditions that will cause the rule to run. To always run the rule, clear all conditions. Click .
5. On the Select Rule Properties page, enter a descriptive **Rule Name:** and **Rule Description:**.
6. Click to save the new rule.

Add a rule to disable Standby mode:

1. In the site Setup tab, click  .

   The Rules dialog box is displayed.

2. Click and select the events that will trigger the rule. Click .
3. On the Select Rule Action(s) page, select **Resume device**. Click .
4. On the Select Rule Condition(s) page, select one or more conditions that will cause the rule to run. To always run the rule, clear all conditions. Click .
5. On the Select Rule Properties page, enter a descriptive **Rule Name:** and **Rule Description:**.
6. Click to save the new rule.

Microphone

Use the Microphone dialog box to change the settings for any audio input device that is connected to a camera or Avigilon video analytics appliance. You can also link the audio to other cameras.

To use this feature, a microphone must be connected to the device.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the device Setup tab, click  .

   The Microphone dialog box is displayed.

2. If the device supports multiple audio inputs, select the one you want to edit from the **Microphone Inputs:** list.
3. Click the **Microphone Off** toggle to enable audio recording from microphones connected to the device.

   Click the toggle again to disable the feature.

4. Enter a meaningful name for the microphone.

   The default microphone name is assigned by the camera.

5. In the **Gain:** drop-down list, select the amount of analog gain that is applied to the audio input. The higher the dB setting, the louder the volume.
6. At the bottom of the dialog box, click **Listen** to test the sound from the microphone.

   Tip: You must have speakers connected to the computer to hear the audio.

7. In the **Link to Camera(s):** area, select cameras to link to this audio.
8. Click **OK**.

Speaker

Use the Speaker dialog box to change the settings for any audio output that is connected to a device (a camera or video analytics appliance). You can also link the audio to other devices.

To use this feature, speakers must be connected to the device and a microphone must be connected to your local Client.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the device Setup tab, click  .

   The Speaker dialog box is displayed.

2. If multiple **Speaker Outputs:** are listed, select the one you want to edit.
3. Click the **Speaker Off** toggle to enable enable audio broadcasting. Speakers connected to the device will broadcast audio from the microphone that is connected to the local Client.

   Click the toggle again to disable the feature.

4. Select the **Record:** check box to record what is broadcast.
5. Enter a name for the speaker.
6. The **Volume:** slider controls the volume of the speakers.

7. In the **Link to Camera(s):** area, select cameras to link to the speakers.
8. To test the **Microphone Level:**, speak into the microphone. The red bar will move to show the audio input level.
9. Click **OK**.

If you want to enable two-way audio for your local application, see *General Settings* below.

Application Preferences

The Client Settings are used to set your preferences for your local copy of the ACC Client software. This includes saving your password, setting the language, saving your last window layout, configuring your joystick, and manually adding and removing sites.

General Settings

Use the General settings to set your local Client preferences. Any changes you make will only affect this copy of the Client software.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

1. In the top-right corner of the Client, select > **Client Settings**.
2. In the General tab, make any required changes:
   - **Save/restore window layout:** Select this check box if you want the Client to remember your layout preferences.
   - **Automatically launch full screen:** Select this check box if you want the Client to automatically launch in full screen mode each time it starts.
   - **Display Notifications:** Select this check box if you want the Client to display system messages. System messages are listed in the red box at the top-right corner of the Client - click the red box to see the messages. System messages notify you of site events, system events and possible device connection issues.

     If this check box is cleared, all system messages are hidden.
   - **Synchronize recorded video playback:** Select this check box to allow the system to automatically synchronize the Timelines in all new View tabs.

     For more information, see *Synchronizing Recorded Video Playback* on page 148.
   - **Beta Feature - Focus Of Attention** - Focus of Attention is a beta feature for Enterprise users. For information on how to enable it and provide feedback, contact **producteval@avigilon.com**.
   - **Cycle dwell time:** Enter the number of seconds the Client waits before it cycles to a different View tab. For more information, see *Cycling Through Views* on page 121.
   - **Language:** Select a language from the drop-down list to change the Client language. Select **Windows Default** for the Client to use the same language as the operating system.

- **Automatically log in to sites:** Select this check box to automatically log in to all sites you can access. Select the type of login you use:
  - Select **Using Windows Authentication** if you use your Windows login to access sites.
  - Select **Using saved user name and password:** if you use your Avigilon Control Center username and password.
- In the **Maximum Incoming Client Bandwidth:** area, you can set how much bandwidth is received by the client. This includes video streaming.

  You can select **Unlimited** or **Other:**, and specify the maximum bandwidth allowance in kilobits per second (kbit/s).
- In the **Client Duplex Audio Setting:** area, decide if you want to enable two-way audio. This allows people in the video to talk with the operator monitoring the video.

  You have the option of **Full-duplex** audio, which allows simultaneous communication, or **Half-duplex**, which only allows communication from one side at a time. To use this feature, you need to set up microphones and speakers to cameras. For more information, see *Microphone* on page 110 and *Speaker* on page 111.

3. Click **OK** to save your changes.

Video Display Settings

You can adjust the Client Display settings to improve how video is displayed on your monitor.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

1. In the top-right corner of the application window, select > **Client Settings** > **Display**.
2. Complete any of the following procedures to adjust how video is displayed in image panels.

Displaying Analog Video in Deinterlaced Mode

Select the **Display Deinterlaced Images** check box if the analog video you are watching is showing interlacing artifacts. This setting will help improve video image and smooth out some of the artifacts.

Displaying Logical IDs

Select the **Display Logical IDs** check box if you need to see the Logical ID of all devices. Logical IDs must be unique numbers. This setting will display the device's Logical ID in brackets beside the device's name in the System Explorer.

When this setting is enabled, the device's name in the System Explorer is displayed in the following format:

<Device Name>(Serial Number) (Logical ID).

For example, *2.0-H3A-DP1(574065) (101).*

The Device Name and Serial Number can be changed in the device's General settings dialog box by editing the **Device Name:** field. Edit the **Logical ID:** field in the same dialog box to change the device's Logical ID.

Displaying Device Preview

Select the **Display Device Preview** check box to enable the system to show a preview of the device video.

When this setting is enabled, you will see a preview of the device video when you hover over the device in the System Explorer and on a map.

Changing Display Quality

If your computer does not have enough network bandwidth or processing power, you may not be able to watch video at its full image rate and quality. You can configure the image panels to display video in high quality and low frame rate, or low quality and high frame rate.

Select a higher display quality setting if you need to see specific details or faces in the scene. Select a lower display quality setting if it's more important to see moving events as they occur.

The Display Quality: settings only affect the image panel display and do not affect the actual video quality or image rate between the camera and the server. Therefore, you can review recorded footage later to confirm what you saw in the image panel.

In the Display Quality: area, select one of the following options:

- **Maximum:** displays video at full resolution with the lowest image rate.
- **High (Default):** displays video at 1/4 resolution.
- **Medium:** displays video at 1/16 resolution.
- **Low:** displays video at 1/64 resolution with the highest image rate.

Changing Display Adjustment Settings

The Display Adjustment Settings: allow you to configure the default values that will be applied to all video displayed in the View tab.

NOTE: This setting does not affect recorded video. Options that are not supported by the device will be disabled or hidden.

1. In the **Display Adjustment Settings:** area, move the sliders to adjust the **Gamma:**, **Black Level:**, and **White Level:** settings.

   By default, the **Gamma:** setting is set to 0.55, the **Black Level:** setting is set to 0.5%, the **White Level:** setting is set to 98%, and Auto-Contrast is disabled.

2. Select the **Enable Auto-Contrast** check box to allow the system to automatically adjust the contrast level for the video stream.

   NOTE: When Auto-Contrast is disabled, the **Black Level:** and **White Level:** settings cannot be adjusted.

3. Click **Restore to Factory Default** to revert to the factory default Display Adjustment Settings: settings.
4. Click **OK** to save your changes.

If video is being displayed in a View tab, the new settings will not take effect until the **Restore Defaults** option is selected in the image panel.

Overlay Settings

You can adjust the Client Overlays settings to improve how video is displayed on your monitor.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

1. In the top-right corner of the application window, select > **Client Settings** > **Overlays**.
2. Complete any of the following procedures to adjust how video is displayed in image panels.

Displaying Image Overlays

Select any of the Image Overlays: options to set the type of information that is displayed over video.

Overlay	Description
Device Name	Displays the name assigned to the camera.
Device Location	Displays the location assigned to the camera.
Playback Timestamp	(Recorded video only) Displays the exposure timestamp for the video. From the Timestamp Zone: area, select the time that should be displayed: • **Show device time** — If you have cameras installed at different locations in your system, select this option to display the time recorded at the camera location. • **Show local time** — Select this option to display the recorded video time in your local timezone.
Live Timestamp	(Live video only) Displays the current date and time to the millisecond. From the Timestamp Zone: area, select the time that should be displayed: • **Show device time** — If you have cameras installed at different locations in your system, select this option to display the time at the camera location. • **Show local time** — Select this option to display the time in your local timezone.
Record Indicator	(Live video only) Displays the recording status of a camera. The recording status is indicated by the round icon on the top-left corner of the image panel. The color of the icon shows the camera's recording status. •  : recording triggered by a motion event •  : recording •  : not recording. Click this icon at any time to begin manual recording.
Motion Activity	Highlights motion in red.
Video Analytics Activity	For Classified Object Motion Detection, bounding boxes outline objects detected in the video. The color of the bounding box identifies the object type: • Red — a person • Blue — a vehicle For Unusual Motion Detection, teal bounding boxes trail a moving object. The Video Analytics Activity overlay is only activated for video from a video analytics device.

Overlay	Description
	NOTE: The bounding boxes may not be displayed if the feature is disabled on the specific device. For more information, see *Enabling or Disabling Video Analytics Display* on page 97.
License Plate	(Live video only) Displays license plate numbers as they are detected. **NOTE:** This feature is only available if the *License Plate Recognition* feature is installed.

Joystick Settings

There are two types of joysticks supported by the Client: standard Microsoft DirectX USB joysticks and the Avigilon USB Professional Joystick Keyboard.

Access the Joystick settings to install the required drivers and configure your joystick options.

Configuring an Avigilon USB Professional Joystick Keyboard For Left-Hand Use

The Avigilon USB Professional Joystick Keyboard is a USB add-on that contains a joystick for controlling zooming and panning within image panels, a jog shuttle for controlling the Timeline, and a keypad programmed with the Client software keyboard commands. For more information about the keypad commands that control the Client software, see *Keyboard Commands* on page 201.

By default, the keyboard is installed in right-hand mode. Change the Joystick settings to configure it for left-hand mode.

1. Connect the keyboard.
2. In the top-right corner of the Client, select > **Client Settings** > **Joystick**.

   If the keyboard is not automatically detected, an error message is displayed. Click **Scan for Joysticks...**.
3. In the Joystick tab, select the **Enable left-hand mode** check box.
4. Click **OK**. The keyboard is now configured for left-hand mode.
5. Rotate the keyboard until the joystick is on the left and the jog shuttle is on the right. Reinstall the keypad cover with the View button labels at the top.

For more information about the Avigilon USB Professional Joystick Keyboard, see the installation guide that is included with the device.

Configuring a Standard USB Joystick

Use the Joystick settings to configure the buttons used in your standard Microsoft DirectX USB joystick.

1. Connect the joystick. In the top-right corner of the Client, select > **Client Settings** > **Joystick**.
2. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.
3. In the Joystick tab, choose an action for each button on the joystick:
    a. Press a button on the joystick to highlight its label in the dialog box.
    b. Select an action for the button from the drop-down list.

    Options include ways to control recorded video, Views, image panels, instant replay, audio, snapshots and PTZ.

    c. Repeat this procedure for each button on the joystick.
4. Click **OK**.

Discovering Sites

If your computer is on the same network segment (subnet) as a site, that site is automatically discovered and displayed in the System Explorer.

If the site you want to access is not listed, it is because the site is on a different subnet and must be manually discovered. There is no limit to the number of sites that can be discovered by the Client software.

Tip: After you discover and login to a parent site, all the child sites are automatically discovered.

By default, when a server is first connected to the system, it is added to a site with the same name. To locate a new server, you need to search for its site.

1. Open the Find Site dialog box.
    - In the top-left corner of the application window, select > . In the Site Login tab, click **Find Site...**.
    - Or, select > **Client Settings** > **Site Networking**. In the Site Networking tab, click **Find Site...**.
2. In the dialog box, enter the **IP Address/Hostname:** and the **Base Port:** of the server in the site you want to discover.

    The base port is 38880 by default. You can change the base port number in the Avigilon Control Center Admin Tool. For more information, see *The Avigilon Control Center Server User Guide*.
3. Click **OK**.

If the site is found, it is automatically added to the site list.

If the site is not found, check the following then try again:

- The network settings are configured correctly.
- The firewall is not blocking the application.
- The Avigilon Control Center Server software is running on the server you searched for.

Managing Site Logs

The Site Logs record events that occur in the ACC software. This can be useful for tracking system usage and diagnosing issues.

You can filter the items displayed in the log and save the log to a separate file for sending to Avigilon support.

If an Access Control Manager (ACM) appliance is connected to your site, you can track access control objects like doors and inputs.

NOTE: The Site Logs maintain a record of system events for as long as video data is available or 90 days, whichever is longer.

1. In the New Task menu, click .

   The Site Logs tab is displayed.
2. In the top-left Event Types to Show: area, select the types of logs that you want to see.
3. In the Event Sources: area, you can filter the logs by selecting the specific site, server or device logs that you want to see.

   If an ACM appliance is connected to your site, you can also filter by access control objects.

   NOTE: The available access control objects depend on your permissions in the ACM appliance. Contact your ACM administrator to update your permissions.
4. In the Time Range to Search: area, set the date and time range of the search.
5. Click **Search**.
6. Select a search result to display the event details at the bottom of the tab.
7. To save the log search results, click **Save events to file...**. You can choose to save the search results as a text file or a comma-separated values (CSV) file.

Live Monitoring

Users responsible for monitoring live video in a surveillance site can display live video and configure each View tab to meet surveillance requirements.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Organizing Views

A View tab is where you watch camera video. Inside the View tab is a set of image panels that allows you to organize how video is displayed.

You can arrange image panels into different layouts to take advantage of different camera angles and save View layouts that you like.

You can share Views with other users during investigations, and organize how video is displayed across multiple monitors.

Adding and Removing a View

View tabs allow you to customize how you monitor video. You can open a new View in the current window or open a View in a new window to make use of multiple monitors. Views can also be removed as required.

If you want to make use of a large number of monitors, like a video wall, see *Virtual Matrix* on page 123.

To...	Do this...
Open a new View tab	Click . Or, press `Ctrl + T`.
Close a View tab	On the View tab, click . Or, press `Ctrl + W`.
Open a new window	Select  > **New Window**. Or, press `Ctrl + N`. A new window appears. You can now position this window to make use of multiple monitors.
Close a window	In the top-right corner of the window, click . **NOTE:** If you see a confirmation dialog box, it is because there is only one window open and closing this window will also close the application.

View Layouts

You can organize how video is displayed through View layouts. You can choose to display video in 1 - 64 image panels. You can also customize the shape of image panels to accommodate cameras that are installed vertically to capture long hallways.

There are 10 pre-configured layouts that you can edit to fit your needs.

Selecting a Layout for a View

You can organize how video is displayed by selecting a View layout.

- On the toolbar, click  then select one of the layout options.

Editing a View Layout

If the default View layouts do not fit your surveillance requirements, you can customize a View layout.

1. On the toolbar, select  > **Edit Layouts...**.
2. In the Edit Layouts dialog box, select the layout you want to change.
3. Enter the number of **Columns:** and **Rows:** you want in your layout.
4. In the layout diagram, do any of the following to further customize the layout.

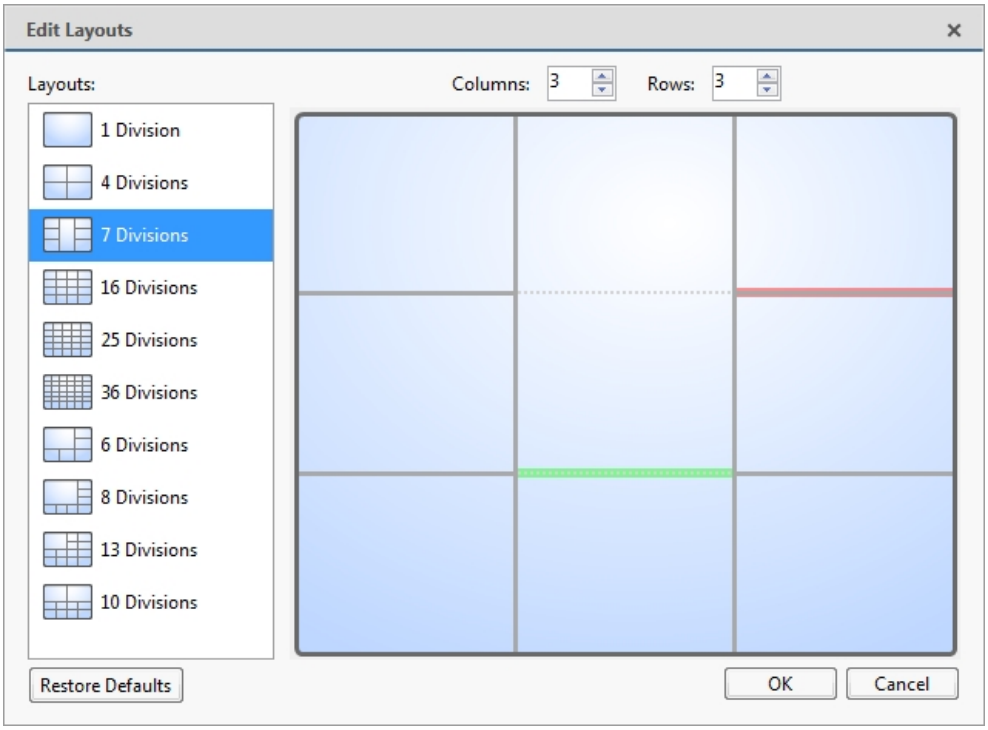


Figure 12: The Edit Layouts dialog box

- To create a larger image panel, select a gray line to delete the border between two image panels. When a line is highlighted in red, the line can be deleted.
- To restore an image panel, select a dotted line to divide a larger image panel into two. When a

dotted line is highlighted in green, the line can be restored.

- To restore all default View layouts, click **Restore Defaults**. All custom layouts in the Layouts: list will be replaced.

NOTE: You can only add or subtract lines to create a rectangular shape.

5. Click **OK** to save your changes. The previous View layout has been replaced with your customized layout.

Tip: The keyboard commands used to access View layouts are linked to the layout's position in the Layouts: list. For example, if your custom layout is placed at the top of the Layouts: list (layout 1), you can press `Alt + 1` to use that layout.

Making a View Full Screen

You can maximize a View to fill an entire monitor screen.

- On the toolbar, click .

Ending Full Screen Mode

- While the View is in full screen mode, click .

Cycling Through Views

If you have multiple View tabs open, you can cycle through them by displaying each one for a few seconds. This is useful when monitoring a large number of cameras.

To specify the amount of time each View is displayed, change the **Cycle dwell time:** setting in the  **> Client Settings > General** tab. For more information, see *General Settings* on page 112.

- To activate the Cycle Views feature, click .

Saved Views

After you add videos to a View, adjust the layout to fit your preferences and zoom-in each video to the area of interest, you can save the View to share with other users in the site. A saved View remembers the current View layout, the cameras displayed in each image panel, and the image panel display settings.

Saving a New View

1. From the toolbar, select  **> Save As New View**.
2. In the following dialog box, complete the following:
    a. Select the site that the View should be added to.
    b. Give the saved View a name.
    c. Assign a number to the saved View in the **Logical ID:** field. The logical ID is a unique number that is used to open the saved View through keyboard commands.

d. If it is not displayed, click  to display the Site View Editor and choose where the saved View appears in the System Explorer.

- In the  site directory, drag the saved View up and down the right pane to set where it is displayed.
- If your site includes  folders, select a location for the saved View in the left pane. The right pane updates to show what is stored in that directory.

e. Click **OK**.

Your saved View is added to the System Explorer under the selected site. You can now manage the saved View as a part of your site.

Opening a Saved View

Do one of the following:

- In the System Explorer, double-click the saved View ().
- In the System Explorer, right-click  and select **Open**.
- Drag  from the System Explorer to the current View in the application or new window.
- On your keyboard, press `CTRL + G`. When you are prompted, enter the saved View's logical ID then press `Enter`.

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. From the tool bar, select  > **Update Saved View**.

Renaming a Saved View

1. In the System Explorer, right-click  and select **Edit...**.
2. In the Edit View dialog box, enter a new name or logical ID and click **OK**.

Deleting a Saved View

1. In the System Explorer, right-click  and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Collaborating

If you want to show another user an incident or need help investigating an event, you can share your current View with another user. You will both be able to control the View and show each other your findings.

Sharing a View

1. In the toolbar, click .
2. In the following dialog box, select the user you want to collaborate with, then click **OK**.

   The users are listed by username and computer name. The computer name is used to help you identify a specific user if the username is shared by several people. Only users who are currently logged in to the site are displayed.

   a. The user you select will see a pop-up message with your invitation to collaborate and may choose to accept or decline.
   b. You will receive a pop-up message with the user's response to your invitation.

      If they say *Yes*, the View you are looking at is automatically opened as a new tab in your collaborator's window.
3. Repeat this procedure to collaborate with multiple users.

While you are collaborating, any changes made to the current View by a collaborator are shared with the other collaborators. Anything that you can do in a standard View can be done in a shared View.

Leaving a Shared View

- To leave a shared View, just close the View tab. The remaining users stay in collaboration mode.

Virtual Matrix

The optional Virtual Matrix feature allows you to control the View displayed on multiple monitors, or a video wall, from any instance of the application. To use this feature, the Virtual Matrix software must be installed on the system that all the displays are connected to, and users must have the **Manage virtual matrix monitors** group permission.

A copy of the Virtual Matrix software can be downloaded from the Avigilon website.

For more information about the Virtual Matrix software, see *The Avigilon Control Center Virtual Matrix User Guide*.

Once the Virtual Matrix has been installed and loaded, the monitors connected to the system are automatically added to a site. All monitors linked by the Virtual Matrix software are displayed in the System Explorer as  followed by the monitor name.

Controlling Virtual Matrix Monitors

In the System Explorer, each  represents a View that is displayed on a connected Virtual Matrix monitor.

To control what is displayed on each Virtual Matrix monitor, you need to open the monitor:

- In the System Explorer, right-click  and select **Open**.
- Double-click or drag  from the System Explorer to the current View.

The Virtual Matrix monitor is opened in a new tab and can be controlled like any View — you can change the View layout, control video display, and use any active PTZ controls. The changes you make should automatically appear on the Virtual Matrix monitor.

When you are done, you can close the Virtual Matrix monitor tab. The monitor will continue to display the View you have configured until you make new changes or the Virtual Matrix is shut down.

Editing Virtual Matrix Monitors

In the Avigilon Control Center Client software, you can edit the name and logical ID of Virtual Matrix monitors. Adding or removing active Virtual Matrix monitors must be done through the Avigilon Control Center Virtual Matrix software.

1. In the System Explorer, right-click and select **Edit...**.
2. In the following dialog box, enter a new name and logical ID for the Virtual Matrix monitor.
3. If it is not displayed, click to display the Site View Editor and choose where the monitor appears in the System Explorer. By default, the monitor is added to the site that you initially selected.
   - In the site directory, drag the monitor up and down the right pane to set where it is displayed.
   - If your site includes folders, select a location for the monitor in the left pane. The right pane updates to show what is stored in that directory.
4. Click **OK**.

   Your changes are saved and sent to the Virtual Matrix software.
5. To delete a disconnected Virtual Matrix monitor:

   NOTE: You can only delete a monitor that has been disconnected or removed from the Virtual Matrix software.

   a. Right-click and select **Delete**.
   b. When the confirmation dialog box is displayed, click **Yes**.

For more information, see the *Avigilon Control Center Virtual Matrix User Guide*.

Controlling Live Video

Tip: If video appears slow, it may be a network issue between the ACC Client software and the server that the camera is connected to. Actual recorded video quality is not affected.

Adding and Removing Cameras in a View

To monitor video, add a camera to a View tab. Camera video can be removed from a View tab at any time.

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.

- If your cameras are assigned a Logical ID:, press / and enter a logical id. For more information, see *Cycling Through Cameras* below.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click .

Viewing Live and Recorded Video

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Tip: If you cannot see either  **Live** or  **Recorded** on the toolbar, you may need Dual Authorization. For more information, see *Requesting Dual Authorization* on page 145.

When you monitor video, you can choose to watch live and recorded video in the same View tab, or only one type of video per View tab.

Once you've added cameras to the View tab, you can do the following:

- To switch all of the image panels in the View between live and recorded video, click either  **Live** or  **Recorded** on the toolbar.
- To switch individual image panels between live and recorded video, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying recorded video have a **green** border.

Cycling Through Cameras

If you have many cameras in a site, you can cycle through them to determine which one you want to open in a new image panel.

The cameras must have a Logical ID assigned. For more information, see *Setting a Device's Identity* on page 74.

Tip: To view the camera's Logical ID in the System Explorer, go to the  > Client Settings > Display tab and select the **Display Logical IDs** check box. For more information, see *Displaying Logical IDs* on page 113.

To cycle through cameras from more than one site at a time, in the  > Client Settings > General tab, select the **Display next camera by logical ID across all sites** check box.

If a camera with a Logical ID is selected in the System Explorer or in an image panel, the cameras will begin cycling from that Logical ID.

1. Hold / and:

Press	To preview video from...
+	the camera with the next Logical ID
–	the camera with the previous Logical ID

2. Release / to select a camera.

   The camera opens in a new image panel.

Standby Mode

If a device is in Standby mode, the image panel will stop streaming video and display: **Standby**.

Video streaming and recording are paused until the device is no longer in Standby mode.

For more information, see *Configuring Standby Mode* on page 109.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.
- On the toolbar, select  or , then click the image panel until you reach the desired zoom depth.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel.
- On the toolbar, select , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click .
- Double-click the image panel.

Making Image Panel Display Adjustments

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings. These settings can also be adjusted in Client Settings. For more information, see *Changing Display Adjustment Settings* on page 114.

1. Right-click an image panel and select **Display Adjustments...**.

   The Display Adjustments... settings are displayed in a floating pane immediately beside the image panel.

2. Move the sliders to adjust the **Gamma:**, **Black Level:** and **White Level:**.

   By default, **Gamma:** is set to 0.55, **Black Level:** is set to 0.5%, **White Level:** is set to 98%, and Auto-Contrast is disabled.

   The image panel displays your changes.

3. Select the **Enable Auto-Contrast** check box to allow the system to automatically adjust the contrast level for the video stream.

   NOTE: When Auto-Contrast is disabled, the **Black Level:** and **White Level:** cannot be adjusted.

4. To clear your changes, click **Restore Defaults**.

   If display adjustments have been made in the Client Settings, they will be applied to the image panel.

5. To set the selected levels as the default settings for all image panels going forward, click **Save as Defaults**.

Using Digital Defog

If a camera supports digital defog, the  icon is displayed in the image panel. Digital defog uses an image processing algorithm to increase image quality when dealing with rainy, misty, or foggy conditions in outdoor surveillance applications. Digital defog is disabled by default.

The digital defog levels set in the image panel are applied to all user views and will be seen in recorded video.

To control digital defog, do any of the following:

- In the lower-right corner of the image panel, click  to enable digital defog.
- To change the digital defog level, move the slider.

  If the connected device supports discrete levels, the slider will snap to the nearest level.

- If the connected device supports automatic adjustments, click the digital defog button until  is displayed to enable automatic digital defog.
- To disable digital defog, click the digital defog button until  is displayed.

Changing Day/Night Mode

If the camera supports day/night control from the image panel, one of the following icons is displayed in the lower-right corner of the image panel. The icon that is displayed reflects the current setting.

Day/night mode uses a camera's built-in IR cut filter to help capture high quality images based on the amount of light in the scene. Most cameras provide you with the ability to set day/night mode from the Image and Display dialog box, but only some give you the ability to change this setting from the image panel.

The image panel setting is applied to all user views and will be seen in recorded video.

In the lower-right corner of the image panel, click the **Set Day/Night Mode** button and select one of the following:

- **Automatic** — allow the camera to control the infrared cut filter based on the amount of light in the scene.
- **Day Mode** — the camera will only stream in color and the IR cut filter is disabled.
- **Night Mode** — the camera will only stream in black and white, and the IR cut filter is enabled to capture near infrared light.

Listening to Audio in a View

If there is an audio input device linked to a camera, the button is displayed in the image panel when you watch the camera's video. To listen to the streaming audio, make sure there are speakers connected to your computer. By default the audio is muted.

The camera's microphone must be enabled before you can listen to any audio. The button is not displayed if the microphone is disabled.

To control audio playback, do any of the following:

- In the lower-right corner of the image panel, click to mute or activate the audio.
- Move the slider to change the volume.

To enable the camera's microphone, see *Microphone* on page 110 for more information.

Broadcasting Audio in a View

If there are speakers linked to a camera, the button is displayed in the image panel when you watch the camera's video. The button allows you to broadcast your verbal response to what is occurring in the video, like a Public Address (P.A.) system.

The camera's speakers must be enabled before you can broadcast any audio. The button is not displayed if the speakers are disabled.

- To broadcast audio, hold  and speak into your microphone. The red bar moves to show the microphone's audio input levels. If the level is low, speak louder or adjust the microphone volume in the Windows Control Panel.
- Release the button to stop the broadcast.

To set up two-way audio, see *General Settings* on page 112.

For more information about enabling camera speakers, see *Speaker* on page 111.

Using Instant Replay

To review an event that just occurred, you can immediately access recently recorded video through the instant replay feature.

- Right-click the image panel and select one of the instant replay options:
  - **Replay - 30 Seconds**
  - **Replay - 60 Seconds**
  - **Replay - 90 Seconds**

The image panel immediately plays back the camera's most recently recorded video.

PTZ Cameras

PTZ cameras can be controlled through the image panel on-screen controls or by using the tools in the PTZ Controls pane.

Some tools and features may not be displayed if they are not supported by your camera.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ features. You can control a PTZ camera by using the on-screen controls or by using the tools in the PTZ Controls pane.

For other ways to use the PTZ Controls, see *Keyboard Commands* on page 201.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. In the toolbar, click . PTZ controls are now enabled in image panels that are displaying PTZ video.
2. In the image panel, click .

   The PTZ Controls are displayed in a floating pane immediately beside the image panel.

   NOTE: The controls may appear differently depending on the camera. Some options are disabled or hidden if they are not supported by the camera.

3. To pan or tilt, do one of the following:
    - In the image panel, drag your mouse from the center to move the camera in that direction. The farther the cursor is from the center of the image panel, the faster the camera will move.
    - If the camera supports Click to Center, click anywhere on the image panel to center the camera to that point.



Figure 13: PTZ On-screen controls

4. Use the other PTZ controls to perform any of the following:

To...	Do this...
Zoom	• Click  to zoom in. • Click  to zoom out. • Click the image panel and use the mouse scroll wheel to zoom in and out. • If the camera supports Drag to Zoom, click and drag to create a green box to define the area you want to zoom in and see. • Right-click the image panel and select **Zoom Out Full**.

To...	Do this...
Control the iris	• Click to close the iris. • Click to open the iris.
Control the focus	• Click to focus near the camera. • Click to focus far from the camera.
Program a PTZ preset	1. Move the camera's field of view into position. 2. In the **Presets** drop-down list, select a number then click . 3. In the dialog box, enter a name for the preset. 4. Select the **Set as home preset** check box if you want this to be the camera's Home preset. 5. Click **OK**.
Activate a PTZ preset	Select a preset then click .
Return to the Home preset position	If the PTZ camera supports a Home preset position, click to return the camera to its Home position.
Program a PTZ pattern	1. In the PTZ Controls pane, select a pattern number and click . 2. Use the PTZ controls to move the camera and create the pattern. 3. Click to stop recording the pattern.
Activate a PTZ pattern	In the PTZ Controls pane, select a pattern number and click . The pattern will repeat until the pattern is stopped or another pattern is run.
Program a PTZ tour	For more information, see *Programming PTZ Tours* on the next page.
Activate a PTZ tour	In the PTZ Controls pane, select a tour number and click . The tour will repeat until stopped or until other PTZ controls are used.
Activate an auxiliary command	1. Select an aux command number and click . 2. Click to turn off the auxiliary output.
Display the PTZ camera on-screen menu	1. Click . 2. To move through the menu options, click any of the

To...	Do this...
	following: • Click to move down the options. • Click to move up the options. • Click to confirm your selection. • Click to cancel your selection.
Lock the PTZ controls	Click . Other users will be unable to use the PTZ controls for this camera until you unlock the controls or log out. Users ranked higher in the Corporate Hierarchy will be able to override and re-assign the lock to themselves. **NOTE:** Override feature is only available if all servers in the site are running the same version of the ACC Server software.

Programming PTZ Tours

If the PTZ camera supports guard tours, the tours can be programmed through the PTZ controls pane. Tours allow the PTZ camera to automatically move between a series of preset positions, and can be set to pause at each preset for a specific amount of time for video monitoring.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. Create all the PTZ presets you need for this tour.
2. In the PTZ Controls pane, select a tour number then click . The Edit PTZ Tour dialog box is displayed.
3. Give the tour a name.
4. In the **Tour Pause Duration:** field, enter the amount of time before the tour repeats. Tours repeat until manually stopped, or until other PTZ controls are used.
5. In the **Tour Mode:** drop-down list, select one of the following:
   - **Sequential:** the PTZ camera will go to each preset in the set order.
   - **Random:** the PTZ camera will go to each preset in random order.
6. Select the **Set as default tour** check box if you want this tour to run automatically.
   - The **Default Tour Idle Start Time:** field is now enabled. Enter the amount of time the PTZ camera must be idle before this tour automatically starts.

7. To add a preset to the list, click .
    a. In the **Preset** column, select a preset from the drop-down list.
    b. In the **Move Speed** column, enter how fast you want the PTZ camera to move to this preset. The higher the %, the faster the camera moves.
    c. In the **View Time** column, enter the amount of time you want the PTZ camera to stay at this preset position. The view time is 10 seconds by default.
    d. Repeat this step until all the presets for the tour have been added.
8. To remove a preset, select the preset then click .
9. To re-order a preset, select the preset then click  or . The preset order only affects tours that use Sequential mode.
10. Click **OK** to save the tour.

Triggering Manual Recording

Cameras are set to follow a recording schedule. If an event occurs outside the camera's recording schedule, you can click the record indicator icon to force the camera to record the event. For more information about recording schedules, see *Recording Schedule* on page 62.

The Record Indicator overlay must be enabled to use manual recording. For more information, see *Video Display Settings* on page 113.

Camera Recording States

		
Recording	Recording triggered by an event	Not recording

Starting and Stopping Manual Recording

In an image panel that is displaying video, do either of the following:

- In the top-left corner of the image panel, click  to start manual recording.

  The recording indicator is highlighted in blue to show that the camera is recording. Manual recording continues until it is stopped or until the maximum manual recording time is reached.

- Click  to manually stop video recording.

The maximum manual recording time is configured in the Manual Recording dialog box. For more information, see *Manual Recording* on page 94.

Triggering Digital Outputs

While you monitor live video in an image panel, you can manually trigger any digital output that is connected to the camera.

Digital outputs are configured in the Digital Inputs and Outputs dialog box. For more information, see *Setting Up Digital Outputs* on page 109.

To trigger a digital output:

1. Open the camera's live video in an image panel.
2. In the image panel, click .
3. If there is more than one digital output linked to the camera, you will be prompted to select the digital output you want to trigger.

Answering a Video Intercom Call

If a visitor presses the call button on an Avigilon Video Intercom device, and you are set up to receive calls from that device, a video intercom call opens in a new image panel and you see the caller.

You can click to start a call session with the Video Intercom, or  to ignore the call and close the image panel.

Important: If the call is not answered or ignored the image panel stays open until you close it.

Answering a Call

To answer a call, click .

The following controls are displayed:

Icon	Description
	Mute microphone.
	Adjust volume.
	End call.

You can talk to the caller and trigger any action available in the image panel, such as a door grant, digital output, or recording. As you speak, a dynamic audio bar provides feedback that your microphone is working.

Tip: You can trigger any action in the image panel without answering the call.

NOTE: The ability to grant door access depends on your permissions in the ACM appliance. For more information, see *Granting Door Access* on the next page.

Eliminating Voice Echoing in a Video Intercom Call

Echo cancellation can be configured on the Video Intercom device's Web Interface so that the operator's voice on the speaker is not picked up by the Video Intercom's microphone. However, this will not eliminate echo from the caller's voice unless the microphone used on the ACC Client computer supports echo cancellation.

For best results, ACC operators should use a headset.

Multiple ACC Users Receiving and Answering a Video Intercom Call

After you connect, other ACC users set up to receive calls can click and join in the session. All users who join the session can interact with the visitor according to their privileges.

When more than one operator answers the call, the visitor will hear all operators, but operators may not hear each other. If there are multiple ACC Servers in the site, answering operators must be connected to a common ACC Server to hear the visitor together.

Ending a Call

Click to end the call and close the image panel.

NOTE: An in-progress call session with a Video Intercom does not end if you close your ACC Client or server, log out from your ACC Client, or the ACC Server goes down during a call session. If recording during a call session is configured, it continues until the session on the Video Intercom times out.

Ignoring a Call

To ignore a call, click .

The image panel closes. You can no longer connect to that call session.

Other users enabled to receive calls from that device can still answer the call. The call to those users will continue until it is answered or ignored, or until the session on the Video Intercom times out.

Granting Door Access

If your site is connected to an Access Control Manager appliance, you may be able to grant door access from any camera that is linked to a door.

NOTE: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. For more information, see *Importing ACM Roles* on page 43. Contact your ACM administrator to update your permissions.

1. Open the camera's video in an image panel.
2. Confirm that the person in the video has permission to use the door.
3. In the top-left corner of the image panel, click .

   NOTE: If the camera is not linked to a door, the icon is not displayed.

   If there is more than one door linked to the camera, you will be prompted to select one.

Door access is granted.

Identity Verification

If your camera is linked to a door in the ACM appliance, you can monitor authorized and unauthorized door activity in an adjacent image panel.

NOTE: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. For more information, see *Importing ACM Roles* on page 43. Contact your ACM administrator to update your permissions.

When someone swipes an ACM badge, the identity verification image panel displays a card with the following information if available:

- Badge photo
- First and last name
- Date and time
- ACM door event

The ACM door event provides information about whether door access was granted or denied. The card will have a red border if an unauthorized person tries to gain access or a forced door event occurs.

Compare the video to the badge photo to verify the person's identity and prevent unauthorized access.

Monitoring Door Access

1. Open the camera's video in an image panel.
2. In the top-right corner of the image panel, click  and select the door you want to monitor.

   NOTE: If the camera is not linked to a door, the icon is not displayed.

   An identity verification image panel is displayed. The most recent activity is displayed at the top.

   Tip: You can resize the badge photo using the slider at the top of the identity verification image panel.

NOTE: Activity is only captured for Live video while the View tab is active. If you switch to Recorded mode, the identity verification image panel will remain empty. When you return to Live video, or return from a different tab, three dots will denote that activity may have occurred while you were away.

Monitoring Live POS Transactions

If a camera is linked to a point of sale (POS) transaction source, you can monitor live POS transactions while you monitor video from the linked camera.

1. Open the camera's video in an image panel.
2. In the image panel, click .

   NOTE: If the camera is not linked to a POS transaction source, the icon is not displayed.

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   Each transaction is separated by date and time, and the most recent transaction is highlighted in blue.

3. To display cameras that are linked to the POS transaction source, click  in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.

Triggering Custom Keyboard Commands

If your system has custom keyboard commands set up to run specific rule events, you can activate the keyboard commands by doing the following:

1. Press **Ctrl** + **K** on your keyboard.
2. Enter the custom keyboard command number to begin running the rule event.

Consult your system administrator for details about the custom keyboard commands that are available in your system. Custom keyboard commands are set up as rule events through the Rules engine. For more information about setting up rule events, see *Rules* on page 53.

Working with Maps

A map is a graphical reference of your surveillance site. You can create a map out of any image of your location, then add cameras, encoders, saved Views, and other maps to the image to help you quickly navigate through your surveillance site.

Adding a Map

You can create a map from any image in JPEG, BMP, PNG, or GIF format. The image is used as the map background and cameras are added on top to show where they are located in your surveillance site.

NOTE: The recommended map image size should be no more than 3000 x 3000 px or 9 MP. Larger images may cause rendering issues.

1. In the System Explorer, right-click a site or site folder and select **New Map...**.
2. In the Map Properties dialog box, click **Change Image...** and locate your map image.
3. In the **Name:** field, enter a name for the map.
4. If it is not displayed, click  to display the Site View Editor and choose where the map appears in the System Explorer. By default, the map is added to the site that you initially selected.
   - In the site directory, drag the map up and down the right pane to set where it is displayed.
   - If your site includes folders, select a location for the map in the left pane. The right pane updates to show what is stored in that directory.
5. Click **OK**.

   In the following Editing: Map tab, you can click **Edit Properties...** to open the Map Properties dialog box again.

6. Drag and place cameras from the System Explorer onto the map.

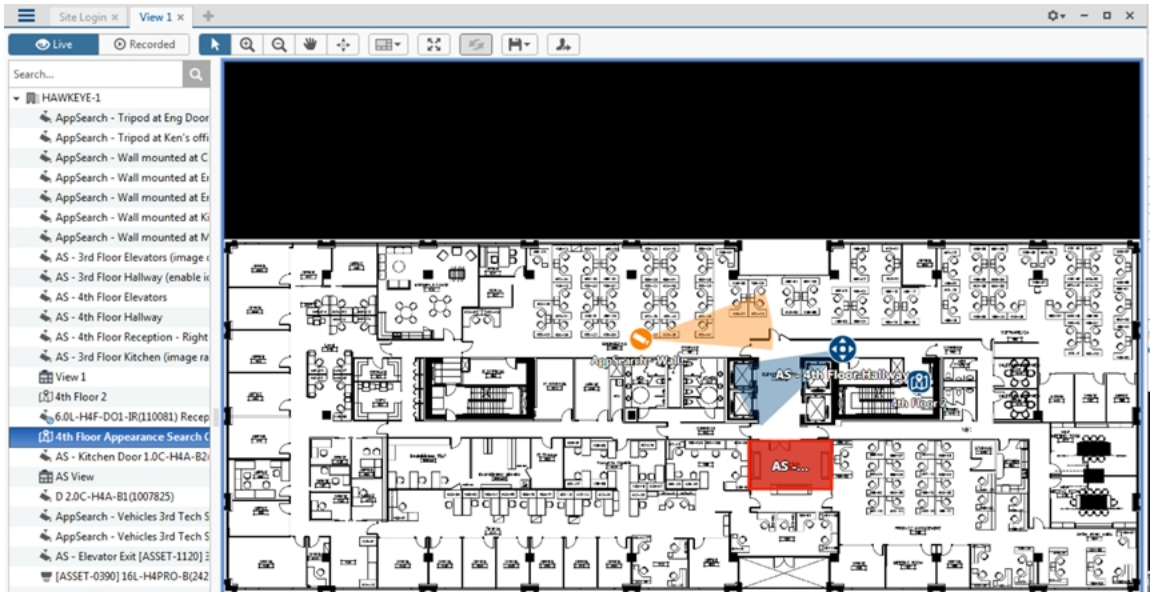


Figure 14: The Editing: Map tab

By default a camera is displayed as an icon with a yellow triangle to represent its field of view.

- Drag the black points at the end of the yellow field of view to re-size and position the camera angle.

7. Drag encoders, saved Views and other maps that you need from the System Explorer onto the map.
8. In the **Map Icon Properties** options, you can change the size and way icons or shapes are displayed on the map. Select any icon on the map then do the following:

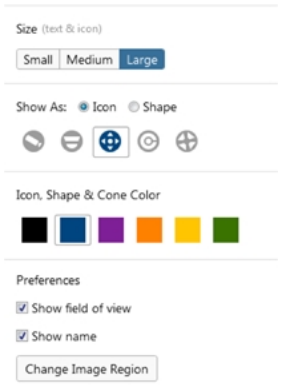


Figure 15: Map Icon Properties options

a. Select **Size** to display the text and icon.

b. To display an icon or shape, select one of the buttons in **Show As:**. Select the color of the icon, shape and cone to display on the map.

c. Select the **Show name** check box to display the object's name on the map.

d. Click **Delete from Map** to remove the object from the map.

e. (Cameras only) Select the **Show field of view** check box to display the camera's yellow field of view. This option is only available when the camera icon is used.

   Drag the corners of the yellow triangle to expand the field of view. Drag the black circle at the end of the triangle to rotate the field of view.

f. (Cameras only) Click **Change Image Region** to define the specific area that is displayed when you access the camera from the map.

   In the following dialog box, move and resize the green overlay to select the region you want to focus on, then click **OK**.

9. Click  to save your new map.

Using a Map

You can open a map in any image panel, then open video or alarms from the map.

1. To open a map in an image panel, do one of the following:
   - Double-click  in the System Explorer.
   - Drag  from the System Explorer to an image panel.
   - In the System Explorer, right-click  and select **Add To View**.
2. When the map appears in an image panel, do any of the following:



Figure 16: Map in an image panel

To...	Do this...
Review an alarm	When a camera flashes in red, an alarm linked to the camera has been triggered. • Click the camera to monitor the live alarm video.
Display video from a camera on the map	• Drag a camera from the map to a different image panel, or • Click the camera on the map.
Display a preview of the video from a camera	• Hover over a camera in the System Explorer or on the map.
Open a linked map	• Click the map icon on the map. You can use the **Forward** and **Back** buttons to move between maps.
Open a linked View	• Click the saved View on the map.

Editing and Deleting a Map

You can update a map or delete an old map anytime.

1. In the System Explorer, right-click  then select one of the following:
   - To edit the map, select **Edit...**. For more information about the available map options, see *Adding a Map* on page 137.
   - To delete the map, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Working with Web Pages

You can quickly review online content while monitoring videos by adding web pages to the System Explorer.

NOTE: Web pages will not load if you do not have internet access.

Adding a Web Page

You can add web pages to a site for quick access to internet content that is related to your surveillance system.

1. In the System Explorer, right-click a site or site folder and select **New Web Page...**.

   The Web Page Properties dialog box is displayed.
2. In the **Name:** field, enter a name for the web page.
3. Enter the web page URL in the **URL:** field.
4. Select a **Zoom level:** for viewing the web page inside an image panel.
5. If it is not displayed, click  to display the Site View Editor and choose where the web page appears in the System Explorer. By default, the web page is added to the site you initially selected.
   - In the  site directory, drag the web page up and down the right pane to set where it is displayed.
   - If your site includes  folders, select a location for the web page in the left pane. The right pane updates to show what is stored in that directory.
6. Click **OK**.

Using a Web Page

To open a web page, do one of the following:

- Double-click  in the System Explorer.
- Drag  from the System Explorer to an image panel.
- In the System Explorer, right-click  and select **Add To View**.

The web page is displayed in one of the image panels. Use the web browser buttons to navigate through the internet.



Figure 17: Web Page controls

NOTE: If the web page does not render, you may need to install the latest version of Internet Explorer.

Editing and Deleting a Web Page

Whenever a web page address becomes out of date, you can choose to update the web page or delete the web page from the site.

- In the System Explorer, right-click URL then select one of the following:
  - To edit the web page, select **Edit...**. For more information about the editable options, see *Adding a Web Page* on the previous page.
  - To delete the web page, select **Delete**. When the confirmation dialog box is displayed, click **Yes**.

Monitoring License Plates

License Plate Recognition (LPR) is a licensed feature that allows you to monitor vehicle license plates that are detected by the ACC software.

You can use the license plate overlay to monitor license plates as they are detected. You can also use the License Plate Watch List feature to alert you when specific license plates are detected. For more information, see *License Plate Recognition* on page 48.

License Plate Overlay

While you monitor video in an image panel, you can also monitor license plates as they are detected by the system.

When the license plate overlay is enabled, detected license plate numbers are displayed in the bottom-right corner of the image panel.

To enable the License Plate overlay:

1. In the top-right corner of the Client window, select ⚙ > **Client Settings** > **Display**.
2. In the Image Overlays: area, select the **License Plate** check box.
3. Click **OK**.

When you display live video for a camera that is configured for license plate recognition, the detected license plates are displayed by the overlay.

Reviewing License Plate Matches

If your system is configured to track specific license plates using a Watch List, you will be notified by a pop-up dialog box when matches are detected.

Select one of the license plate matches and do any of the following:

- Click **View this Event** or double-click the selected license plate to open a snapshot of the detected license plate in a new View.
- Click **Delete** to delete the license plate from the list.
- Click **Clear All** to empty the current match list. The list will be repopulated as new license plates are detected.

Investigating Events

When you receive a report about an event, you can review the recorded video and use the following tools to investigate the sequence of events. The results of your investigation can be exported to provide evidence for prosecution as required.

Controlling Recorded Video

Tip: If video appears slow, it may be a network issue between the ACC Client software and the server that the camera is connected to. Actual recorded video quality is not affected.

Adding and Removing Cameras in a View

To monitor video, add a camera to a View tab. Camera video can be removed from a View tab at any time.

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.
- If your cameras are assigned a Logical ID:, press / and enter a logical id. For more information, see *Cycling Through Cameras* on page 125.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click .

Viewing Live and Recorded Video

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Tip: If you cannot see either  **Live** or  **Recorded** on the toolbar, you may need Dual Authorization. For more information, see *Requesting Dual Authorization* on the next page.

When you monitor video, you can choose to watch live and recorded video in the same View tab, or only one type of video per View tab.

Once you've added cameras to the View tab, you can do the following:

- To switch all of the image panels in the View between live and recorded video, click either **Live** or **Recorded** on the toolbar.
- To switch individual image panels between live and recorded video, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying recorded video have a **green** border.

Requesting Dual Authorization

You need Dual Authorization if a second user must also log into your ACC Client before you can see recorded video.

Before you begin, request permission from a user with authorization power.

1. In the ACC Client, right-click the site then select **Dual Authorization Log In**.
2. In the following dialog box, the second user must enter their username and password.
3. Click **Log In**.

You now have access to recorded video.

Playing Recorded Video with the Timeline

The Timeline displays when video was recorded and lets you control video playback. Recorded video may be stored on the ACC Server or the archive storage location.

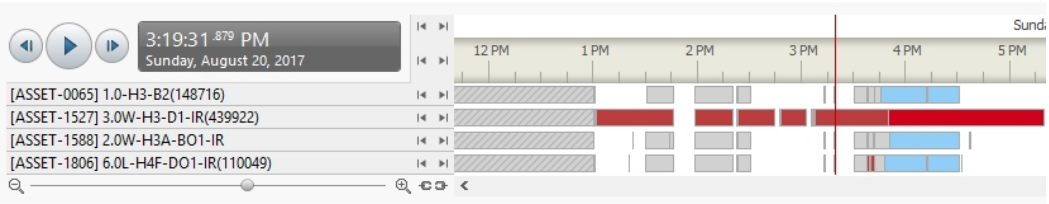


Figure 18: Playback controls on the Timeline

The colored bars on the Timeline show the camera's recording history:

- — shows the camera has recorded a motion event.
- — shows the camera has recorded video.
- — is a bookmark of a recorded event.
- — shows that video archived by the Continuous Archive feature is available. Click the area to load archived video from that time range:
  - — shows archived video of a motion event.
  - — shows archived video.

  Tip: You can also review archived video by opening the archived AVK file in the ACC Player software.

You can view and play through archived video, but you cannot skip between recorded events or search archived video.

- White areas show that there is no recorded video.

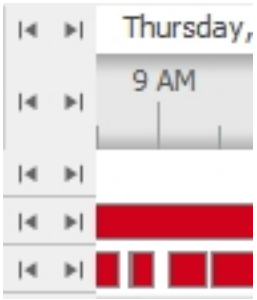
For more information about bookmarks, see *Bookmarking Recorded Video* on page 149.

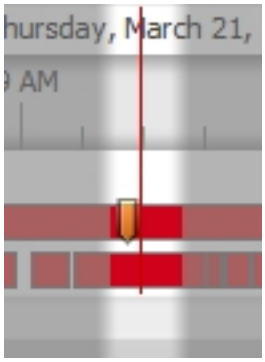
If a camera is configured with failover connections:

- The camera can appear in multiple locations in the system tree. Contact your system administrator to configure your privileges to view the camera under each failover connection.
- To view recorded video, select any instance of the camera in the system tree. A seamless Timeline across failover events is displayed. The video is played from the server that recorded the video.

  For more information, see *Failover Connections* on page 27.

Using the Timeline

To...	Do this...
Select a playback time	• Click the dark gray date display and select a specific date and time. • Click a point on the Timeline.
Start playback	Click . • Click  to fast forward. Tap the arrow again to increase the playback speed. • Click  to rewind. Tap the arrow again to increase the playback speed. You can play the video up to eight times the original speed.
Stop playback	Click . • Click  to step forward one frame. • Click  to step backward one frame.
Jump forward or backward on the Timeline	 On the Timeline, click or to move to set points on the Timeline.
Zoom in or out of the Timeline	 • Move the slider on the bottom left to zoom in or out on the Timeline. • Place your mouse over the Timeline and use the scroll wheel to zoom in or out on the Timeline. You can zoom in to a quarter of a second, and zoom out

To...	Do this...	
		to see years if recorded video exists.
Center the Timeline on the time marker		Right-click the Timeline, and select **Center on Marker.**
Pan the Timeline		• Click and drag the time marker through the Timeline. • Move the horizontal scroll bar under the Timeline. • Right-click and drag the Timeline.

Viewing Unusual Motion Events

When viewing video recorded from an Unusual Motion video analytics device, the Timeline displays both motion events and Unusual Motion events. You can filter the Timeline to display Unusual Motion events only.

NOTE: The Unusual Motion filter is only available if there is at least one camera in the View tab with the Unusual Motion analytics mode enabled.

1. In the top-left corner of the Timeline, select the **Unusual Motion** check box.

   Only Unusual Motion events are displayed on the Timeline. To increase or decrease the number of events displayed, use the Unusual Motion filters. For more information, see *Filtering Unusual Motion Events* on the next page.

2. Use the Timeline controls to view the event video.

   Unusual Motion is trailed by bounding boxes. Image panels without Unusual Motion are dimmed.

   Tip: Select the **Skip Play** check box to skip to the next Unusual Motion event when playing video.

You can bookmark and export Unusual Motion events like other video analytics events. For more information, see *Bookmarking Recorded Video* on page 149 and *Export* on page 173.

Filtering Unusual Motion Events

When the Unusual Motion check box is selected, you can interactively control the amount of Unusual Motion events displayed in the Timeline using the filters described below.

Filter	Description
Anomaly Type	From the drop-down menu, select which Unusual Motion anomalies are displayed: • **All** — All Unusual Motion events are displayed. This is the default setting. • **Speed** — Events with motion at an unusual speed are displayed. • **Direction** — Events with motion in an unusual direction are displayed. • **Location** — Events with motion in an area where motion does not typically occur are displayed.
Rarity	Move the slider to set how rare an Unusual Motion event must be to be displayed on the Timeline. The further right the slider is, the more rare the event. To reduce noise, keep the slider towards the right.
Minimum Duration	Enter a value between **0** and **59** seconds to set the minimum amount of time an Unusual Motion event must last to be displayed on the Timeline. The default value is **2** seconds.

Synchronizing Recorded Video Playback

Synchronizing recorded video playback allows you to synchronize Timelines across multiple tabs while they are in recorded mode.

Synchronized recorded video playback is disabled by default. Once it is enabled, it will remain enabled until it is manually disabled.

NOTE: Tabs can only be synchronized to one time. You cannot synchronize groups of tabs to separate times.

Enabling Synchronized Recorded Video Playback

- To enable synchronized video playback in all new View tabs, select > **Client Settings** > **General** > **Synchronize recorded video playback**.

  The Timelines in new View tabs are automatically centered on the current time.

  Enabling synchronized recorded video playback in the Client Settings dialog box will not synchronize the Timelines of previously opened tabs, it will only synchronize new tabs that are opened after enabling synchronized recorded video playback. Previously opened tabs need to be synchronized individually.

- To synchronize playback between specific tabs, click at the bottom of each Timeline. The icon changes to to show that it is now synchronized.

  The Timeline will synchronize with the first tab you selected.

Disabling Synchronized Recorded Video Playback

- To disable synchronized recorded video playback in all new View tabs, clear the **Synchronize recorded video playback** check box in the Client Settings dialog box.

  Previously synchronized tabs will remain synchronized.

- To disable synchronized video playback in individual tabs, click at the bottom of the Timeline. The icon changes to to show that synchronized playback is disabled.

  The Timeline will continue to display the same time but will no longer be synchronized with other Timelines.

Initiating a Search

While reviewing recorded video, you can initiate a search to find other instances of an object or event.

- In the top-left corner of the image panel, click then select one of the following search options:
  - **Appearances**
  - **Identity**
  - **Motion**
  - **Events**
  - **LPR**
  - **Thumbnails**
  - **Text Source Transactions**
  - **Alarms**
  - **Bookmarks**

  The search will only be performed on the selected camera video.

  For more information about the available search options, see *Search* on page 156.

Bookmarking Recorded Video

You can add bookmarks to recorded video to help you find and review an event later. Bookmarked video can be protected against scheduled data cleanup so that the video is never deleted.

Adding a Bookmark

Tip: You can add a bookmark any time the Timeline is displayed.

1. Drag the time marker to where you want to start the bookmark, then right-click the Timeline and select **Add Bookmark**.

   The Edit Bookmark dialog box appears, and the bookmark time range is highlighted on the Timeline.

2. Enter a name for the New Bookmark.

3. In the **Cameras:** pane, select all the cameras that need to be attached to this bookmark.

   NOTE: You can only bookmark multiple cameras from the same site.

4. In the **Time Range to Bookmark:** area, enter the full duration of the bookmark.

   You can also move the black time range markers on the Timeline to adjust the time range.

5. In the **Description:** field, enter any extra information that you want to include with the bookmark.
6. To protect the bookmark video from being deleted, select the **Protect bookmark data** check box.

   NOTE: Protected bookmarks are never deleted. Be aware that bookmarked videos take up space and can become the oldest video on the server.
7. To make the bookmark private, select the **Bookmark is private** check box. Private bookmarks are only visible to the user who marked the bookmark as private, and the system administrator. No one else will have access to the bookmark.
8. Click **OK**.

Exporting, Editing, or Deleting a Bookmark

- Click the bookmark on the Timeline, then do one of the following:

To...	Do this...
Export a bookmark	Click **Export**, then complete the Export tab. For more information, see *Export* on page 173.
Edit a bookmark	Click **Edit**, then make your changes. For more information about the editable options, see *Adding a Bookmark* on the previous page.
Delete a bookmark	Click **Delete**. When the confirmation dialog box appears, click **Yes**.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.
- On the toolbar, select  or , then click the image panel until you reach the desired zoom depth.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel.
- On the toolbar, select , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click .
- Double-click the image panel.

Making Image Panel Display Adjustments

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings. These settings can also be adjusted in Client Settings. For more information, see *Changing Display Adjustment Settings* on page 114.

1. Right-click an image panel and select **Display Adjustments...**.

   The Display Adjustments... settings are displayed in a floating pane immediately beside the image panel.

2. Move the sliders to adjust the **Gamma:**, **Black Level:** and **White Level:**.

   By default, **Gamma:** is set to 0.55, **Black Level:** is set to 0.5%, **White Level:** is set to 98%, and Auto-Contrast is disabled.

   The image panel displays your changes.

3. Select the **Enable Auto-Contrast** check box to allow the system to automatically adjust the contrast level for the video stream.

   NOTE: When Auto-Contrast is disabled, the **Black Level:** and **White Level:** cannot be adjusted.

4. To clear your changes, click **Restore Defaults**.

   If display adjustments have been made in the Client Settings, they will be applied to the image panel.

5. To set the selected levels as the default settings for all image panels going forward, click **Save as Defaults**.

Listening to Audio in a View

If there is an audio input device linked to a camera, the  button is displayed in the image panel when you watch the camera's video. To listen to the streaming audio, make sure there are speakers connected to your computer. By default the audio is muted.

The camera's microphone must be enabled before you can listen to any audio. The  button is not displayed if the microphone is disabled.

To control audio playback, do any of the following:

- In the lower-right corner of the image panel, click  to mute or activate the audio.
- Move the slider to change the volume.

To enable the camera's microphone, see *Microphone* on page 110 for more information.

Reviewing Recorded POS Transactions

While you watch recorded video, you can review POS transactions that occurred at the same time.

1. Select a camera that is linked to the POS transaction source and display the camera's recorded video
2. In the image panel, click .

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   - Each transaction is separated by date and time.
   - When you select a transaction, the video jumps to that event on the Timeline.
   - Scroll up or down to see other recorded POS transactions.
3. To display cameras that are linked to the POS transaction source, click in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.
4. Use the Timeline to review the video in more detail.

For more information about Timelines, see *Playing Recorded Video with the Timeline* on page 145.

If you want to find a specific POS transaction, see *Performing Text Source Transactions Search* on page 170.

Triggering Custom Keyboard Commands

If your system has custom keyboard commands set up to run specific rule events, you can activate the keyboard commands by doing the following:

1. Press **Ctrl** + **K** on your keyboard.
2. Enter the custom keyboard command number to begin running the rule event.

Consult your system administrator for details about the custom keyboard commands that are available in your system. Custom keyboard commands are set up as rule events through the Rules engine. For more information about setting up rule events, see *Rules* on page 53.

Monitoring Alarms

The Alarms tab allows you to monitor and acknowledge alarms. You can quickly review video of the event, bookmark the recorded incident, and export alarm video for further investigation.

Accessing the Alarms Tab

- At the top-left corner of the application window, select > .

The Alarms tab is divided into a series of vertical alarm panels. The panels display alarms that are currently active, acknowledged or assigned to a user.

To view more alarm panels, use the horizontal scroll bar at the bottom of the Alarms tab.

Tip: The most relevant alarm is in the leftmost panel. Alarm names that are displayed in red indicate alarms that have not been acknowledged.

Panels are sorted from left to right by:

- Alarm status: Alarms Assigned to Me, Active Alarms, Alarms Assigned to Others, Acknowledged Alarms
- Priority
- Most recent alarm trigger time

The alarm panel is divided into the following areas:

- The top of the panel displays the alarm name and status.
- The middle of the panel displays video from all of the cameras linked to the alarm.
- The bottom of the panel displays the Alarm Triggers list and the available alarm response actions.

Reviewing Alarms

In the Alarms tab, you can review and manage alarms. Active alarms can be assigned to yourself, and acknowledged alarms can be exported or purged as required.

Reviewing Alarm Video

You can review active and acknowledged alarms in detail through the alarm panel, or by opening the alarm video in a new View.

Each panel in the Alarms tab displays a different alarm.

1. At the top of the tab, click any of the filters to choose the types of alarms that are displayed.

   Alarms can be filtered by **Active Alarms**, **Alarms Assigned to Me**, **Alarms Assigned to Others**, and **Acknowledged Alarms**.

2. In the Alarm Triggers list, select an alarm trigger to display video for that instance of the alarm.
   - Select **Live** from the top of the list to display the live video stream from the same cameras.
3. You can zoom and pan in the image panels like you would in a regular image panel. For information, see *Zooming and Panning in a Video* on page 150.
4. Click **Open In View** to open the alarm video in a new View.

Acknowledging an Alarm

Acknowledging an alarm shows that an alarm has been reviewed and is no longer active. You can acknowledge any alarm that is active or assigned to you.

Tip: To hide Acknowledged alarms without purging them, disable the **Acknowledged Alarms** filter at the top of the tab.

1. Click **Acknowledge**.
2. If required, enter notes describing the nature of the alarm in the **Acknowledge Alarm** text box.
3. If there is a digital output linked to the alarm, a dialog box may appear to ask for permission to activate the digital output. Activate the digital output as required.

The Alarm is given an Acknowledged status in the system.

Assigning an Alarm

You can assign an alarm to yourself to let others know that the alarm is being reviewed. This includes re-assigning alarms that are currently assigned to someone else.

Although you can only assign alarms to yourself, you can unassign the alarm at any time.

1. In the alarm panel, click **Assign Alarm**.
2. To unassign an alarm, in the alarm panel click **Unassign Alarm**.

Bookmarking an Alarm

You can bookmark active and acknowledged alarm video.

1. Select an alarm then click **Bookmark Alarm**.
2. When the Edit Bookmark dialog box appears, define the details of your bookmark.

   The Edit Bookmark dialog box automatically selects all the cameras that are linked to the alarm, and sets the time range to span the first and last alarm trigger.

3. Click **OK** to save the new bookmark.

For more information about the bookmark options, see *Bookmarking Recorded Video* on page 149.

Purging an Alarm

Purging an alarm removes the acknowledged alarm from the Alarms tab until the alarm is activated again. Although purged alarms are no longer visible, you can still search through the alarm's history.

- In the acknowledged alarm panel, click **Purge Alarm**.

Searching Alarms

You can search through an alarm's history to review other instances of the alarm.

- In the acknowledged alarm panel, click **Search Alarm**.

For more information about searching alarms, see *Performing an Alarm Search* on page 171.

Exporting Alarms

You can export alarm video for review on other computers.

- In the acknowledged alarm panel, click **Export Alarm**.

For information about the export options, see *Export* on page 173.

Arming Image Panels

Arming an image panel reserves the image panel specifically for displaying video linked to alarms or rules. Armed image panels allow you to review and acknowledge alarms while monitoring video in a View. Any image panel can be armed or disarmed as required.

If there are no armed image panels, alarm video will appear in the next empty image panel in the current View, or in a new View if all current image panels are in use.

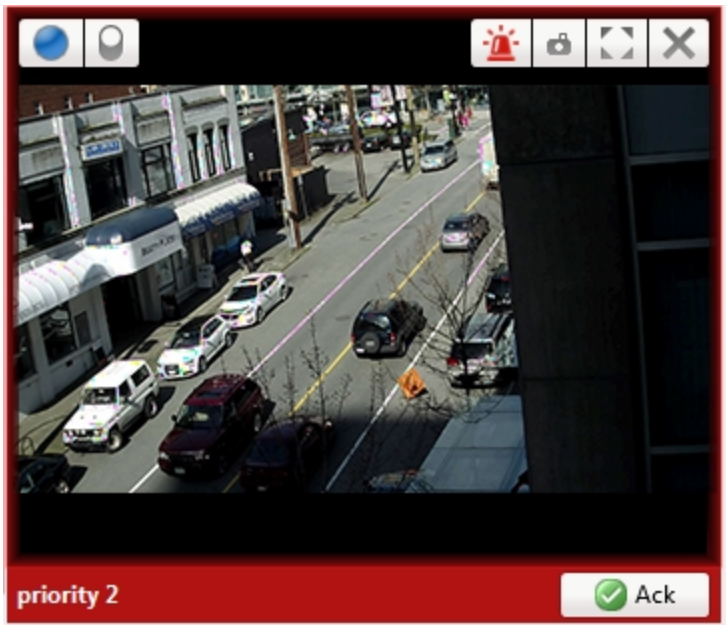


Figure 19: Armed image panel

Tip: You can still use the features that are common to all image panels in an armed panel, like taking snapshots or maximizing the image panel.

To...	Do this...
Arm an image panel	In an image panel, click . The image panel is given a **red** border and an alarm label to show that it is armed.
Acknowledge an alarm	Click .
Move between linked alarm video	If the alarm is linked to multiple cameras, use the green arrows to move between the linked cameras.
Disarm an image panel	In an armed image panel, click .

If multiple alarms are triggered at the same time, the linked videos are queued inside the armed image panel. The alarm videos are displayed by order of alarm priority, then time. Once an alarm is acknowledged or assigned to a user, the alarm video is removed from the armed image panel.

NOTE: If you choose to close a video in the armed image panel, the video is removed but the alarm continues to be active.

Videos triggered by a rule are queued in the armed image panel after alarms, with the most recent video displayed first. Rule videos are not labeled and do not need to be acknowledged.

Search

You can quickly search for recorded video that is linked to an event or search through a camera's recording history. You can also search for presence events detected by the Avigilon Presence Detector sensor.

The different search tabs can be accessed in the following ways:

- At the top-left corner of the application window, click  to open the New Task menu then choose one of the **Search** options. This is the only option available for the Avigilon Presence Detector sensor, which is an indoor-only device that uses a sensor to detect fine motion such as respiration within a short range.
- While the View tab is in Recorded mode, select the  **Search** menu from the toolbar then choose one of the search options.
- While watching recorded video, click  in the image panel then select an available search option. This search will only be performed on the selected camera video.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Avigilon Appearance Search Query

An Avigilon Appearance Search query can be performed after suspicious or unusual activity has been reported. Once the object of interest has been found, you can find instances of a person or vehicle across the entire site.

For example, an employee reports a suspicious man who left a bag at a ticketing counter then left in a red truck at around noon. With this search, you can view the person's movement throughout the site and export the results for the authorities.

As of ACC software version 6.10, you can search for a person by entering their description. You can still search for people or vehicles of interest using an example of the person or vehicle found in recorded video.

NOTE: The search only returns results from Avigilon cameras that have self-learning video analytics and with the Avigilon Appearance Search feature enabled. For more information, see *Enabling the Avigilon Appearance Search™ Feature* on page 73.

Initiating a Search

There are three ways to initiate an Avigilon Appearance Search query:

- Search for a person by their description at a certain time across your site.
- Search recorded video for a person or vehicle at a certain time and place.
- Search recorded video for a person in your ACM system by their door transactions.

The first two methods are described below. For more information on the third method, see *Performing an Identity Search* on page 163.

Searching by Description

If you have a description of a person of interest, you can start an Avigilon Appearance Search query based on the reported characteristics. The results will come from all cameras with the Avigilon Appearance Search feature enabled.

1. Start the search:
   - In the New Task menu , click **Appearances**.
   - In a Recorded View tab, click and select **Appearances**.

   The Appearance Search Options dialog box is displayed.
2. Enter the person of interest's description. You can enter as many or as few descriptors as you want. The system will rank search results that match all descriptors higher.
   - In the **Personal Characteristics** section, select the icons that best represent the person's overall description.
   - In the **Clothing** section, select the icons that best represent what the person is wearing.

     You can select multiple icons for most descriptors.
3. In the **Date Range** section, select a time, date, and duration of video to search.
4. In the **Cameras** section, select which cameras to search. By default, all cameras in your site with the Avigilon Appearance Search feature enabled are selected. You must select at least 1 camera.
5. Click **Search**.

   A Search: Appearance tab opens with search results displayed. Search results that match all of the criteria appear first.

   Only the first 30 minutes of results are shown in the Timeline window, although the selected time range may be longer. Move the window along the Timeline to view results from other times, or use the Search Results Graph. For more information, see *Using the Search Results Graph* on page 159.

   On the left, the Appearance Description panel contains tags that show which descriptors were used.
6. In the Appearance Description panel, refine the search results by adding or removing descriptors.
   - To add a descriptor, expand a category and select a new descriptor.
   - To remove a descriptor, in its tag click **X** or clear the descriptor.

   The search results update automatically.

   Tip: In the Search Results Graph, slide the time box over clusters of peaks to view possible matches. For more information, see *Using the Search Results Graph* on page 159.
7. When you find an image of the person of interest, hover over the search result and click .

   The search results display all instances of the selected person over the selected cameras and time range. The search results can be reviewed and refined. For more information, see *Reviewing Search Results* on the next page.

Searching Recorded Video

If you know where and when a person or vehicle of interest appeared, you can start an Avigilon Appearance Search query by searching recorded video.

1. Search for an instance of the person or vehicle:
    - Perform a Motion, Thumbnails or Alarms search.
    - Use the Timeline to find the reported instance of the person or vehicle you are searching for.
2. Click the Classified Object bounding box around the person or vehicle of interest.
3. Select one of the following to view Avigilon Appearance Search results in a new tab:
    -  **Find Appearances After This** — searches for an instance of the person or vehicle after the selected instance.

      The first 15 minutes of results are shown in the Timeline window, although the Timeline spans 6 hours after the starting point.
    -  **Find Appearances Before This** — searches for an instance of the person or vehicle before the selected instance.

      The last 15 minutes of results are shown in the Timeline window, although the Timeline spans 6 hours before the starting point.
    -  **Additional Search Options** — allows you to select a time range and cameras before performing the search.

      The first 15 minutes of results are shown in the Timeline window, although your time range may be greater.

Reviewing Search Results

The search results populated on the screen may not always show an exact match of the person or vehicle you are looking for. For example, the search results may show other people with similar clothing, or different vehicle models of the same color.

Review search results to determine if they are relevant to the investigation. The following sections describe how to review search results.

Star relevant search results to improve the search accuracy. For more information, see *Refining Search Results* on page 160.

Reference Images

The Appearance Description panel displays a Full Profile reference image. It also displays Face Profile image if the original image or a starred result provides a clear reference image.

Refer to the Appearance Description panel to compare search results with the object of your search.

In the top-left corner, click  to show or hide the Appearance Description panel.

Using the Search Results Graph

The Search Results Graph shows when potential search results appeared. Peaks are more likely to match the search criteria. The yellow star identifies the original search object. More stars are added as you refine the search results and include additional reference images. For more information, see *Refining Search Results* on the next page.

Use the Search Results Graph to view potential results.

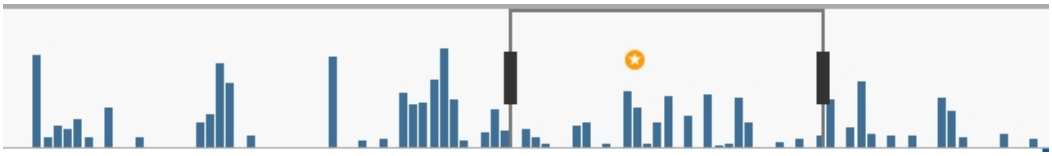


Figure 20: The Search Results Graph.

- The boxed area is a 15-minute segment from which search results are displayed. The time range of the boxed area is displayed above the Search Results Graph. This will typically be a smaller interval within the overall time range for your search.
- Drag the box over clusters of peaks to view search results from that time. You can also expand the time range by dragging the box handles.
- Use your mouse's scroll button to zoom in and out of the graph.
- To update the Search Results Graph time range, click **Edit Time Range**. Enter a new time range and click **Update** to refresh the search results.

  NOTE: Only the first 15 minutes of results are shown in the Timeline window, although the selected time range may be longer. Move the window to see more results.

Sorting Search Results

By default, search results are sorted by **Relevance** and are displayed in decreasing confidence for each time interval.

To view search results grouped by camera:

- In the top-left area click **Camera**.

  Search results are displayed in decreasing confidence from left to right for each camera.

Reviewing Search Result Video

The video associated with a search result is displayed in the image panel on the right. View the search result video to confirm that it relates to the search.

- To play the video associated with a search result, click in the image panel.
- To view video zoomed in on the area of interest, hover over the search result and click or double-click the search result.

  The video associated with the search result is displayed in the image panel, zoomed in on the area of interest.

A white bounding box indicates the detected person or vehicle match. For example, if the video shows two people close together, the person detected will have a white bounding box. If the detected person is a true match, you can star the result. If the detected person is not a true match, you can remove the search result.

Changing Sites or Cameras

You can change which cameras to show results from to refine your search.

If you are logged into multiple sites that support the Avigilon Appearance Search feature and are running the same version of the ACC software, you can view results from different sites.

NOTE: You can only view search results from one site at a time. However, any starred results will remain in the results list.

To change which sites or cameras search results are from:

1. In the top-left area, click **Change Sites/Cameras** or **Change Cameras**.

   A list of sites and cameras with the Avigilon Appearance Search feature enabled are displayed.
   - To show search results from all cameras in a site, select the site check box.
   - To show search results from a camera, select the camera check box.

2. Click **Update**.

   The search results are updated based on the selected cameras.

Restarting a Search

If you're not satisfied with a person search, you can discard the current results and search for a new reference image:

1. In the Appearance Description panel, click **Modify Description**.

   A warning is displayed.

2. Click **Continue**.

   If you had previous descriptors, those results are displayed.

3. Add or update the descriptors and select a new reference image.

Refining Search Results

You can refine the search results by marking good matches with a star to confirm the person or vehicle you are looking for. Starred results are used as reference images to generate improved search results. This allows the system to better identify additional matches of the objects you are looking for.

- To star an image, hover over the search result and click .

  The results are automatically updated with refined search results. The starred search result is displayed at the top of the list, and its associated clip is marked on the Timeline.

  When searching for a person, if the starred result provides a reference image of a person's face, it is added to the Appearance Description panel. Use the image as a reference when reviewing other search results.

  Tip: To show or hide the Appearance Description panel, in the top-left corner click .

- To star multiple search results:
  1. Click the check box in the top-left corner of each search result you want to star.
  2. Below the search results, click .

     The results are automatically refreshed and refined. The starred clips are marked on the Timeline.

- To remove a star from an image, click .

  The search result will no longer be used as a marker and the search results are updated.

- To view additional search results, click **Load More Results**.

Once the results have been refined, you can view the object's sequence of events and save the results. For more information, see *Bookmarking Search Results* below.

Removing Search Results

To help you see the sequence of events more clearly, you can remove search results. Removing search results does not refine the search. It removes the search results from this instance of the search. If the same or similar search is performed again, the removed search results will be displayed again.

For example, if the search results show many instances of a woman instead of a man, or many instances of a red sedan instead of a truck, they can be removed.

1. Select the check box in the top-left corner of each search result.
2. From below the search results, click .

Bookmarking Search Results

The search results can be bookmarked for future reference. You can bookmark starred search results or specific search results.

Bookmarking Starred Results

Starred search results can be bookmarked and used later to perform other searches or to be exported at your convenience. You can bookmark all starred results at once for further investigation.

1. In the top-left area of the Search: Appearance tab, click .

   The New Bookmark dialog box is displayed.

2. Enter a bookmark name and description and click **OK**. For more information, see *Adding a Bookmark* on page 149.

   The bookmark is saved.

Bookmarking Selected Results

Search results often show details of the reported incident, even if they are not starred. These clips can be bookmarked for further investigation.

1. Select the check box in the top-left corner of each search result.
2. From below the search results, click .

   The New Bookmark dialog box is displayed.

3. Enter a bookmark name and description and click **OK**. For more information, see *Adding a Bookmark* on page 149.

   The bookmark is saved.

Exporting Search Results

Search results can be exported for review by other parties. You can export starred search results or specific search results.

Exporting Starred Results

Starred search results can be exported and used later to perform other searches. You can export all starred results at once for further investigation.

1. In the top-left area of the Search: Appearance tab, click .

   An Export tab opens.

2. Update the export settings and click **Start Export**. For more information, see *Export* on page 173.

   The video is exported.

Blurring Exports

To address privacy concerns, you can blur irrelevant details in AVI video exports. This option is available when exporting starred search results, and blurs everything in the field of view around the bounding box for the detected person or vehicle.

If you export multiple starred results, you will blur the field of view surrounding the detected person or vehicle for all results.

NOTE: You cannot blur AVE video exports.

- In the AVI video Export tab, select the **Blur background** check box.

  The export video is blurred.

Exporting Selected Results

Search results often show details of the reported incident, even if they are not starred. These clips can be exported for further investigation.

1. Select the check box in the top-left corner of each search result.
2. From below the search results, click .

   An Export tab opens.
3. Update the export settings and click **Start Export**. For more information, see *Export* on page 173.

   The video is exported.

Identity Search

If your ACC system is connected to an ACM appliance, you can search for a person by their door transactions at a certain date and time. For example, you can determine whether a badged employee tried to access an unauthorized area at a given time. You can also search for video of a person of interest if you know they were with a badged employee who accessed a particular door at a certain time.

The search will display all door transactions for the specified ACM identity along with any video clips from cameras linked to those doors. You will only see video from cameras you have access to.

If your system is configured to use the Avigilon Appearance Search feature, and cameras with the feature enabled are linked to doors, you may be able to initiate an Avigilon Appearance Search query from the search results.

NOTE: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. For more information, see *Importing ACM Roles* on page 43. Contact your ACM administrator to update your permissions.

Performing an Identity Search

You can search for a person in your ACM system by their name or badge ID.

1. Start the search:
   - In the New Task menu, click **Identity**.
   - In a Recorded View tab, click and select **Identity**.

   The Identity Search Options dialog box is displayed.
2. In the **Search:** box:
   a. Enter the person of interest's name or badge ID. Press **Enter** or click .

      Identities and their badge photos, if available, are displayed.

   b. Select the person of interest.

3. In the **Date Range** section, select a time, date, and duration of video to search.
4. In the **Door** section, select the doors you want to search. By default, all doors you have access to are selected. You must select at least 1 door.
5. Click **Search**.

   A Search: Identities tab opens with the person of interest's most recent door transactions from the selected time range. Under each door transaction are video clips from linked cameras. Up to 50 transactions are displayed.

   On the left, the Identity Details panel shows the badge photo of the person of interest, if available. You can select whether to view Access Granted, Access Denied or All transactions.

   If you have cameras with the Avigilon Appearance Search feature enabled that are linked to doors, click **Appearances Only** to view only clips that you can start an Avigilon Appearance Search query from or click **All** to view footage from all cameras linked to doors.

   The search results can be reviewed and refined. For more information, see *Reviewing Search Results* below.

Reviewing Search Results

The video from a search result may show footage from 5 seconds before or after the door transaction. This footage may not always match the person of interest. For example, the video may show a person who entered the door shortly after the person of interest.

Review search results to determine if they are relevant to your investigation.

Reviewing Search Result Video

You can view video from a search result. The video associated with a search result is displayed in the image panel on the right.

- To play the video associated with a search result, click  in the image panel.
- To view video zoomed in on the area of interest, hover over the search result and click  or double-click the search result.

  The video associated with the search result is displayed in the image panel, zoomed in on the area of interest.

If the video is of interest, you can bookmark or export the search result. For more information, see *Bookmarking Search Results* on the next page and *Exporting Search Results* on the next page.

Search results without video footage appear as . This happens if recorded video is no longer stored, or if the camera was not scheduled to record at that time.

Starting an Avigilon Appearance Search Query

If you have cameras with the Avigilon Appearance Search feature enabled that are linked to doors, you can start an Avigilon Appearance Search query from a search result.

- Hover over the search result and click .

  A Search: Appearance tab opens and you can refine your search. For more information, see *Refining Search Results* on page 160.

Changing Doors

You can refine your search by selecting which doors to view transactions from.

1. In the top-left area, click **Change Doors**.

   A list of doors you have access to is displayed.

   - To show search results from a door, select its check box.
   - To hide search results from a door, clear its check box.
   - To show search results from all doors, select the site check box.
2. Click **Update**.

   The search results are updated.

Changing the Time Range

You can refine your search by selecting a different time range.

1. In the top-left area, click **Edit Time Range**.
2. Enter a new time range and click **Update**.

   The search results are updated.

Bookmarking Search Results

You can bookmark search results of interest for further review.

1. Select the check box in the top-left corner of each search result.
2. From below the search results, click .

   The New Bookmark dialog box is displayed.
3. Enter a bookmark name and description and click **OK**. For more information, see *Adding a Bookmark* on page 149.

   The bookmark is saved.

Exporting Search Results

You can export search results of interest for further investigation.

1. Select the check box in the top-left corner of each search result.
2. From below the search results, click .

   An Export tab opens.

3. Update the export settings and click **Start Export**. For more information, see *Export* on page 173.

   The video is exported.

Performing a Motion Search

The  Motion Search tab allows you to search for classified object motion and pixel motion.

NOTE: Classified Object Motion search is always displayed but only video from a self-learning video analytics device will generate meaningful search results.

1. Open the Search: Motion tab. For more information about accessing the search tab, see *Search* on page 156.
2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. Select the type of motion search that you would like to perform:

Search Type	Description
Click **Classified Object Motion** to search for objects detected by a video analytics camera.	a. In the Classified Object Motion area, check the  box to search for persons. b. Check the  box to search for vehicles. c. Move the **Confidence:** slider to set how certain the system must be that it identified the correct object type. d. Enter a time in seconds in the **Object Duration:** field to define how long each result must be in the scene. e. Select one of the following options: • **Individual objects** — select this option to display each classified object as an individual search result. • **Joined by time** — select this option to display objects that appear simultaneously as one search result. Define the minimum number of **seconds apart** before the next search result is generated.
Click **Pixel Motion** to search for tiny pixel changes in a specific area in the camera's field of view.	a. In the Pixel Search Options: area, click the toggle to set the Motion Activity overlay on or off. If enabled, pixel motion in the search results are highlighted in red. b. Drag the **Threshold:** slider to select the amount of motion required to return a search result. A high threshold requires more pixels to change before

Search Type	Description
	results are found. c. Enter a number in the **Join results less than** field to set the minimum number of seconds between separate search results. You can enter any number between 1-100 seconds.

5. Define the green search area by using the tools above the image panel.

   For more information about using the classified object motion tools, see *Setting Up Classified Object Motion Detection* on page 104.

   For more information about using the pixel motion tools, see *Setting Up Pixel Motion Detection* on page 102.

6. Click **Search**.

Viewing Search Results

Depending on the type of Motion Search you performed, some of the following options may not be available.

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and available video is displayed in the image panel. Details about the search result are displayed to the right.

   If you performed a Classified Object Motion search, the objects in the search result are highlighted in the image panel.

2. Use the Timeline controls to review the event.

   For more information, see *Playing Recorded Video with the Timeline* on page 145.

3. Click **Export this event** to export the selected event video.

   For more information, see *Export* on page 173.

4. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see *Bookmarking Recorded Video* on page 149.

5. Click **Add to new View** to display the search result video in a new View tab.

6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a text file or a comma-separated values (CSV) file.

7. If you performed a Classified Object Motion search and chose to join the search results, you will have the option to **Find individual objects in this event**. Click this button to perform a new search to identify each individual object in the search result.

Performing an Event Search

The  Event Search allows you to search for specific events that the system is configured to identify.

1. Open the Search: Event tab. For more information about accessing the search tab, see *Search* on page 156.
2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Events to Search For:** area, select the types of events to include in the search.
   - Select **Motion Events** to find events detected in the camera's Motion Detection area.
   - Select **Digital Input Events** to find events detected by digital inputs that are connected to the selected cameras.
   - Select **Classified Object Events** to find events detected in the camera's Analytic Events area.
   - Select **Arbitrary Events** to find events configured through the ONVIF compliant driver.
   - Select **Presence Events** or **Presence Dwell Events** to find events detected by the Avigilon Presence Detector (APD) sensor.
5. Click **Search**.

Viewing Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and available video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see *Playing Recorded Video with the Timeline* on page 145.
3. Click **Export this event** to export the selected event video.

   For more information, see *Export* on page 173.
4. If you want to further refine your search, click **Perform a motion search on this event**. You can now search for detailed changes in the selected search result.

   For more information, see *Performing a Motion Search* on page 166.
5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see *Bookmarking Recorded Video* on page 149.
6. Click **Add to new View** to display the search result video in a new View tab.
7. Click **Open View to Event Time** to display the search result video in a new View tab. If the device is not connected to a camera, the View tab will be empty. Add a camera to see video from that time.
8. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a text file or a comma-separated values (CSV) file.

Performing a License Plate Search

The  License Plate Search allows you to search for detected license plates.

NOTE: The License Plate Search is only available if the License Plate Recognition feature is installed.

1. Open the Search: License Plates tab. For more information about accessing the search tab, see *Search* on page 156.
2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **License Plate Search Options:** area, enter the license plate you want to find and a minimum confidence of a match.
5. Click **Search**.

Viewing Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and available video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see *Playing Recorded Video with the Timeline* on page 145.
3. If the search result is linked to multiple cameras, select a camera from the drop-down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see *Export* on page 173.
5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see *Bookmarking Recorded Video* on page 149.
6. Click **Add to new View** to display the search result video in a new View tab.
7. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a text file or a comma-separated values (CSV) file.

Performing a Thumbnail Search

The  Thumbnail Search is a visual search that displays search results as a series of thumbnail images.

1. Open the Search: Thumbnails tab. For more information about accessing the search tab, see *Search* on page 156.
2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the image panel, move or drag the edges of the green overlay to focus the search on one area in the video image. Only the area highlighted in green will be searched.
5. Click **Search**.

Viewing Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails** or **Small Thumbnails** from the menu above the search results.

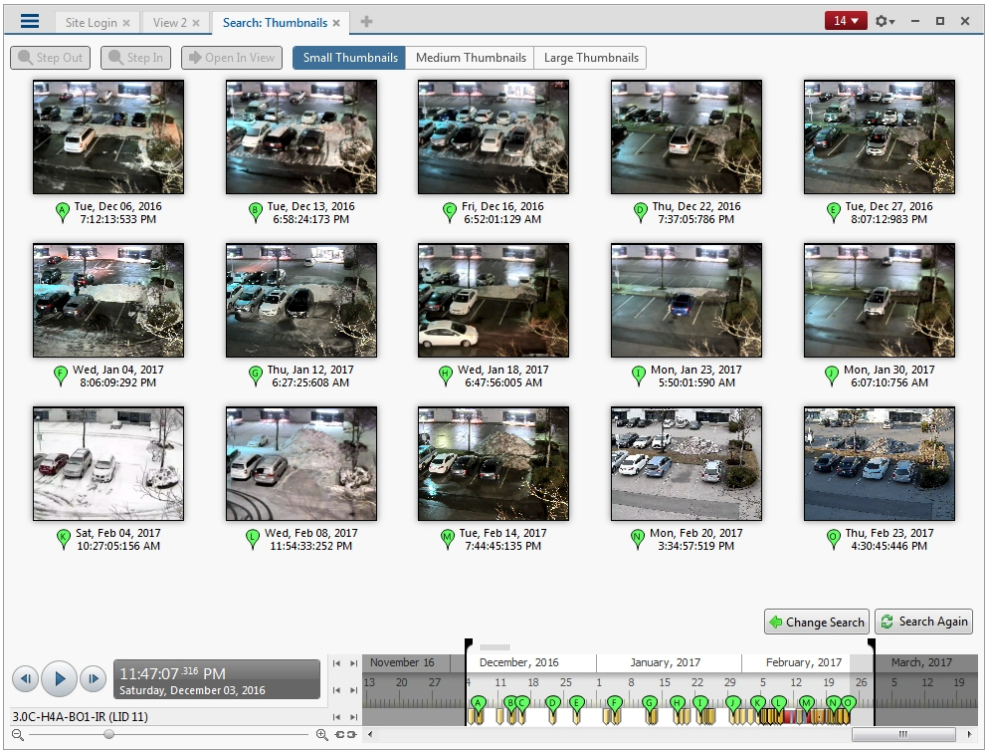


Figure 21: The Search: Thumbnails results tab

2. Select a thumbnail to highlight the video on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Step Out** to return to the previous results page.
4. Click **Open In View** (after selecting a thumbnail) to open the recorded video in a new View.
5. Click **Change Search** to change the search criteria.

Performing Text Source Transactions Search

The Text Source Transactions Search allows you to search for specific transactions recorded by the POS transactions feature.

1. Open the Search: POS Transactions tab. For more information about accessing the search tab, see *Search* on page 156.
2. In the **POS Transaction Sources to Search:** area, select all the POS transaction sources you would like to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is

highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. In the **Search Text:** area, enter any text that will help you filter the search results. For example, you can enter product names or transaction values.

   Use **Wildcards** and **Regular expressions** search methods to find a range of results. Leave the **Text:** field blank to find all transactions.

5. Click **Search**.

Viewing Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and available video is displayed in the image panel. Details about the search result are displayed to the right.

   You can resize the image panel, search results and result details to see the information more clearly.

2. Use the Timeline controls to review the event.

   For more information, see *Playing Recorded Video with the Timeline* on page 145.

3. If the search result is linked to multiple cameras, select a camera from the drop-down list above the image panel to change the video that is displayed.

4. Click **Export this event** to export the selected event video.

   For more information, see *Export* on page 173.

5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see *Bookmarking Recorded Video* on page 149.

6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a text file or a comma-separated values (CSV) file.

Performing an Alarm Search

The Alarm Search allows you to search through an alarm's history.

1. In the New Task menu, click  in the **Search** area.

   The Search: Alarms tab is displayed.

2. In the Alarms to Search: list, select all the alarms you would like to include in the alarm search.

3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. Click **Search**.

Viewing Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and available video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see *Playing Recorded Video with the Timeline* on page 145.
3. If the search result is linked to multiple cameras, select a camera from the drop-down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see *Export* on the next page.
5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see *Bookmarking Recorded Video* on page 149.
6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a text file or a comma-separated values (CSV) file.

Performing a Bookmark Search

The  Bookmark Search allows you to search for a specific bookmark.

1. Open the Search: Bookmark tab. For more information about accessing the search tab, see *Search* on page 156.
2. In the **Search:** field at the top of the tab, enter any text that may appear in the bookmark's title, description, linked camera name or the name of the user who created the bookmark.

   The search is automatically performed on all the listed bookmarks until only the matches are displayed.

Viewing Search Results

1. In the Bookmark list, select a bookmark.

   The bookmark is highlighted on the Timeline and the video is displayed in the image panel. Details about the bookmark are displayed under the image panel.

   To select and configure multiple bookmarks, see *Managing Multiple Bookmarks* on the next page.
2. Use the Timeline controls to review the event.

   For more information, see *Playing Recorded Video with the Timeline* on page 145.
3. If the search result is linked to multiple cameras, select a camera from the drop-down list above the image panel to change the video that is displayed.
4. To export the selected bookmark, click **Export this event**.

   For more information, see *Export* on the next page.

5. If you want to further refine your search, click **Perform a motion search on this event**. You can now search for more detailed changes in the selected bookmarked video.

   For more information, see *Performing a Motion Search* on page 166.

6. To edit the bookmark, click **Edit this bookmark**.

   For more information, see *Bookmarking Recorded Video* on page 149.

7. To export a list of all bookmarks in the system, click **Export results to a file** and save the file. The list can be saved as either a text file or a comma-separated values (CSV) file.

Managing Multiple Bookmarks

1. To select multiple bookmarks from the Bookmark list, do any of the following:
   - To select non-consecutive bookmarks, press `Ctrl` + click the bookmarks.
   - To select consecutive bookmarks, press `Shift` + click the bookmarks.
   - To select all bookmarks, press `Ctrl + A`.

   Additional options are displayed below the Bookmark list. These options affect the selected bookmarks.

2. To protect selected bookmarks, click .

   The bookmark video is protected from being deleted. Be aware that bookmarked videos take up space and can become the oldest video on the server.

3. To remove protection from protected bookmarks, click .
4. To export the selected bookmarks, click .

   A new Export tab is opened. For more information, see *Export* below.

5. To delete selected bookmarks, click .
6. To deselect the bookmarks, click  on the left of the options bar.

Export

You can export video in multiple video and image formats. The Export tab can be accessed from bookmark options, the New Task menu and any Search tab.

You can also export snapshots of an image panel as you monitor video.

Export video of individual events and back up video for your archives. For more information, see *Storage Management* on page 70.

If a camera is configured with failover connections, you can export a seamless video that includes failover events. The ACC system will automatically select all camera instances and compile the video from the servers that recorded the video. For more information, see *Failover Connections* on page 27.

Exporting a Snapshot of an Image

You can export a snapshot of any image panel with video. When you export a snapshot, you are exporting what the image panel is currently displaying.

1. To export a snapshot, do one of the following:
   - In the image panel, click .
   - Right-click the image panel and select **Save Snapshot**.

   The Export tab opens and your snapshot is displayed in the image panel.
2. In the **Format:** drop-down list, select the export file format then define your preferences:

Format	Export Options
Native **NOTE:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains its original compression and can be authenticated against tampering in the Avigilon Control Center Player software. • Select the **Export Control Center Player** check box if you want to include a copy of the Avigilon Control Center Player software with the export. • Click **Burn to Disc** to burn the export file directly to disk rather than export the file first.
PNG image	1. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop-down arrow to select a standard resolution. **NOTE:** The Resolution: field automatically maintains the image aspect ratio. 2. Select the image overlays you want: **Timestamp**, **Device name** and **Device location**. 3. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and **White Level:**.
JPEG image	1. In the **Quality:** drop-down list, select the exported image quality level. 2. Set the image **Resolution:**. 3. Select the image overlays you want. 4. Click **Display Adjustments...** to modify the image quality.
TIFF image	1. Set the image **Resolution:**. 2. Select the image overlays you want. 3. Click **Display Adjustments...** to modify the image quality.
Print image	1. Select the image overlays you want. 2. Click **Display Adjustments...** to modify the image quality. 3. Click **Printer Settings...** to change the selected printer

Format	Export Options
	and paper size. 4. Click **Add Export Notes...** to add notes about the snapshot. The notes are printed below the image.
PDF file	1. Select the image overlays you want. 2. Click **Display Adjustments...** to modify the image quality. 3. Click **Add Export Notes...** to add notes about the snapshot.

3. Adjust the image region that is exported. You can zoom, pan, or crop the image to only export the region of interest. Depending on the camera, you can adjust the image region in the following ways:
   - If available, use the zoom and pan tools above the image panel to adjust the video image that is exported.
   - Otherwise, click **Change Image Region...**. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**. If you are printing the snapshot, the image is sent to your printer instead.

   The Preview area displays the snapshot you are exporting.
6. When the export is complete, click **OK**.

Exporting Native Video

The Native (AVE) format is the recommended format for exporting video. You can export video from multiple cameras in a single file, and the video maintains its original compression. AVE video export also includes the original video metadata so you can search the exported video, including video analytics data.

AVE video is played in the Avigilon Control Center Player, where the video can be authenticated against tampering and re-exported to other formats. If you enable password-protected export, only viewers with the password will be able to access the video. Password-protected video cannot be re-exported in the Avigilon Control Center Player.

If there is audio linked to the video, the audio is automatically included in the export.

If you are exporting a large duration of video or video from many cameras, use the Maximum file size: option to create multiple smaller files, or archive the video instead. Archiving a large amount of video is faster than exporting. For more information, see *Archiving Recorded Video On Demand* on page 72.

1. At the top-left corner of the application window, select  > . The Export tab opens.
2. In the **Format:** drop-down list, select **Native**.
3. To allow only authorized viewers to see the exported video, select the **Password protect export** check box.
    - Enter a new password and then confirm the new password.

      The strength bar indicates how easy it is for an unauthorized user to guess your password.
4. From the **Cameras:** drop-down explorer, select the camera video that you want to export.

   A preview of the video is displayed in the image panel. Use the Timeline controls to playback the video. For more information, see *Playing Recorded Video with the Timeline* on page 145.

   Tip: You can select more than one camera for this type of export.
5. Enter the Time Range you want to export. The Time Range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
6. If you want to add another video clip to the export, click **Add clip** then select the required cameras and time range.

   The Add clip feature allows you to export video from different combinations of cameras and different time ranges as one export file.

   For example, there is a person that is suspected of stealing from a store. During the investigation, you discover that the same person visits the store multiple times over one week. The Add clip feature allows you to export one file that includes all video of the suspect from the week.

   Repeat this step until you've added all the clips that you need. You can remove a clip from the export by clicking the **X** button in the top-right corner of the clip area.
7. From the **Image Rate:** drop-down list, select how many images per second are exported.

   For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

   To define a specific image rate, select **Custom (ips)** then enter the image rate in minutes and seconds. If you enter 1 minute and 0 seconds, one frame of video is exported for each minute of the export.

   NOTE: If you are exporting video from H.265 or H.264 cameras, use the default **Full** image rate setting. Partial and custom image rate exports only apply to cameras using MJPEG or JPEG2000 compression.
8. If the export duration is long or includes many cameras, select a **Maximum file size:** to automatically divide the export into separate files.

   This option lets you export smaller files for storage on a flash drive or on optical media, and minimizes exporting and loading issues.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
9. If you want to include a copy of the Player application with the export, select the **Export Control Center Player** check box.

10. To export the file, do one of the following:
    - To save the file locally, click **Start Export**.
        - In the Save As dialog box, name the export file and click **Save**.
    - To burn the file directly to disc media, click **Burn to Disc**.
        a. When the dialog box appears, insert a disc and select the media burning drive.
        b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.
        c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.
        d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

    Tip: While the file is being exported, you can continue to use the Client software in other tabs.

    The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with lower compression to enhance the function of HDSM technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

    Generally, if you export a 2 minute video from a 2MP H.264 HD camera into AVE format, you will export a 93 MB file.

11. When the export is complete, click **OK**.

Exporting AVI Video

Video exported in Audio Video Interleave (AVI) format can be played in most media players. You can only export one video per tab in this format, but you can have several export tabs active at the same time. If you choose to export to a disc, you can simultaneously export one video for each DVD-R drive on your machine.

If there is audio linked to the video, the audio is automatically included in the export.

1. At the top-left corner of the application window, select  > . The Export tab opens.
2. In the **Format:** drop-down list, select **AVI video (legacy)**.
3. From the **Cameras:** drop-down explorer, select the camera video that you want to export.

    A preview of the video is displayed in the image panel. Use the Timeline controls to playback the video. For more information, see *Playing Recorded Video with the Timeline* on page 145.
4. Enter the Time Range you want to export. The Time Range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.

    The export will automatically skip any recording gaps in the selected time range.
5. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop-down arrow to select a standard resolution.

    NOTE: The Resolution: field automatically maintains the image aspect ratio.

6. Select the image overlays that you want to display in the export: **Timestamp**, **Device name** and **Device location**.

   NOTE: The Timestamp displays the time that was recorded by the server that the camera is connected to.

   Select the **Video analytics activity** check box to include classified object and unusual motion bounding boxes in the export. The bounding boxes will be embedded in the video and cannot be removed from the export.

7. Adjust the image region that is exported. You can zoom, pan, or crop the image to only export the region of interest. Depending on the camera, you can adjust the image region in the following ways:

   - If available, use the zoom and pan tools above the image panel to adjust the video image that is exported.
   - Otherwise, click **Change Image Region...**. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.

8. To export the file, do one of the following:

   - To save the file locally, click **Start Export**.
     - In the Save As dialog box, name the export file and click **Save**.
   - To burn the file directly to disc media, click **Burn to Disc**.
     a. When the dialog box appears, insert a disc and select the media burning drive.
     b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.
     c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.
     d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

   Tip: While the file is being exported, you can continue to use the Client software in other tabs.

   The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to enhance the function of HDSM technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

   Generally, if you export a 2 minute video from a 2MP H.264 HD camera into uncompressed AVI format, you will export a 2.7 GB file.

   To reduce the file size you can reduce the video resolution, or focus the export on a specific image region. Note that reducing the resolution may result in blurriness.

   If it is important to have a high quality export, use the AVE export format instead. AVE export intelligently compresses the video to create a smaller export file while maintaining video data so that you can search, re-export video, and authenticate the video against tampering through the Avigilon Control Center Player software.

9. When the export is complete, click **OK**.

Exporting Still Images

Video can be exported as a series of still PNG images, JPEG images, or TIFF images. When you export a series of still images, you are exporting each frame of video as an independent file.

If you only want one photo of the video you are watching, take a snapshot. For more information, see *Exporting a Snapshot of an Image* on page 173.

1. At the top-left corner of the application window, select  > . The Export tab opens.
2. In the **Format:** drop-down list, select **PNG images**, **JPEG images**, or **TIFF images**.
3. From the **Cameras:** drop-down explorer, select the camera video that you want to export.

   A preview of the video is displayed in the image panel. Use the Timeline controls to playback the video. For more information, see *Playing Recorded Video with the Timeline* on page 145.
4. Enter the Time Range you want to export. The Time Range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. (JPEG only) In the **Quality:** drop-down list, select the exported image quality level.
6. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop-down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
7. From the **Image Rate:** drop-down list, select how many images per second are exported.

   For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

   To define a specific image rate, select **Custom (ips)** then enter the image rate in minutes and seconds. If you enter 1 minute and 0 seconds, one frame of video is exported for each minute of the export.
8. To limit the number of images that are exported, enter a maximum number in the **Images to Export:** field or use the default Unlimited setting.

   The export stops when the maximum number is reached, or when the end of the export time range is reached.
9. Select the image overlays that you want to display in the export: **Timestamp**, **Device name** and **Device location**.

   NOTE: The Timestamp displays the time that was recorded by the server that the camera is connected to.
10. Adjust the image region that is exported. You can zoom, pan, or crop the image to only export the region of interest. Depending on the camera, you can adjust the image region in the following ways:

    - If available, use the zoom and pan tools above the image panel to adjust the video image that is exported.
    - Otherwise, click **Change Image Region...**. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
11. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:**, **White Level:**, or **Enable Auto-Contrast**.

The Display Adjustment Settings: can be adjusted and restored for all image panels from the **Client Settings**. For more information, see *Changing Display Adjustment Settings* on page 114.

The Display Adjustment Settings: can be adjusted for each image panel or for all image panels from the **Display Adjustments...** floating pane. For more information, see *Making Image Panel Display Adjustments* on page 151.

12. Click **Start Export**.
13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video you are exporting.
14. When the export is complete, click **OK**.

Exporting a Print Image

You can export a frame of video directly to your printer or as a PDF. The export can also include any notes you may have about the image.

Tip: You can perform a similar export by taking a snapshot. For more information, see *Exporting a Snapshot of an Image* on page 173.

1. At the top-left corner of the application window, select  > . The Export tab opens.
2. In the **Format:** drop-down list, select **Print image** or **PDF file**.
3. From the **Cameras:** drop-down explorer, select the camera video that you want to export.

   A preview of the video is displayed in the image panel. Use the Timeline controls to playback the video. For more information, see *Playing Recorded Video with the Timeline* on page 145.
4. On the Timeline, move the red time marker to locate the video image that you want to export.
5. Select the image overlays that you want to display in the export: **Timestamp**, **Device name** and **Device location**.

   NOTE: The Timestamp displays the time that was recorded by the server that the camera is connected to.
6. Adjust the image region that is exported. You can zoom, pan, or crop the image to only export the region of interest. Depending on the camera, you can adjust the image region in the following ways:
   - If available, use the zoom and pan tools above the image panel to adjust the video image that is exported.
   - Otherwise, click **Change Image Region...**. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
7. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:**, **White Level:**, or **Enable Auto-Contrast**.

   The Display Adjustment Settings: can be adjusted and restored for all image panels from the **Client Settings**. For more information, see *Changing Display Adjustment Settings* on page 114.

The Display Adjustment Settings: can be adjusted for each image panel or for all image panels from the **Display Adjustments...** floating pane. For more information, see *Making Image Panel Display Adjustments* on page 151.

8. (Print Image Only) Click **Printer Settings...** to change the printer and paper size.
9. Click **Add Export Notes...** to add notes about the exported image. The notes are added below the image.
10. Click **Start Export**.
    - If you are exporting a Print image, the image is sent to the printer.
    - If you are exporting a PDF file, save the image.

    The Preview area displays the video you are exporting.
11. When the export is complete, click **OK**.

Exporting WAV Audio

If you want to export audio with video, simply export the video in Native or AVI format. Any audio that is linked to the video is automatically included in the export file.

This procedure exports the audio alone.

1. At the top-left corner of the application window, select > . The Export tab opens.
2. In the **Format:** drop-down list, select **WAV audio**.
3. In the **Cameras:** drop-down list, select the camera that the audio is linked to.
4. Enter the Time Range you want to export. The Time Range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video that is linked to the audio you are exporting.
7. When the export is complete, click **OK**.

Appendix

Detailed Feature Descriptions

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

This section provides a detailed list of the options that are available when you configure the following features:

Email Notification Trigger Descriptions

The following table shows the email notification trigger options that are available when you set up an email notification. For more information about setting up an email notification, see *Configuring Email Notifications* on page 44.

Email Notification Trigger	Description
System event	Email notifications are sent when one of the following rule events occurs: • Server application starting up • Server application shutting down • Server application terminated unexpectedly • Server application low on resources • Server application installation error • Server connection lost • Server hardware event • Connection created to standby server • Connection removed from standby server • Connection failed • Connection restored • Network connection found • Network connection lost • Network packet loss acceptable • Network packet loss unacceptable • License expires soon • License expired • Database error • Data initialization error • Data volume size reduced • Data write error • Data upgrade started

Email Notification Trigger	Description
	• Data upgrade completed • Data upgrade failed • Data volume failed • Data volume recovered • Data recovery started • Data recovery completed • Data recovery failed • Firmware upgrade failed • Recording interrupted • Recording resumed
Motion detected on _	An email notification is sent when camera motion detection has started. You can select the camera.
Digital input activated on _	An email notification is sent when a digital input has been activated. You can select the digital input.
POS transaction exception on _	An email notification is sent when a POS transaction exception occurs. You can select the transaction source.

Group Permission Descriptions

The following table shows the options that are available when you set up a permission group. For more information about setting up a permission group, see *Adding Groups* on page 39.

Group Permission	Description
View live images	Allows users to watch a camera's live video stream in a View.
Use PTZ controls	Allows users to use a camera's PTZ controls.
Lock PTZ controls	Allows users to lock a camera's PTZ controls.
Trigger manual recording	Allows users to record video outside of a camera's recording schedule while watching video in a View.
Trigger digital outputs	Allows users to trigger digital outputs while watching video in a View.
Broadcast to speakers	Allows users to broadcast audio through speakers that are connected to a camera.
View high-resolution images	If there are multiple video resolution streams, allows users to watch, export, and archive a camera's high-resolution video stream.
View recorded images	Allows users to watch a camera's recorded video in a View.

Group Permission	Description
Export images	Allows users to export recorded images.
View images recorded before login	Allows users to view images recorded before their current login session.
Archive images	Allows users to back up recorded images.
Create teach markers	Allows users to assign Teach Markers in recorded video.
Identity-related search	Allows users to perform the following searches, if configured: • Appearances • Identity • LPR • Text Source Transactions
Manage saved views	Allows users to add and edit saved Views.
Trigger Digital Output	Allows users to trigger digital outputs from an image panel.
Manage maps	Allows users to add and edit maps.
Manage web pages	Allows users to add and edit web pages.
Manage virtual matrix monitors	Allows users to add and edit Virtual Matrix monitors.
Initiate collaboration sessions	Allows users to initiate collaboration sessions with other users on the same network.
Manage user sessions	Allows users to log other users out of the site.
Listen to microphones	Allows users to listen to microphones that are connected to a camera.
Broadcast to speakers	Allows users to broadcast audio from camera speakers.
Setup devices	Allows users to configure cameras.
Setup general settings	Allows users to edit a camera's General dialog box.
Setup network settings	Allows users to edit the Network dialog box.
Setup image and display settings	Allows users to edit the Image and Display dialog box.
Setup web configuration settings	Allows users to edit the Web Configuration dialog box.
Setup image and display settings	Allows users to edit the Image and Display dialog

Group Permission	Description
	box.
Setup compression and image rate settings	Allows users to edit the Compression and Image Rate dialog box.
Setup image dimension settings	Allows users to edit the Image Dimensions dialog box.
Setup motion detection settings	Allows users to edit the Motion Detection dialog box.
Setup privacy zone settings	Allows users to edit the Privacy Zones dialog box.
Setup manual recording settings	Allows users to edit the Manual Recording dialog box.
Setup digital input & output settings	Allows users to edit the Digital Inputs and Outputs dialog box.
Setup microphone settings	Allows users to edit the Microphone dialog box.
Setup speaker settings	Allows users to edit the Speaker dialog box.
Setup analytics settings	Allows users to edit the Analytic Events dialog box.
Setup teach by example	Allows users access to the Teach By Example tab, and the ability to apply or remove Teach Markers from an analytics device.
Setup PTZ settings	Allows users to edit PTZ presets and tours.
Setup sites	Allows users to configure sites.
Setup name	Allows users to edit the site name.
Manage site	Allows users to add and upgrade servers in a site.
Setup site view	Allows users to organize the order of cameras in the System Explorer.
Setup user and group settings	Allows users to edit the Users and Groups dialog box.
Setup Active Directory Synchronization	Allows users to set up Active Directory Synchronization.
Setup corporate hierarchy	Allows users to edit the Edit Corporate Hierarchy dialog box.
Setup alarm management settings	Allows users to edit the Alarms dialog box.
Setup POS transaction settings	Allows users to edit the POS Transactions dialog box.

Group Permission	Description
Setup LPR settings	Allows users to edit the License Plate Recognition dialog box.
Setup external notification settings	Allows users to edit the Email Notifications dialog box.
Setup rule engine settings	Allows users to edit the Rules dialog box.
View site logs	Allows users to view Site Logs.
Connect and disconnect devices	Allows users to connect and disconnect cameras and other devices to servers.
View Site Health	Allows users to see Site Health details.
Setup servers	Allows users to configure servers.
Manage server	Allows users to edit the server name.
Setup schedule settings	Allows users to edit the camera Recording Schedule.
Setup recording and bandwidth settings	Allows users to edit the camera Recording and Bandwidth settings.
Setup Storage Management	Allows users to set up Scheduled Archive.
Backup settings	Allows users to back up server settings.
Setup server analytics	Allow users to configure analytics on supported servers.

Video Analytics Event Descriptions

The following table shows the Activity: options that can be used when configuring video analytics events. These triggers are based on the activity of detected classified objects.

NOTE: All events are reset when their duration reaches the specified Timeout: period.

For more information, see *Adding Video Analytics Events* on page 92.

Activity:	Description	Advanced Options
Objects in area	The event is triggered when the selected number of objects are present in the region of interest (ROI). The object can appear from within the ROI or enter from outside. Only one event is activated when the specified number of classified objects are detected in the area. Additional ROI in the area do not trigger additional events.	• **Number of Objects:** enter the maximum number of objects that can be in the ROI before the event is triggered. The default number is 1. • **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the

Activity:	Description	Advanced Options
		system.
Object loitering	The event is triggered for each object that stays within the ROI for an extended amount of time. The event is reset when the object leaves the ROI.	• **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Objects crossing beam	The event is triggered when the specified Number of Objects: have crossed the directional beam placed over the camera's field of view. The beam can be unidirectional or bidirectional. If the number of objects is exceeded, a new event is not triggered until the event timesout.	• **Number of Objects:** if the specified number of objects chosen is 1, then the video analytic event is triggered as soon as 1 object crosses the beam. If the specified number of objects is 2 or more, then the video analytic event is triggered when the specified number of objects cross the beam. The objects must be travelling in the direction set by the user, during the chosen time threshold. • **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Object appears or enters area	The event is triggered once for each classified object in the ROI. The classified object can appear from within the ROI or enter from outside the ROI. This video analytic event causes many alarms. For example, if 20 objects are detected within the ROI, 20 rules/alarms are triggered– one for each object.	• **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Object not present in area	The event is triggered when no objects are present in the ROI.	• **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Objects enter area	The event is triggered when the specified number of classified objects are detected in the field of view (FoV) then subsequently enters the ROI. The ROI must be less than the camera FoV, so that there is time to detect the object before it enters the ROI.	• **Number of Objects:** if the specified number of objects chosen is 1, then the video analytic event is triggered as soon as 1 object enters the area. If the specified number of objects is 2 or more, then the video analytic event is triggered when the

Activity:	Description	Advanced Options
	Only one event is activated when the specified number of classified objects are detected within the configured time threshold. Additional ROI do not trigger additional events.	specified number of objects enters the area. The objects must enter the area during the chosen time threshold. • **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Objects leave area	The opposite of Objects enter area. The event is triggered when the specified number of classified objects is detected inside the ROI then subsequently exits the ROI. The ROI must be less than the FoV of the camera.	• **Number of Objects:** if the specified number of objects chosen is 1, then the video analytic event is triggered as soon as 1 object exits the area. If the specified number of objects is 2 or more, then the video analytic event is triggered when the specified number of objects exits the area. The objects must enter the area during the chosen time threshold • **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Object stops in area	The event is triggered if a classified object is detected moving within the ROI then stops moving for the specified time. One event is activated for each classified object that stops. **NOTE:** An object can be tracked for up to 15 minutes.	• **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system.
Direction violated	The event is triggered for each object that moves within 22 degres of the prohibited direction. One event is activated for each classified object that moves in the prohibited direction.	• **Timeout:** enter the maximum duration of the event. After this time, if the event is still active, a new event is triggered in the system. • **Prohibited Direction:** move the arrow in the circle to define the direction that objects should not be traveling.

Rule Event and Action Descriptions

The following tables describe the trigger events, actions, and conditions that are available when you set up a rule. For more information about setting up a rule, see *Adding a Rule* on page 53 or *Adding a Rule for an ACM Appliance Event* on page 36.

Focus of Attention is a beta feature. For information on how to enable it and provide feedback, contact **producteval@avigilon.com**.

Rule Events

Rule events are the events that trigger a rule.

Server Events

Event	Description
Server application starting up	Server software starts up.
Server application shutting down	Server software shuts down.
Server application terminated unexpectedly	Server software shuts down unexpectedly.
Server application low on resources	Server software is low on memory or storage.
Server application installation error	Server software was installed incorrectly.
License expires soon	Server software license expires soon.
License expired	Server software license has expired.
Database error	Server database has generated an error.
Data initialization error	Server database has generated an error during initialization.
Data volume failed	Server data volume has failed.
Data volume recovered	Server data volume was recovered.
Data volume size reduced	Server data volume size was reduced.
Data write error	Server generated an error while writing data.
Data upgrade started	Server data upgrade has started.
Data upgrade completed	Server data upgrade has completed.
Data upgrade failed	Server data upgrade has failed.
Data recovery started	Server data recovery has started.
Data recovery completed	Server data recovery has completed.
Data recovery failed	Server data recovery has failed.
Bookmark save failed	A bookmark failed to save.

Event	Description
Network connection found	Server network connection was found.
Network connection lost	Server network connection was lost.
Email send error	An error was generated while sending an email notification.
Server hardware event	A server hardware error has occurred.
Archiving started	Server backup has started.
Archiving completed	Server backup has completed.
Archiving interrupted	Server backup has failed.
Server connection lost	Server connection to the site was lost.
Analytics server queue full	Video analytics service is unable to process all the objects detected by the system. This typically occurs if the system detects a large number of objects in a short period of time.
Analytics server connection lost	Server is unable to communicate with the video analytics service to perform Avigilon Appearance Search queries.
LPR Start/Stop	The LPR service has stopped or restarted.

Device Events

Event	Description
Connection created	A camera or device has connected to a server.
Connection removed	A camera or device has disconnected from a server.
Connection created to standby server	A camera or device has connected to a standby server.
Connection removed from standby server	A camera or device has disconnected from a standby server.
Connection failed	A camera or device connection has failed.
Device failed	A camera or device connection has failed for more than 5 minutes.
Connection restored	A camera or device connection has been restored.
Network packet loss unacceptable	A camera or device network packet loss is unacceptable.
Network packet loss acceptable	A camera or device network packet loss is acceptable.
Motion detection started	Motion detection has started on a camera.
Motion detection ended	Motion detection has ended on a camera.

Event	Description
Video analytics event started	A video analytics event has started.
Video analytics event ended	A video analytics event has ended.
Tampering detected	A video analytics camera or device has detected an unexpected change in the scene.
Recording started	A camera or device recording has started.
Recording ended	A camera or device recording has ended.
Recording interrupted	A camera or device recording was interrupted.
Recording resumed	A camera or device recording has resumed.
Digital input activated	A camera or device digital input was activated.
Digital input deactivated	A camera or device digital input was deactivated.
Firmware upgrade started	A camera or device firmware upgrade has started.
Firmware upgrade completed	A camera or device firmware upgrade has been completed.
Firmware upgrade failed	A camera or device firmware upgrade has failed.
Obsolete firmware detected	A camera or device is detected to be running obsolete firmware. The system is unable to perform an automatic upgrade.
User-defined event started	Customized third-party camera ONVIF event has started.
User-defined event ended	Customized third-party camera ONVIF event has ended.
Presence detected	A presence has been detected in range of an Avigilon Presence Detector sensor.
Presence dwell time exceeded	A continuous presence has been detected in range of an Avigilon Presence Detector sensor for longer than the configured dwell time.
Presence dwell ended	The presence detected for longer than the configured dwell time by an Avigilon Presence Detector sensor has ended.
Presence ended	The presence detected is no longer in range of the Avigilon Presence Detector sensor. If the presence was longer than the configured dwell time, a Presence dwell ended event will also be triggered.

User Events

Event	Description
User login	A user has logged in.
User logout	A user has logged out.
Server setting changed	A user has changed the server settings.
Site setting changed	A user has changed the site settings.
Device setting changed	A user has changed the camera or device settings.
Device connected	A user has connected a camera or device to a server.
Device disconnected	A user has disconnected a camera or device from a server.
Digital output triggered	A user has manually triggered a digital output.
Bookmark added	A user has added a bookmark.
Bookmark updated	A user has updated a bookmark.
Bookmark deleted	A user has deleted a bookmark.
PTZ moved	A user has moved a PTZ camera.
PTZ idle	A user has left a PTZ camera idle.
Export performed	A user has performed a video export.
Speaker activated	A user is broadcasting audio through camera or device speakers.
Speaker deactivated	A user has stopped broadcasting audio.
Virtual matrix monitor opened	A user has opened a Virtual Matrix monitor in the View.
Map added	A user has added a new map.
Map updated	A user has updated a map.
Map deleted	A user has deleted a map.
View added	A user has added a saved View.
View updated	A user has updated a saved View.
View deleted	A user has deleted a saved View.
Web Page added	A user has added a new web page.
Web Page updated	A user has updated a web page.
Web Page deleted	A user has deleted a web page.

Event	Description
Site View updated	A user has updated the way cameras are organized in the System Explorer.
Custom keyboard command triggered	A user has triggered a custom keyboard command.

Alarm Events

Event	Description
Alarm acknowledged	An alarm has been acknowledged.
Alarm auto acknowledged	An alarm has been acknowledged automatically.
Alarm triggered	An alarm has been triggered.
Alarm assigned	An alarm has been assigned to a user.
Alarm unassigned	An alarm has been unassigned from a user.
Alarm purged	An alarm has been purged.

POS Transaction Events

Event	Description
POS transaction started	A POS transaction has started.
POS transaction ended	A POS transaction has ended.
POS transaction exception	A POS transaction exception has occurred.

License Plate Recognition Events

Event	Description
License plate detection started	License plate detection has started.
License plate detection ended	License plate detection has ended.
License plate watch list match	A license plate on a LPR Watch List has been detected.

Access Control Events

Event	Description
Door access denied	Possible reasons: • Unknown card • Expired card attempt • Valid card at an unauthorized reader • Deactivated card attempt

Event	Description
	• Invalid card schedule • Invalid PIN code has been entered • Invalid facility code • Valid card with an incorrect issue level • Antipassback error • Deny count exceeded • Invalid forward card read • Invalid reverse card read • Attempt to open locked door • Two card control violation - second card not presented • Access denied - occupancy limit reached • Access denied - area disabled • Invalid card - before activation • Invalid facility code ext • Invalid card format • Invalid PIN only request • Door mode does not allow card • Door mode does not allow unique PIN
Door access granted	Possible reasons: • Local grant • Opened unlocked door • Local grant - APB error - not used • Local Grant - APB error - used • Facility code grant - not used • Local grant - not used • Facility code grant • Local grant use pending
Door closed	A door closed.
Door forced	A door was forced.
Forced door closed	A forced door was closed.
Door held open	A door was held open.
Held door closed	A held-open door was closed.
Door opened	A door opened.
Door duress	Possible reasons:

Event	Description
	• Duress detected - access denied • Local grant - duress - Not Used • Local Grant - Duress - Used
Door request to exit	Possible reasons: • Request to exit Pressed, Non-verified • Request to exit Pressed, Door not used • Request to exit Pressed, Door used • Request to exit Pressed, Use Pending • Host Request to exit, Non-verified • Host Request to exit, Door not used • Host Request to exit, Door used • Host Request to exit, Use Pending
Input activated	An installed ACM panel or subpanel input was activated.
Input deactivated	An installed ACM panel or subpanel input was deactivated.
Input fault detected	An error was detected for an installed ACM panel or subpanel input. Tampering may have occurred.
Input fault cleared	An error detected for an installed ACM panel or subpanel input has ended.

Rule Actions

Rule actions are the response to a rule event.

User Notification Actions

Action	Description
Display on-screen message	An on-screen message is displayed about the rule event.
Send email	An email notification is sent about the rule event to the selected recipient(s).
Send notification to Central Monitoring Station	A notification is sent to the central monitoring station.
Play a sound	A notification sound is played within the Client when the rule event occurs.

Monitoring Actions

Action	Description
Start live streaming	The linked live video stream is displayed when the rule event occurs.
Video intercom call	The linked live video intercom call opens in a new image panel with a ring tone.
Create Bookmark	The recorded video of the rule event is bookmarked.
Open a saved view	The selected saved View is automatically displayed.
Start live streaming on a virtual matrix monitor	The live stream from the selected camera is automatically displayed on the selected Virtual Matrix monitor.
Open a map on a virtual matrix monitor	The selected map is automatically displayed on the selected Virtual Matrix monitor.
Open a web page on a virtual matrix monitor	The selected web page is automatically displayed on the selected Virtual Matrix monitor.

Device Actions

Action	Description
Reboot device	The camera or device reboots when the rule event occurs.
Pause device	The camera or device is put on standby when the rule event occurs. Streaming and recording are paused.
Resume device	The standby camera or device resumes streaming and recording activity when the rule event occurs.
Activate digital output	A digital output is triggered when the rule event occurs.
Deactivate digital output	A digital output is deactivated when the rule event occurs.

PTZ Actions

Action	Description
Go to Preset	The selected PTZ camera moves to the selected preset position when the rule event occurs.
Go to Home Preset	The selected PTZ camera moves to the home position when the rule event occurs.
Run a Pattern	The selected PTZ camera runs a selected pattern when the rule event occurs.
Set Auxiliary	The selected PTZ camera starts the selected auxiliary command when the rule event occurs.
Clear Auxiliary	The selected PTZ camera ends the selected auxiliary command when the rule event occurs.

Alarm Actions

Alarm	Description
Trigger an alarm	An alarm is triggered when the rule event occurs.
Acknowledge an alarm	An alarm is acknowledged when the rule event occurs.

Rule Conditions

Rule conditions are the scenarios that must be met before the rule is triggered.

Device Events

Condition	Description
Digital input is active	The rule is triggered if the connected digital input is active while the selected rule event occurs.
Digital input is not active	The rule is triggered if the connected digital input is inactive while the selected rule event occurs.

Alarm Trigger Source Descriptions

The following table shows the Alarm Trigger Source: options that are available when you set up an alarm. For more information about setting up an alarm, see *Adding a New Alarm* on page 50.

Alarm Trigger Source:	Description
Motion Detection	The alarm is triggered when motion is detected by the selected cameras.
Video Analytics Event	The alarm is triggered when a video analytics event is detected by the selected cameras.
Digital Input Activation	The alarm is triggered when the selected digital inputs are activated.
License Plate Watch list Match	The alarm is triggered when a license plate on the Watch List is detected.
POS Transaction Exception	The alarm is triggered when a POS transaction exception has occurred.
Device Error	The alarm is triggered when a camera error occurs. Possible errors include: • Device connection lost for less than 5 minutes • Device connection lost for more than 5 minutes • Firmware upgrade failed • Recording interrupted • Tampering • Alarm triggered
System Error	The alarm is triggered when a system error occurs. Possible errors include: • Storage initialization error • Storage write queue full

Alarm Trigger Source:	Description
	• Storage writes blocked • Storage writes failed • Storage low disk space • Storage recovery ended • Storage upgrade data ended • Storage volume failed • System hardware error • System server connection lost • Application license expiry • Application bad shutdown • Database environment recovered • System email error • LPR process unexpected shutdown
External Software Event	The alarm is triggered by third party integration software.

Updating the ACC Client Software

Avigilon Control Center Client software updates are typically included with the Avigilon Control Center Server update packages. When you first open the Client software, you may be prompted to update with a popup message similar to the following :

A new version of Avigilon Control Center Client is available for download from server 123.

Choose one of the following options:

- Click **Update** to allow the Client software to update. The software update is automatically downloaded and a dialog box displays the download progress.

  When the update has finished downloading, click **Update Avigilon Control Center Client**. When the installation wizard appears, follow the prompts to complete the update.

- Click **Do Not Update** to continue working with the Client software without updating. The Client software will not be updated, and you can continue working with the software as before.

The Client software can also be downloaded from the Software Updates & Downloads page of the Avigilon website: avigilon.com/support-and-downloads/.

Supported License Plates

The following license plates are supported by LPR6 and LPR5 licenses. The options available will depend on the type of license. To configure the license plate format for your server, see *Setting Up License Plate Recognition* on page 69.

If the license plate format you need is not listed, you can email Avigilon Technical Support at **support@avigilon.com** and request an LPR Font Template.

License Plates Supported by LPR6

- Argentina
- Australia
- Brazil
- China
- Europe[1]
- India
- Indonesia
- Japan
- Middle East[2]
- New Zealand
- North America[3]
- Russia
- Saudi Arabia
- South Africa
- South Korea
- Thailand
- United Arab Emirates
- United Kingdom

[1] Includes Kazakhstan and Turkey. May experience lower accuracy for license plates from Armenia, Georgia, and Kosovo.
[2] Includes Bahrain, Egypt, Iraq, Jordan, Kuwait, Oman, and Qatar.
[3] Includes Canada, Mexico, and USA.

License Plates Supported by LPR5

Africa

- Morocco
- South Africa

Asia-Pacific

- Australia
  - Victoria
  - Western Australia
- China
- Korea
- New Zealand
- Pakistan
- Russia
- RU-UA-EE-BY-LT-LV
- Singapore
- South Korea
- Thailand

Europe

- Belarus
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Estonia
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia

- Netherlands
- Poland
- Portugal
- Romania
- Spain
- Switzerland
- Turkey
- Ukraine
- United Kingdom
- BE-DE-NL
- BG-DE
- BG-DE-RO
- HRV-DEU-HUN-ITA
- UK-IE
- UK-FR

Middle East

- Bahrain
- Dubai
- Israel
- Jordan
- Kuwait
- Lebanon
- Qatar
- Saudi Arabia

North America

- Canada
    - British Columbia
    - New Brunswick
    - Ontario
    - Quebec
- Mexico
- USA
    - Alabama
    - Alaska
    - Arizona
    - California
    - Connecticut
    - Florida
    - Georgia
    - Illinois
    - Indiana
    - Kansas
    - Louisiana
    - Massachusetts
    - Michigan
    - Minnesota
    - Mississippi
    - Missouri
    - Montana
    - New Hampshire
    - New Jersey
    - New Mexico
    - New York
    - North Carolina
    - North Dakota
    - Ohio
    - Pennsylvania
    - South Carolina
    - Texas
    - Utah
    - Virginia
    - Washington
    - Wisconsin
    - Wyoming
    - AZ-CA
    - CT-NY-NJ
    - MI-IN-OH
    - NY-VA-MD
    - MO-KS
    - MT-WY
    - NC-VA-MD
    - NY-NJ

South America

- Argentina
- Argentina-Chile
- Brazil
- Chile
- Colombia

Reporting Bugs

If an error occurs in the ACC software, you can contact Avigilon Technical Support at **support@avigilon.com** or +1.888.281.5182 option 1.

To help diagnose your problem, the Avigilon Technical Support team may ask you to provide a System Bug Report. The System Bug Report is a zip file generated by the Avigilon Control Center Client software that contains the system log and error reports for each of the servers that you can access.

To generate a System Bug Report:

1. Select > **System Bug Report...**.
2. When the Download System Bug Report dialog box appears, click **Download**.
3. In the Save As dialog box, name the file and click **Save**.
4. Once the System Bug Report has downloaded successfully, click **Close**.

Keyboard Commands

Use any of the keyboard commands below to help you navigate the Avigilon Control Center Client software.

The Key Combination column shows the commands used on a standard keyboard, while the Keypad Combination column shows the commands used on an Avigilon USB Professional Joystick Keyboard.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

Image Panel & Camera Commands

Command	Key Combination	Keypad Combination (Image Panel buttons)
Select an image panel Image panel # is displayed after pressing the first key.	* + *<image panel #>* + Enter	SELECT + *<image panel #>* + ENTER
Display a specific camera in the View The camera's ***Logical ID*** is required.	/ + *<logical ID>* + Enter	CAMERA + *<logical ID>* + ENTER

Command	Key Combination	Keypad Combination (Image Panel buttons)
Display the next camera by camera's ***Logical ID*** in the View	/ +	
Display the previous camera by camera's ***Logical ID*** in the View	/ -	
Select the next image panel	Tab	
Select the previous image panel	Shift + Tab	
Clear image panel selection	* + 0 + Enter	
Remove camera from the selected image panel	Backspace	
Maximize/Restore the selected image panel	Ctrl + E	
Replay 30 seconds	Ctrl + ,	
Replay 60 seconds	Ctrl + .	
Replay 90 seconds	Ctrl + /	
Add a bookmark for selected camera **NOTE:** For recorded video only.	Ctrl + B	
Start/Stop manual recording for the selected camera	R	
Activate/Mute audio for the selected camera In a Video Intercom panel, answer a call and activate bi-directional audio	A	
Broadcast audio	S Hold to speak. Release to stop broadcasting.	 Hold to speak. Release to stop

Command	Key Combination	Keypad Combination (Image Panel buttons)
	In a Video Intercom panel, press to mute microphone. Press again to unmute.	broadcasting.
In a Video Intercom panel, ignore or hang up a call	X	
Take a snapshot of the selected image panel	F4	
Display linked POS transaction source/camera	Ctrl + I	
Enable digital output	K	
Opens the grant door access menu	U	
Acknowledge the alarm currently displayed in an armed image panel	L	
Trigger custom keyboard command	Ctrl + K	

View Tab Commands

Command	Key Combination	Keypad Combination (View buttons)
Select the next View	Ctrl + Tab	
Select the previous View	Ctrl + Shift + Tab	
Jump to View #_	Ctrl + 1 to 9	
Start/Stop cycle Views	Ctrl + Y	
Open a new View	Ctrl + T	
Close current View	Ctrl + W	
Open a new window	Ctrl + N	
Switch current View to display live video	Ctrl + L	

Command	Key Combination	Keypad Combination (View buttons)
Switch current View to display recorded video	Ctrl + P	
Remove all cameras from the current View	Ctrl + Backspace	
Full screen a View/End full screen	F11	
Open a saved View The saved View's ***logical ID*** is required.	Ctrl + G + *<logical ID>*	OPEN 3 + *<logical ID>* + ENTER
Open a Virtual Matrix monitor The Virtual Matrix monitor's ***logical ID*** is required.	Ctrl + G + *<logical ID>*	OPEN 3 + *<logical ID>* + ENTER

View Layout Commands

NOTE: Customized View layouts are linked to their position in the Layouts list. For example, if your custom layout is placed at the top of the Layouts list, you can use the keyboard command for layout 1 to select the custom layout.

Command	Key Combination	Keypad Combination (View buttons)
Change to layout 1	Alt + 1	LAYOUT 4 + PREV 1
Change to layout 2	Alt + 2	LAYOUT 4 + NEXT 2
Change to layout 3	Alt + 3	LAYOUT 4 + OPEN 3
Change to layout 4	Alt + 4	LAYOUT 4 + LAYOUT 4
Change to layout 5	Alt + 5	LAYOUT 4 + 5
Change to layout 6	Alt + 6	LAYOUT 4 + CLOSE 6
Change to layout 7	Alt + 7	LAYOUT 4 + 7
Change to layout 8	Alt + 8	LAYOUT 4 + 8
Change to layout 9	Alt + 9	LAYOUT 4 + 9
Change to layout 10	Alt + 0	LAYOUT 4 + 0

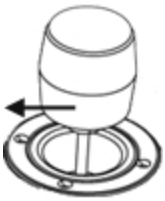
Command	Key Combination	Keypad Combination (View buttons)
Change to next layout	Alt +]	
Change to previous layout	Alt + [	

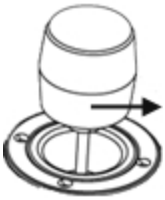
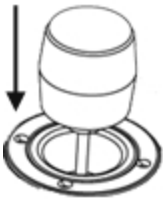
Playback Commands

Command	Key Combination	Keypad Combination (Timeline buttons)
Play/Pause video playback	Spacebar	
Increase playback speed	Page Up	
Decrease playback speed	Page Down	
Step to next frame	Shift + →	
Step to previous frame	Shift + ←	
Go to next event	Alt + →	
Go to previous event	Alt + ←	
Go forward one second	Ctrl + →	
Go forward five seconds	Ctrl + Shift + →	
Go backward one second	Ctrl + ←	
Go backward five seconds	Ctrl + Shift + ←	
Zoom in on the Timeline	Ctrl + Alt + +	
Zoom out on the Timeline	Ctrl + Alt + –	
Scroll forward on the Timeline	Ctrl + Alt + →	
Scroll backward on the Timeline	Ctrl + Alt + ←	

Command	Key Combination	Keypad Combination (Timeline buttons)
Move the Timeline marker forward		
Move the Timeline marker backward		
Go to the start of the Timeline	Ctrl + Alt + Home	
Go to the end of the Timeline	Ctrl + Alt + End	
Center the Timeline on the time marker	Ctrl + C	

PTZ Commands (Digital and Mechanical)

Command	Key Combination	Keypad Combination (PTZ buttons)
Toggle PTZ controls	Ctrl + D	
Zoom in	+	
Zoom out	–	
Pan left	←	

Command	Key Combination	Keypad Combination (PTZ buttons)
Pan right	→	
Tilt up	↑	
Tilt down	↓	
Open iris	Home	
Close iris	End	
Focus near	Insert	
Focus far	Delete	
PTZ menu left	←	
PTZ menu right	→	
PTZ menu up	↑	
PTZ menu down	↓	
Activate preset	Q + *<Preset #>*	PRESET + *<Preset #>* + ENTER
Run pattern		PATTERN + *<Pattern #>* + ENTER
Start auxiliary	W + *<Aux #>*	START + *<Aux #>* + ENTER

Command	Key Combination	Keypad Combination (PTZ buttons)
Stop auxiliary	E + <*Aux #*>	 + <*Aux #*> + ENTER