Avigilon Control Center™ Client User Guide

Version 7.14

© 2006 - 2021, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON CONTROL CENTER, ACC, ACCESS CONTROL MANAGER, ACM, AVIGILON CLOUD SERVICES, AVIGILON PRESENCE DETECTOR, APD, HIGH DEFINITION STREAM MANAGEMENT, HDSM, HDSM SmartCodec, and AVIGILON APPEARANCE SEARCH are trademarks of Avigilon Corporation. Celeron, Intel and Intel Core are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. App Store is a trademark of Apple Inc., registered in the U.S. 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. Covered by one or more claims of the patents listed at **patentlist.hevcadvance.com**.

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-CLIENT7-G

Revision: 6 - EN

20211103

Table of Contents

What Is the Avigilon Control Center Client Software? 1
System Requirements 1
Avigilon Certified Solution 1
ACC™ Client Software Requirements 1
Getting Help 2
Updating the Help Files 2
For More Information 3
Getting Started 4
Initial System Setup 4
Starting Up and Shutting Down 4
Discovering Sites 4
Sharing Discovered Sites 5
Disabling Automatic Site Discovery 5
Setting the Connection Type 6
Logging In and Out 6
Logging In 6
Logging Out 6
Changing Your Password 6
Activating an Initial Trial License 7
Navigating the Software 8
Application Window Features 8
System Explorer Icons 9
System Management 10
Licensing the Site 10
Activating a License 10
Online Activation 10
Offline Activation 10
Changing Site Edition 11
Deactivating a License 12
Reactivating a License 13
Refreshing a License 14
Sites 14
Naming a Site or Server 15
Configuring FIPS Compliance 15

Server Communication 15
Client Communication 15
Avigilon Certificates 16
Site Settings 16
Client Settings 16
Trusted Device Certificates 16
Encrypting Video 17
Encrypting Video from All Sites 17
Encrypting Video from Specific Sites 17
Multiple Server Sites 18
Connecting Servers to a Site 18
Disconnecting Servers from a Site 19
Site Health 20
Exporting a Report 20
Filtering Site Information 21
Viewing Site Logs 27
Exporting Site Log Results 28
Event Details 28
Site Log Descriptions 28
Server Events 28
Device Events 30
User Events 31
Access Events 33
Site Log Examples 34
User Group Added 34
Access Granted to a Device 34
User Accessed Footage from Multiple Cameras 35
User Group Privileges Update 35
User Information Update 36
User Performed Appearance Search 37
User Login Failed 37
Upgrading Your Site Remotely 37
Removing an Upgrade Installer 39
Backing Up Site Settings 39
Restoring Site Settings 40
Servers and Storage 41
Identity Data Retention 41

Recording and Bandwidth 42
Video Retention 42
Data Aging 42
Configuring Data Aging 43
Continuous Archive 44
Enabling Storage Management 44
Enabling Continuous Archive 45
Resetting Continuous Archive 46
Manual Recording Setup 46
Setting Up a Weekly Recording Schedule 46
Recording Schedule Templates 47
Adding a Template 47
Editing and Deleting a Template 48
Failover Connections 48
Editing Failover Connections 49
Failover Examples 49
Recovering Video from Profile G Cameras 50
Server Management 51
Devices 51
Discovering a Device 51
Connecting a Device 53
Enabling FIPS Cryptography for Avigilon Devices 54
Device Network Settings 55
Disconnecting a Device 56
Replacing a Device 56
Rebooting a Device 58
Upgrading Camera Firmware 58
Changing from LAN to WAN 58
Device Configuration 59
Setting a Device's Identity 59
Changing the Camera Operating Priority 59
Compression and Image Rate 60
Manually Adjusting Video Streams for Recording 61
Enabling HDSM SmartCodec™ Technology 63
Enabling Idle Scene Mode 64
Image and Display Settings 64
Image Dimensions 67

Privacy Zones 68
Adding a Privacy Zone 68
Editing Privacy Zones 68
Configuring PTZ 68
Configuring Digital Inputs 69
Configuring Digital Outputs 70
Configuring the Device Microphone 70
Configuring the Device Speakers 71
Video Intercom 72
Adding Rule to Answer Calls 72
Recording Video during a Call 73
Avigilon Presence Detector™ Sensors 73
Analytics 74
Enabling Analytics 74
Configuring Data Retention 75
Disabling Analytics 75
Configuring Data Retention 75
Configuring Camera Analytics 75
Analytic Settings 76
Configuring Skin Temperature Thresholds 77
Toggling Degrees Celsius and Fahrenheit 78
Unusual Motion and Unusual Activity 78
Video Analytics Mode 79
Self-Learning 79
Self Learning Progress Bar 79
Resetting the Learning Progress 80
Teach By Example 81
Assigning Teach Markers 81
Editing and Removing Teach Markers 81
Applying Teach Markers 82
Teach Marker Status 82
Disabling Tampering Detection 82
Configuring Rialto Video Analytics Appliances 83
Users, Groups, and Permissions 83
Best Practices for Large Organizations 84
Best Practices 84
Importing Active Directory Users 85

Enabling the Active Directory 85
Nested Groups 86
Importing Groups 86
Importing Users 87
Adding a User 87
Editing and Deleting a User 88
Adding Groups 89
Editing and Deleting a Group 90
Emergency Privilege Override 90
Group Privileges 91
Resetting a Password 94
Managing User Connections 95
Corporate Hierarchy 95
Setting Up a Corporate Hierarchy 95
Ranks 96
Unranked Groups 97
Deleted Ranks 97
Ranked Site Families 97
Site Families 97
Connecting Site Families 97
Disconnecting Site Families 98
Restricting Login to Parent Sites 98
Avigilon Cloud Services 98
Connecting to the Cloud 99
Before Connecting Your ACC Site 99
Registering Your Organization 99
Adding a Site to Your Organization 100
Adding Users to Avigilon Cloud Services 100
Signing In to Avigilon Cloud Services 101
Giving Users Additional Privileges 101
* Avigilon Cloud Services Regions 101
Disconnecting from the Cloud 101
ACM™ Appliances 101
Before Adding an ACM Appliance 102
Connecting an ACM Appliance to an ACC Site 104
Importing ACM Roles 104
Linking Doors to Cameras 105

Adding a Link 106
Editing and Deleting a Link 106
Adding Rules for ACM Appliance Events 106
Customizing ACC 108
Application Settings 108
Automatically Logging In to Sites 108
Changing the Theme 108
Changing the Language 108
Saving the Layout 108
Setting the Maximum Incoming Bandwidth 109
Displaying System Messages 109
Display Settings 109
Editing the System Explorer 109
Changing the Video Display Settings 110
Video Overlays 111
Configuring Standby Mode 112
Changing Day/Night Mode 112
Using Digital Defog 113
Dewarping Fisheye Displays 113
Zooming and Focusing the Camera Lens 114
Measuring Pixels in the Field of View 115
Configuring Infrared LEDs 116
Displaying Video Analytics Activity 116
Injecting Text and Overlaying it on Video 117
Searching the Injected Text 118
Events and Rules 118
Analytic Events 118
Adding an Analytic Event 118
Editing and Deleting Video Analytics Events 120
Analytic Event Descriptions 120
Activities In Regions of Interest 120
Temperature Detection Activities 122
Motion Detection Events 123
Setting Up Classified Object Motion Detection 123
Setting Up Pixel Motion Detection 124
Adding a Rule 126
Scheduling Rules 126

Editing and Deleting Rules 127
Rule Events and Actions 128
Rule Events 128
Rule Actions 135
Rule Conditions 136
Notifications and Alarms 137
Alarms 137
Adding an Alarm 137
Editing and Deleting Alarms 138
Adding an Analytics Alarm 138
Email Notifications 139
Configuring the Email Server 139
Adding Recipients 139
Editing Email Notifications 140
Email Notification Triggers 140
Central Station Monitoring 141
Face Recognition 142
Face Watch Lists 142
Editing a Watch List 142
Adding a Watch List 142
Deleting a Watch List 143
Configuring Data Retention 143
Exporting a Watch List to Another Site 143
Adding Watch List Profiles 143
Adding a Profile from Recorded Video 144
Profile Status and Quality 144
Editing a Profile 145
Changing Profile Expiry 145
Moving a Profile 145
Deleting a Profile 145
Searching from a Face Watch List Profile 146
License Plate Recognition 146
Setting Up License Plate Recognition 146
Configuring LPR Data Retention 147
Displaying the LPR Overlay 147
LPR Watch Lists 147
Adding a Watch List 147

Exporting a Watch List 148
Editing or Deleting a Watch List 148
Supported License Plates 148
POS Transactions 149
Adding a POS Transaction Source 149
Adding Data Formats 150
Adding Transaction Exceptions 150
Editing Transaction Sources 151
Joystick Settings 151
Configuring an Avigilon USB Professional Joystick Keyboard for Left-Hand Use 151
Configuring a Standard USB Joystick 151
Virtual Matrix 152
Adding a Virtual Matrix 152
Adding Sites 152
Changing Primary Sites 153
Deleting a Virtual Matrix 153
Maps 153
Adding a Map 153
Adding Cameras to a Map 153
Editing and Deleting Maps 154
Web Pages 154
Adding a Web Page 154
Editing and Deleting Web Pages 155
Using ACC 156
Controlling Live and Recorded Video 156
Adding and Removing Cameras 156
Requesting Dual Authorization 157
Manually Recording Video 157
Playing Recorded Video with the Timeline 157
Synchronizing Recorded Video Playback 159
Enabling Synchronized Playback 160
Disabling Synchronized Playback 160
Using Instant Replay 160
Viewing Unusual Events 161
Zooming and Panning 161
Controlling PTZ Cameras 162
PTZ Presets, Patterns, and Tours 164

Accessing the PTZ Controls Pane 164
Adding a PTZ Preset 164
Adding a PTZ Pattern 164
Adding a PTZ Tour 164
Activating a Preset, Pattern, or Tour 165
Using the H4 IR PTZ Wiper 165
Using the H5 Hardened PTZ Illuminator 166
Live Monitoring 166
Focus of Attention 166
The Overview 167
Zooming and Panning the Overview 167
Changing Focus of Attention Settings 168
Monitoring Events 168
Managing Alarms 168
Reviewing Alarms 168
Acknowledging Alarms 169
Arming Image Panels 169
Reviewing Alarms 169
Identity Verification 170
Monitoring License Plates 170
Enabling License Plate Overlays 170
Reviewing LPR Watch List Matches 171
Monitoring POS Transactions 171
Displaying Cameras Linked to POS Sources 171
Browsing the ACM Appliance in the ACC Client 171
Using a Map 172
Opening a Web Page 173
Paused Video 173
Using Linked Devices 173
Granting Door Access 174
Using Video Intercom 174
Using Audio 174
Configuring Two-Way Audio 174
Listening to Audio 175
Broadcasting Audio in a View 175
Triggering Digital Outputs 175
Managing Views 175

Cycling Cameras 175
Cycling Cameras across Sites 176
Adding and Removing Views 176
Cycling Views 176
View Layouts 176
Saving Views 177
Saving a View 177
Editing a Saved View 177
Renaming a View 177
Deleting a Saved View 177
Shared Views 178
Sharing a View 178
Leaving a Shared View 178
Searching 178
Avigilon Appearance Search™ Feature 179
Searching by Description 179
Searching Recorded Video 179
Searching by Uploaded Photo 180
Avigilon Appearance Search Results 180
Refining Results 180
Saving Results 181
Identity Search 181
Identity Search Results 182
Refining Results 182
Saving Results 182
Searching Alarms 182
Searching Events 182
Searching Motion 183
Classified Object Motion 183
Pixel Motion 184
Searching License Plates 184
Searching Text Source Transactions 184
Searching Thumbnails 185
Searching by Drawing Box Around Object of Interest 185
Reviewing Search Results 186
Reviewing Results 186
Saving Results 186

Exporting 186
Adding Content to Export 186
Combining Export Files 187
Exporting Video History 187
Exporting Files 188
Export Options 188
Bookmarking Recorded Video 189
Adding a Bookmark 189
Managing Bookmarks 190
Archiving Recorded Video 190
Enabling Emergency Privilege Override 191
Additional Support 192
Reporting Issues 192
Anonymous Data Collection 192
Basic ACC System Health Check 192
Keyboard Commands 194
Image Panel and Camera Commands 194
View Tab Commands 196
View Layout Commands 197
Playback Commands 197
PTZ Commands (Digital and Mechanical) 199
Joystick Controls 200

What Is the Avigilon Control Center Client Software?

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

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

The ACC Client software can run on the same computer as the ACC 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 ACC Client software depends on the site edition license. There are three editions available: Core, Standard and Enterprise. Visit the Avigilon website at **avigilon.com** for an overview of the features available in each edition.

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 8.1 (64-bit) or Windows 10 (64-bit) with Microsoft .NET 4.6.2	Windows 10 (64-bit) with Microsoft .NET 4.6.2
CPU	Intel® dual-core CPU (2.0 GHz)	8th Generation Intel Celeron® CPU or higher
System RAM	4 GB DDR3	8 GB DDR4
Video card	PCI Express®, DirectX 10.0 compliant with 256 MB RAM	NVIDIA® Quadro® P620
Network card	1 Gbps	1 Gbps

System Requirement	Minimum requirements	Recommended requirements
Hard disk space	500 MB free disk space	500 MB free disk space

* Run Windows Update before launching the ACC software.

Getting Help

If you want to learn more about a feature or how to accomplish a task, visit **help.avigilon.com/acc** or see our in-product help. You must be logged in to a site to view the help.

- In the top-right corner of the window, select > **Help**.

Updating the Help Files

> **Tip:** Access the latest help online at **help.avigilon.com/acc**.

The help files for the ACC Client software and Virtual Matrix software are stored with the ACC 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 **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

For additional product documentation and software and firmware upgrades, visit **support.avigilon.com**.

Technical Support

Contact Avigilon Technical Support at **support.avigilon.com/s/contactsupport**.

Getting Started

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

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 **avigilon.com/support/software/acc7**.

Starting Up and Shutting Down

You can open or close the ACC Client software at anytime without impacting video recording.

To open the ACC Client software:

- Double-click the desktop shortcut icon .
- In the Start menu, select **All Programs** or **All Apps** > **Avigilon** > **Avigilon Control Center Client**.

To close the ACC Client software:

1. In the top-right corner, click ✕.
2. Click **Yes**.

Discovering Sites

If your computer is on the same network (subnet) as a site, that site is automatically discovered and displayed in the System Explorer.

If your site is not listed, it is because the site is on a different subnet and must be manually 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.

> **Tip:** After you discover and log in to a parent site, all child sites are automatically discovered.

1. In the Site Login tab, click **Find Site**.
2. 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 ACC Admin Tool. For more information, see **The ACC 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 before trying again:

- Network settings are configured correctly.
- Your firewall is not blocking the application.
- The ACC Server software is running on the server you searched for.

Sharing Discovered Sites

Computer administrators can share discovered sites with all users on the same computer or workstation. However, the shared sites' Connection Type: will be the default value (WAN (Secured)) for each user.

Discovered sites are not shared with other computers or workstations on the network.

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Site Networking tab, click **Share Sites**.
3. In the following dialog box, click **Continue** to confirm.
4. If prompted, click **Yes** again to let the ACC software make changes to the computer.

   Discovered sites are now shared with all users on the computer.

   Note: Using an older version of the ACC Client software may result in issues with shared discovered sites. For best results, use the latest version.

Disabling Automatic Site Discovery

To improve the security of your ACC system, you can disable automatic site discovery on your ACC Clients. This will stop the unencrypted broadcasting of discovery traffic, and will require sites to be manually discovered. For more information on manually discovering sites, see *Discovering Sites* on the previous page.

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Security tab, select the **Disable automatic site discovery** checkbox.
3. Click **OK**.

Setting the Connection Type

Make sure that ports 51000-55000 UDP are open between the viewing stations and the ACC Servers. If they are closed, all live video will appear as black, however, you can see recorded videos. You need to set the Connection Type: to WAN (Secured).

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Site Networking tab, click on the selected ACC site.
3. Set the Connection Type: to **WAN (Secured)**.
4. Click **OK**.

If needed, perform this procedure on other viewing stations as well.

Logging In and Out

Logging In

When logging in to the site for the first time, the default credentials use `administrator` as the username without a password. You'll be asked to immediately enter a new password.

1. In the New Task menu, click **Site Login**.
2. Select your site from the list of connected sites.

   If you don't see your site, click **Find Site...** to manually search your network. For more information, see *Discovering Sites* on page 4.
3. Enter your credentials, or select **Use current Windows credentials** and click **Log In...**.

Tip:

- If Two-Factor Authentication is required, use a Time-based One-Time Password (TOTP) authenticator app like the Google Authenticator™ mobile app to log in.
- If you can't log in using your Windows credentials, your system may use Kerberos as a network authentication protocol. Contact your network administrator for help.

Logging Out

When you are finished using the ACC Client, log out.

1. In the top-right corner of the ACC Client, select > **Log Out**.
2. Click **Yes**.

Changing Your Password

If it's your first time logging in to a site or your password has expired, you'll need to change it.

If you have forgotten your password, contact your administrator to reset it. For more information, see *Resetting a Password* on page 94.

Important: If you forget the administrator password, resetting it requires assistance from Avigilon Technical Support and will impact every server in the site. Create at least one other administrator-level user as a backup.

1. Enter a new password and confirm your new password.

   The password must meet the minimum strength requirements, defined by how easy it is for an unauthorized user to guess.

   Tip: Try entering a series of words that is easy for you to remember but difficult for others to guess.

2. Click **OK**.

Activating an Initial Trial License

Activate an initial trial license to access the ACC software for 30 days, enable channel licenses for use after the trial has ended, or try out new features like face recognition or license plate recognition.

Tip: Finish organizing your multi-server site before activating a license to avoid reactivating the site license each time a new server is added.

1. In the New Task menu , click **Site Setup**.
2. Select your new site, then click .
3. Click **Request Trial License...**.
4. Select the preferred license edition, then click **Activate Now**.

Navigating the Software

After you log in, you can interact with devices across your site.

Application Window Features

	Area	Description
1	System Explorer	Displays all servers, devices, and views associated with your site. Use the search bar to find devices by name, location, Logical ID, IP address, or serial number.
2	View	Where you can monitor video and organize image panels. You can customize the number of image panels and cameras displayed.
3	Image panel	Displays live or recorded video. Access video controls by moving your mouse over the panel.
4	Toolbar	Provides quick access to tools that interact with video.
5	Tabs	Displays all views and tasks that are currently open. Click + to open a new View tab.
☰	New Task Menu	Access system settings and features, depending on your permissions.
⚙	Application Menu	Access profile and ACC Client Settings.
8	System Messages	Displays system messages that require your attention. Notification color represents severity of your most recent message. • **Red** — Error

Area	Description
	• **Yellow** — Warning • **Green** — Information

System Explorer Icons

Icon	Description
	Site — All connected devices and linked features are nested beneath a site.
	Virtual folder — Used to group and organize items under a View tab.
	Server — Only visible for system administrators.
	Fixed camera.
	Pan, Tilt, Zoom (PTZ) camera.
	Avigilon Presence Detector sensor.
	Encoder — Connected to analog cameras.
	Access Control Manager (ACM) appliance — For ACM appliances connected to a site.
	ACM panel or subpanel.
	ACM input.
	Analytic channel used by Rialto devices.
	Virtual Matrix monitor.
	A saved View.
	A map.
	A web page.

System Management

Manage your site, storage, and devices. Add users and groups, manage permissions, and create corporate hierarchies.

Licensing the Site

You can activate, deactivate, and reactivate product or feature licenses. Licenses are called Product Keys in the ACC system, and Activation IDs in the licensing portal.

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

Activating a License

Once your license is activated, you can immediately use the new licensed features.

> **Tip:** Finish organizing your multi-server site before activating a new license to avoid reactivating the site license each time a new server is added.
>
> Keep a copy of the license for future reference.

Online Activation

If you have internet access, use online activation. However, if your site is large and contains hundreds of licenses, the server may time out. See *Offline Activation* below instead.

1. In the New Task menu , click **Site Setup**.
2. Select your new site, then click .
3. Click **Add License...**.
4. Enter your product keys.

   If you copy and paste more than one comma-separated product key, the system will format it automatically.

   - To remove the last product key, click **Remove Last Key**.
   - To clear all the product keys, click **Clear**.
5. Click **Activate Now**.
6. Click **OK**.

Offline Activation

Offline licensing involves transferring files between a computer running the ACC Client software and a computer with internet access.

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Select your new site, then click .
3. Click **Add License...**.
4. Select the **Manual** tab.
5. Enter your product keys.

   If you copy and paste more than one comma-separated product key, the system will format it automatically.

   - To remove the last product key, click **Remove Last Key**.
   - To clear all the product keys, click **Clear**.
6. Click **Save File...** and choose where you want to save the `.key` file. You can rename the file as required.
7. Copy the `.key` file to a computer with internet access.

In a browser:

1. Go to activate.avigilon.com.
2. Click **Choose File** and select the `.key` file.
3. Click **Upload**.

   Important: When reactivating a site cluster, upload all the deactivation `.key` files first and then the single activation `.key` file at last.

   A `capabilityResponse.bin` file should download automatically. If not, allow the download to occur when you are prompted.
4. Complete the product registration page to receive product updates from Avigilon.
5. Copy the `.bin` file to a computer running the ACC Client software.

In the ACC Client:

1. In the License Management dialog box, click **Apply...**.
2. Select the `.bin` file and click **Open**.
3. Click **OK** to confirm your changes.

Changing Site Edition

If you use multiple editions for your site, you can select which edition license is used for the site overall.

For example, if you had a 5-channel Enterprise edition license and later added a 15-channel Standard edition license, you could change your site from Enterprise to Standard edition and use all 20 channels as Standard edition licenses instead of 5 Enterprise edition channels.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Select an edition from the **Select Edition:** drop-down list.
4. Click **Apply**.

Deactivating a License

> **Note:** A license can be deactivated a limited number of times. If you encounter an error while activating a previously deactivated license, this may be the issue. Contact Avigilon Technical Support for help.

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.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Select the licenses you want to deactivate.
4. Click **Remove License...**.
5. To keep a record of the license, click **Copy to Clipboard** and paste into a text file.

   If you have Internet access:

   - Click **Deactivate Now**.

   If you do not have Internet access:

   > **Note:** You will need a licensing.avigilon.com account. Contact your organization's Technical Contact for access.

   1. Select the **Manual** tab.
   2. Click **Save File...** and choose where you want to save the `.key` file.

      The license is deactivated.

   3. Copy the `.key` file to a computer with internet access:

1. Go to activate.avigilon.com.
2. Click **Choose File** and select the `.key` file.
3. Click **Upload**.

   Important: When reactivating a site cluster, upload all the deactivation `.key` files first and then the single activation `.key` file at last.

   A `capabilityResponse.bin` file should download automatically. If not, allow the download to occur when you are prompted.
4. Complete the product registration page to receive product updates from Avigilon.
5. Copy the `.bin` file to a computer running the ACC Client software.

You can now reactivate the license on a new site.

Reactivating a License

FOR ENTERPRISE EDITION

When servers are added to or removed from a site, the site licenses become inactive and must be reactivated to confirm system changes.

If you do not reactivate the affected licenses, the site will stop normal operations.

1. In the New Task menu, click **Site Setup**.
2. Click the site name, then click .
3. Click **Reactivate Licenses...**.

   If you have Internet access:

   1. Click **Reactivate Licenses**.
   2. Click **OK** to confirm your changes.

   If you do not have Internet access:

   1. Select the **Manual** tab.
   2. Click **Save File...** and choose where you want to save the `.key` files.

      Note: For a site cluster, when you manually save the `.key` files, each site generates a deactivation `.key` file and only one activation `.key` file is generated for the entire site cluster.

3. Copy the `.key` files to a computer with internet access:
    1. Go to activate.avigilon.com.
    2. Click **Choose File** and select the `.key` file.
    3. Click **Upload**.

        Important: When reactivating a site cluster, upload all the deactivation `.key` files first and then the single activation `.key` file at last.

        A `capabilityResponse.bin` file should download automatically. If not, allow the download to occur when you are prompted.
    4. Complete the product registration page to receive product updates from Avigilon.
    5. Copy the `.bin` file to a computer running the ACC Client software.
4. In the License Management dialog box, click **Apply...**.
5. Select the `.bin` file and click **Open**.
6. Click **OK** to confirm your changes.

Refreshing a License

Occasionally, an updated copy of the ACC licenses on your site must be downloaded to take advantage of new features and functionality that have been added, or to reflect an updated expiry date after renewal of a subscription license.

Note: Although a Smart Assurance Plan subscription may have expired and will no longer receive updated entitlements when new versions are released, the entitlement for the current version does not expire.

You need to refresh your site licenses to download an updated copy that reflects your current entitlements.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Click **Refresh Licenses**.

    The ACC system contacts the license server and automatically updates your licenses, displaying any changes to the expiry dates or supported versions.

Sites

Discover and manage sites, monitor site health and logs, and backup and restore site settings.

Naming a Site or Server

Give sites and servers meaningful names to easily identify them in the System Explorer.

1. In the New Task menu, click **Site Setup**.
2. Select a site or server, then click **General**.
3. Enter a name, then click **OK**.

Configuring FIPS Compliance

You can select the level of compliance with the Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules for server and client communication.

Server Communication

Define the level of compliance for cryptographic modules used for server communication.

Servers added to a multi-server site will use the same setting as the site.

1. In the New Task menu, click **Site Setup**.
2. Select a site, then click **Security**.
3. Select the **FIPS 140-2 Mode:**
    - **Off** — Only uses non-FIPS compliant cryptographic modules.
    - **Relaxed** — Prefers communication using FIPS 140-2-compliant cryptographic modules, but allows non-compliant cryptographic modules.
    - **Strict** — Allows communication using only FIPS 140-2-compliant cryptographic modules.
4. Click **OK**.

Tip: Use **Relaxed** mode for:

- The initial configuration of a distributed ACC system, especially if using a laptop.
- ACC systems with components that have not been upgraded to version 7.8 or later.
- ACC systems with third-party integrations that are not FIPS 140-2-compliant.

Client Communication

Define the level of compliance for cryptographic modules used when the client logs in to sites.

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Security tab, select the **FIPS 140-2 Mode:**
    - **Off** — Allows log in using the default Secure Remote Password protocol (SRP).
    - **Relaxed** — Allows log in using FIPS 140-2-compliant cryptographic modules and fallback modules. SRP will not be used.
    - **Strict** — Allows log in using only FIPS 140-2-compliant cryptographic modules.
3. Click **OK**.

Tip: The client setting does not need to match the site setting. The client can log in to sites that use a different FIPS mode.

Avigilon Certificates

By default, the ACC system uses a self-signed certificate for verifying client communications and site management.

If your system is configured to use other trusted certificates, you can disable trusting the Avigilon certificate authority.

Important: Make sure that you have set up trusted certificates on your ACC Servers and Clients before disabling trust for the Avigilon certificate authority. For more information, see the *Avigilon System Hardening Guide* or the **ACC Server User Guide**.

Site Settings

1. In the New Task menu , click **Site Setup**.
2. Select a site, then click **Security** .
3. Select the **Require trusted server certificates** checkbox.
4. Click **OK**.

Client Settings

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Security tab, select the **Require trusted server certificates** checkbox.
3. Click **OK**.

Trusted Device Certificates

By default, the ACC system uses a self-signed certificate for verifying device communications. If your devices are configured to use other trusted certificates, you can disable trusting the default Avigilon certificate authority.

Important:
Make sure that you have set up trusted certificates on your devices before disabling trust for the Avigilon certificate authority. If any connected devices do not have trusted certificates properly setup, you will receive an error message and won't be able to select this checkbox.

Click **Device certificate report** to generate a report of all devices that do not meet the certificate requirements.

For more information on setting up device certificates, see the **Avigilon H4 and H5 Camera Web Interface Guide** or the **Camera Configuration Tool User Guide**.

1. In the New Task menu, click **Site Setup**.
2. Select a site, then click **Security** .
3. Select the **Require trusted device certificates:** checkbox.
4. Click **OK**.

Encrypting Video

To improve the security of your ACC system you have the option of encrypting live video that your ACC Client receives from sites. Recorded video is always encrypted. You can encrypt video from all sites, or choose specific sites that will use encrypted video.

Encrypting Video from All Sites

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Security tab, select the **Encrypt video from all sites** checkbox.
3. Click **OK**.

This setting will enforce encrypted video for any new video streams on your ACC Client. Any previously established connections will continue using their configured settings.

Encrypting Video from Specific Sites

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Site Networking tab, find and select a site that will use encrypted video from the list.
3. In the **Connection Type:** drop-down list, select **WAN (Secured)**.

   Repeat this step for any other sites that should use encrypted video.
4. Click **OK**.

Multiple Server Sites

FOR ENTERPRISE EDITION

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

> **Tip:** Plan how your system should be configured before connecting servers to sites to avoid reconfiguring settings each time a server is added.

Connecting Servers to a Site

Sites only have one server by default, but you can add multiple servers to a site and manage them together. All servers within a site share settings and are represented as one unit in the System Explorer.

When servers are installed a significant distance apart, they may only share users and group information. These sites can be joined into families. For more information, see *Site Families* on page 97.

Note:

- If you're using the Avigilon Artificial Intelligence (AI) Appliance, connect the appliance to an NVR before connecting that NVR to your site.
- Servers must have the same version of the ACC software to be connected.
- Servers should be on the same broadcast domain or broadcast network because the servers will exchange data.
- Ensure ports 38880 to 38884 TCP/UDP are open across the network.
- Ensure servers have unique hostnames.
- When a server joins a site, its site license must be reactivated. For more information, see *Reactivating a License* on page 13.

1. In the New Task menu , click **Site Setup**.
2. Click .

   The Site Management tab lists all accessible and connected sites and servers. If you can't find your site, you'll need to search for it. For more information, see *Discovering Sites* on page 4.
3. Select your server and drag it to a different site.

   Sites without any servers are automatically removed from the list.
4. Reactivate the site license.

After the server is connected to the site, settings are merged and the following rules are applied:

- Unique settings from the server are added to the site.
- When settings are identical, only the site version is kept.
- When a server setting and a site setting share the same name but are configured differently, the server setting is added to the site and renamed: <setting name> (server name), e.g. Email1 (Server2F).
- Site Views are combined.
    - Site organization settings override server settings when merged. Any unorganized elements from the server are listed at the bottom of the site View.
- All user groups are merged.
    - If groups have the same name, the site settings are used and users from both the site and the server are added to the group.
    - New groups to the site automatically receive access to all the devices in the site.
    - New groups to the added server automatically receive access to all the devices that are connected to the server.
- Users with the same name will share configured settings, including passwords, and gain group permissions from the server.
- Active Directory settings are configured at the site level. Before adding a server to a site with Active Directory, check the following or the connection will fail. For more information, see *Importing Active Directory Users* on page 85..
    - A Windows server is connected to the same Active Directory domain as the site.
    - If adding an Avigilon Hardened OS appliance to a site with Windows servers, the site must clear the **Use ACC service account** and **Enable nested groups** checkboxes and enter a username (for example, `john.smith@domain.com`) and password.
    - If Active Directory is configured on an Avigilon Hardened OS appliance, it must be connected to the same Active Directory domain as the site. An appliance without any Active Directory configuration can be added to a site and will inherit the domain from the site.

Note: Disconnect the server from a site before making any of the following changes:

- Changing the hostname
- Changing the IP address
- Reinstalling Windows or installing a different version of Windows
- Replacing the server with another server
- Decommissioning the server

Disconnecting Servers from a Site

When you disconnect a server from a site, it becomes a separate server under its own site.

Disconnected servers retain all settings from the site it was previously connected to.

1. In the New Task menu , click **Site Setup**.
2. Click .The Site Management tab lists all the sites that you can access and all the servers that are connected to each site.
3. Select a server from the site and click **Disconnect from Site...**.
4. After the server is disconnected, you'll need to reactivate the site licenses. For more information, see *Reactivating a License* on page 13.

You can purchase new licenses for a disconnected server or you can deactivate the required licenses from the previous site. Deactivated licenses can be activated for other sites. For more information, see *Deactivating a License* on page 12.

Site Health

The Site Health tab provides an overview of your site.

1. In the New Task menu , click **Site Health**.
2. In the System Explorer, select a site.

> **Tip:** The Site Health report can also be generated from the ACS Web Client. See **Avigilon Cloud Services** on **help.avigilon.com** for more details.

For site families, if you are logged in to the parent site you can see the status of all child sites. If you are only logged in to a child site, the parent site status is displayed as unknown.

The following icons identify the status of each component:

- The component is functioning normally.
- The component requires your attention.
- The component is unavailable or offline.
- The component status is unknown.

To perform a basic system health check, see *Basic ACC System Health Check* on page 192.

Exporting a Report

You can export the site health information as a CSV or PDF file. The CSV file includes additional information about device IDs and connection status.

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

   The report is downloaded.

Filtering Site Information

By default, all server and appliance information as well as device information is displayed.

- In the Find server... search bar, enter the name of the server.
- Below the Site Information: box, click an icon to show or hide a section.

  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.

- In the Find device... search bar, enter the name or any other attribute of the device to filter the device list. You can also filter devices by selecting one of the following statuses from the drop-down menu in the right.

Status	Description
Device Error	A device in an error state that requires your attention.
Device Removed	A device that has been physically removed from the network.
Firmware Upgrade Required	A device that requires a firmware upgrade.

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 camera, FIPS camera, analytics, License Plate Recognition (LPR), Face, and point of sale (POS) channels used over the total number of channels available for the site. **Note:** Channels from ACC ES appliances are not included in this count and can be found in the Server License Usage: area.
Avigilon Cloud Services:	The status of the connection to the Avigilon Cloud Services platform.

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:

Name	Description
Server Version:	The ACC Server version number.
Server IP:	The server's IP address.
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.
Site License Usage:	The number of site licenses used for camera, FIPS camera, analytics, LPR, Face, and POS channels on the server. Devices that do not generate video streams do not use camera channels.
Server License Usage:	The number of factory-installed camera and analytics channels. These channels are used before channels from the site 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 Server Analytics Load by disabling Face Recognition or the Avigilon Appearance Search feature on some cameras. ✖ The ACC Analytics Service is offline.

Name	Description
Peak Load (Last 3 Days):	The highest percent usage of the analytics service over the last 3 days.

Cloud Service:

Name	Description
Representing Site	In a multi-server site, one ACC Server is Active and represents the site while the other ACC Servers are on Standby for automatic activation.
Web Endpoint Status	The operational status of the ACC Web Endpoint Service. The ACC Server communicates with the ACS platform only when the ACC Web Endpoint Service is up and the ACS platform is connected.
Cloud Connection Status	The status of the ACC Server's connection to the ACS platform over the internet of things (IoT) network.
Region	The ACS region that the site is connected to. Displays only when the ACC Server is connected to the ACS platform.
Last Connected	The date and timestamp of the ACC Server's last connection to the ACS platform. Never is displayed until the server is booted up the first time.

Network Adapters:

> **Tip:** For servers with multiple network adapters, use one for the camera network and another for the coroporate network. You can do this by putting the network adapters in different IP subnets.

Name	Description
Adapter Name	The name of the network adapter that is connected to the server.
Status	The operational status of the network adapter.
Link Speed	The maximum speed supported by the network adapter based on its network connectivity. Ensure this is at least 1 Gbps for the camera network.
IP	The IP address of the network adapter. Appears empty for network adapters that are disconnected.
Incoming	The bandwidth usage of incoming data.
Outgoing	The bandwidth usage of outgoing data. This includes video streaming to the

Name	Description
	ACC Client software, ACC Virtual Matrix software, and ACC Mobile 3 application.

Hard Drives:

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) state of the hard disk. Statuses include: • Other • Unknown • OK • Non-critical • Critical • Non-recoverable • Absent
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:

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:

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:

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.

Array Storage Controllers:

Only available if the server is associated to the storage device and the server's SNMP service is enabled.

Name	Description
Name	The storage controller name.
ID	The storage controller identifier.
State	The storage controller state: • **Unknown** — The state is unknown. • **Online** — The controller is available. • **Offline** — The controller is unavailable. It may be in self-test mode.
Status	The storage controller status: • **Unknown** — The status is unknown. • **Unused** — The controller cannot report its status. • **OK** — The controller is working as expected. • **Warning** — The controller requires attention. • **Failed** — The controller has failed.
Location	The storage controller location.
Management URL	The URL to access the storage controller web interface.

Name	Description
Last Updated	Shows when the storage controller status was last updated. If the date is more than 10 minutes in the past, the controller may be offline.

Devices:

Name	Description
General	The name, model number, location, and Logical ID 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 firmware version and serial number of the device. The ⚠ icon is displayed if the device requires a firmware upgrade. **Note:** To download the latest available camera firmware, download the `.fp` version of the firmware file from the **Cameras and Sensors** page on **avigilon.com**. To upgrade the camera firmware, see *Upgrading Your Site Remotely* on page 37.
Encryption	The encryption mode of the device.
Compression	The video compression rate, resolution, quality and images per second (ips) of video streamed from the device. This column may be empty if the device is disconnected.
Retention	The age of the oldest recorded video that is not a protected bookmark, and the age of the oldest archived video if available.
Device ID	CSV export only. The device identifier. This contains information about the camera, server, and site and can be used for third-party integrations.
Analytics	The Avigilon Appearance Search, Face Recognition, or Face Mask Detection feature is enabled, disabled, or unsupported.
Camera ID String	CSV export only. The camera identifier. This can be used in third-party integrations.
Connected	CSV export only. Whether the device is connected to the server or not.

Name	Description
Visible	CSV export only. Whether the device has been discovered by the ACC system or not.
Error Flags	CSV export only. A description of any authorization, network, or connection errors that occurred.
Status	CSV export only. The device status: • **Online** — the device is connected. • **Removed** — the device is disconnected without an error. • **Communication Error** — the device is disconnected for longer than 5 minutes. • **Failed** — an error occurred on the device. • **Unknown** — the device status is unknown.

Access Control Manager Appliance

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

Viewing Site Logs

Track system usage and diagnose issues by viewing a list of events that occurred in the ACC software. System events are kept as long as video data is available or for 90 days, whichever is longer.

1. In the New Task menu, click **Site Logs**.
2. In the top-left area, select the types of events and their details to search. See:
   - *Server Events* on the next page
   - *Device Events* on page 30
   - *User Events* on page 31
   - *Access Events* on page 33
3. Select the site, server, or devices you want to search.
4. Set the date and time range of the search.
5. Click **Search**.
6. Select a column header to sort results by Time, Type, or Message.
7. Click a search result to display the event details at the bottom of the tab. You may need to scroll down to view the entire event details.

Note: It may take 30 minutes for an entry to be displayed, especially Access Events for live or recorded video.

Exporting Site Log Results

Export event details as a text or CSV file. Keep the exports for your records or if you need to troubleshoot an issue with Avigilon Technical Support.

1. In the lower-left corner, click **Save events to file...**.
2. Select a location, file name, and type.

Tip: Entire event details are viewed at the bottom of the Site Logs screen and are not saved to the file. For some examples, see *Site Log Examples* on page 34.

Event Details

The following table describes the event details for a search result.

Property	Description
Event message	An overview of the event.
Time:	The time the event occurred.
Type:	The type of event that occurred.
Server:	The name of the ACC Server that the event occurred on.
Device:	The name of the device. For Device events only.
Client:	The name of the machine and its IP address that the ACC Client runs on. For User events only.
Details:	Additional information about the event that occurred.

Site Log Descriptions

Server Events

The following table describes the events of ACC server operation and failure in site logs.

Event	Description
Start/Stop	Server software has restarted or stopped normally or abnormally.
License	Any of: • Server software license expires soon.

Event	Description
	• Server software license has expired. • Server software license has partially expired.
Database	Any of: • Server database has generated an error. • Server database has generated an error during initialization. • Database environment was deleted or forcefully deleted. • Database was recreated, recovered or lost. • Corrupted database occurred and was unrecoverable. • Database was re-indexed.
Data	Any of: • Server data volume has failed. • Server data volume was recovered. • Server data volume size was reduced. • Server generated an error while writing data. • Server data upgrade has started. • Server data upgrade has completed. • Server data upgrade has failed. • Server data recovery has started. • Server data recovery has completed. • Server data recovery has failed.
Hardware	A server hardware error has occurred.
Archive	Any of: • Server backup has started. • Server backup has completed. • Server backup has failed.
Network	Any of: • Server network connection was found. • Server connection to the site was lost.
Email	An email notification server error has occurred.
Memory	A low memory resources error has occurred.

Event	Description
Installation	Any of: • Server upgrade and/or bundle of components has started. • Upgrade of a component has started or finished. For example, ACC Client.
Analytics	Any of: • 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. • Server is unable to communicate with the video analytics service to perform Avigilon Appearance Search queries
Access Control	Any of: • ACM server was connected or disconnected. • Service was offline or restored. • Input was activated or deactivated. • New certificate or certificate validation has failed. • Input error has occurred.
LPR Start/Stop	The LPR service has restarted or stopped.
Avigilon Cloud Services	Any of: • A user has connected to the Avigilon Cloud Services platform. • A user has disconnected from the Avigilon Cloud Services platform. • A user has connected to Avigilon Cloud Services using an ACC Connect subscription. • A status update of an ACC Connect subscription connection has occurred.
User Sync	Occurs periodically to synchronize any connected Active Directory groups and users information.

Device Events

The following table describes the events of camera or device operation.

Event	Description
Start/Stop	A camera or device has restarted or stopped.
Connection	Any of: • A camera or device has connected to a server.

Event	Description
	• A camera or device has disconnected from a server. • A camera or device has connected to a standby server. • A camera or device has disconnected from a standby server. • A camera or device connection has been restored.
Connection Failure	Any of: • A camera or device connection has failed. • A camera or device connection has failed for more than 5 minutes.
Firmware Upgrade	Any of: • A camera or device firmware upgrade has started. • A camera or device firmware upgrade has been completed. • A camera or device firmware upgrade has failed. • A camera or device is detected to be running obsolete firmware. The system is unable to perform an automatic upgrade.
Network	Any of: • Network packet loss is acceptable for the impacted camera or device. • Network packet loss is unacceptable for the impacted camera or device.
Recording Error	Any of: • A camera or device recording has started. • A camera or device recording has ended. • A camera or device recording was interrupted. • A camera or device recording has resumed.
ONVIF Events	An event has originated from a third-party camera or device.

User Events

The following table describes the events of user and group administration updates.

Event	Description
Site Setting	An administrator has changed site settings. Any of: • A user was added, modified, or deleted. • A user group was added, modified, or deleted.

Event	Description
	• Access rights for a group was added, modified, or deleted. • An entity was added, renamed, or deleted from Site View. • An external directory for an Access Control or Active Directory group or user was added or removed.
Server Setting	A user has changed the server settings.
Device Setting	A user has changed the camera or device settings.
Device Connection	Any of: • A user has connected a camera or device to a server. • A user has disconnected a camera or device from a server.
Digital Output	A user has manually triggered a digital output.
Speaker	Any of: • A user is broadcasting audio through camera or device speakers. • A user has stopped broadcasting audio.
Bookmark	Any of: • A user has added a bookmark. • A user has updated a bookmark. • A user has deleted a bookmark.
PTZ	Any of: • A user has moved a PTZ camera. • A user has left a PTZ camera idle.
View	Any of: • A user has added a saved View. • A user has updated a saved View. • A user has deleted a saved View.
Map	Any of: • A user has added a new map. • A user has updated a map. • A user has deleted a map.
Web Page	Any of: • A user has added a new web page.

Event	Description
	• A user has updated a web page. • A user has deleted a web page.
Site View	A user has updated the way cameras are organized in the System Explorer.
Custom keyboard command	A user has triggered a custom keyboard command.
Central Station	A user has sent a test message, known also as a heartbeat notification, to the central monitoring station.
Access Control	A door event has occurred. Any of: • Door access was denied. • Door access was granted. • Door was closed. • Door was forced. • Forced door was closed. • Door was held open. • Door was opened. • Door was in a duress state. • Door received a request to exit. • ACM panel or subpanel input was activated. • ACM panel or subpanel input was deactivated. • ACM panel or subpanel input was activated. • Fault was detected for the ACM panel or subpanel input. • Fault was cleared for the ACM panel or subpanel input.
Metadata Retention	An operator has changed the settings for Metadata Retention.

Access Events

The following table describes the events of a user or group accessing the ACC system, and live and recorded video.

Event	Description
Export	Any of: • A user has performed a file export. • A user has performed a file export that failed. • A user has performed a video export.
Live Video	A user has accessed a live video stream.

Event	Description
Login Failure	A user login to the server has failed.
Login/Logout	Any of: • A user has logged in or logged out. • A user has enabled or disabled Emergency Privilege Override. • A secondary user provided dual authorization for the primary user.
Recorded Video	A user has accessed a recorded video.
Search	Any of: • A user has performed Appearance Search based on a physical description of a person or vehicle of interest. • A user has performed Appearance Search based on an uploaded image of a person or vehicle of interest. • A user has performed Appearance Search based on a segment of recorded video.

Site Log Examples

User Group Added

The following message shows an event about a user group that was added.

```
Message: Site setting (user group'username') was added by administrator.

 Time:    Fri, Oct 01, 2019 1:23:45 PM
 Type:    User
 Server:  server_name
 Client:  client_name(nnn.nnn.nnn.nnn)
 Details: Group Name (groupname)
          Dual authorization (Clear)
          Two-Factor Authentication (Clear)
          Min Password Strength (strong)
          Rank (Unranked)
```

Access Granted to a Device

The following message shows a user group that was granted access to a device by the administrator user.

```
Message: Site setting (user group 'groupname') - access right to
device,'devicename', was restored by administrator.

 Time:    Fri, Oct 01, 2019 1:23:45 PM
 Type:    User
 Server:  server_name
 Client:  client_name(nnn.nnn.nnn.nnn)
```

```
Details: View live images (Clear ==> Selected)
         Trigger digital outputs (Clear ==> Selected)
         Broadcast to speakers (Clear ==> Selected)
         View high-resolution images (Clear ==> Selected)
         Listen to microphones (Clear ==> Selected)
```

User Accessed Footage from Multiple Cameras

The following message shows an event about a user who has accessed video footage from multiple cameras.

```
Message: Live video viewed for camera 'camera_B' from time 2019-10-01
01:23:12.123 PM to 2019-10-01 01:33:12.123 PM by 'username_A'

Time:   Fri, Oct 01, 2019 01:33:12 PM
Type:   User
Server: server_name

Message: Live video viewed for camera 'camera_A' from time 2019-10-01
01:12:12.123 PM to 2019-10-01 01:22.12.123 PM by 'username_A'

Time:   Fri, Oct 01, 2019 1:22:12 PM
Type:   User
Server: server_name
```

User Group Privileges Update

The following message shows the details of a user group privileges update.

```
Message: Site setting (user group 'groupname') - access right to site view,
'sitename', was added by administrator.

Time:    Fri, Oct 01, 2019 1:23:45 PM
Type:    User
Server:  server_name
Client:  client_name(nnn.nnn.nnn.nnn)
Details: Listen to microphones (Selected)
         Setup general settings (Selected)
         Setup network settings (Selected)
         Setup image and display settings (Selected)
         Setup compression and image rate settings (Selected)
         Setup image dimension settings (Selected)
         Setup motion detection settings (Selected)
         Setup privacy zone settings (Selected)
         Setup manual recording settings (Selected)
         Setup digital input & output settings (Selected)
         Setup microphone settings (Selected)
         Setup speaker settings (Selected)
         Setup analytics settings (Selected)
```

```
Setup teach by example settings (Selected)
Setup PTZ settings (Selected)
Setup web configuration settings (Selected)
Setup name settings (Selected)
Manage site (Selected)
Setup site view (Selected)
Setup user and group settings (Selected)
Setup Active Directory Synchronization (Selected)
View high-resolution images (Selected)
Manage saved views (Selected)
Manage maps (Selected)
Manage web pages (Selected)
Manage virtual matrix monitors (Selected)
Manage collaboration sessions (Selected)
Manage user sessions (Selected)
Setup corporate hierarchy (Selected)
Setup alarm management settings (Selected)
Setup POS transaction settings (Selected)
Setup LPR settings (Selected)
Setup LPR watch lists (Selected)
Setup external notification settings (Selected)
Setup rule engine settings (Selected)
View site logs (Selected)
Connect and disconnect devices (Selected)
View Site Health (Selected)
Manage server (Selected)
Setup schedule settings (Selected)
Setup recording and bandwidth settings (Selected)
Setup Storage Management (Selected)
Manage server (Selected)
Setup schedule settings (Selected)
Setup recording and bandwidth settings (Selected)
Setup Storage Management (Selected)
Backup settings (Selected)
Setup server analytics (Selected)
```

User Information Update

The following message shows specific changes in a user information update.

```
Message: Site setting (user 'username') was updated by administrator.

 Time:    Fri, Oct 01, 2019 1:23:45 PM
 Type:    User
 Client:  client_name(nnn.nnn.nnn.nnn)
```

```
Details: First Name (noname ==> my first name)
         Last Name (noname ==> my last name)
         Password never expires (Clear ==> Selected)
```

User Performed Appearance Search

The following message shows an event about an Appearance Search performed by a user on an uploaded photo, including the reason in Details and the photo, if available.

```
Message: Appearance Search from image performed from 2020-Sep-01 01:45:00.000
PM to 2020-Sep-01 07:50-00.000 PM by administrator.

Time:    Tue, Sep 01, 2020 1:23:45 PM
Type:    User
Server:  server_name
Client:  client_name
Devices: device_name_a, device_name_n
Details: Looking for suspicious individual found on premise.
```

User Login Failed

The following message shows an event about a failed login by a user.

```
Message: Failed login by user 'username' on client 'clientname', client type
'ACC Client'

Time:   Fri, Oct 01, 2019 1:23:45 PM
Type:   User
Server: server_name
Client: clientname
```

Upgrading Your Site Remotely

The ACC Remote Site Upgrade feature lets you update all the servers in your ACC site using the ACC Client instead of applying the component updates on the console of each server. You can install new components or upgrade existing components including services and plugins, language packs, and camera firmware.

Important: ACC is unable to upgrade a site remotely if the ACC service is running in a lower privilege mode like Network Service. To upgrade a site remotely, make sure that the ACC service is running with the correct privileges. By default, the ACC service runs with the correct privileges.

For upgrades to servers and appliances:

- Download and install the latest version of the ACC Client software first.
- NVR servers must run ACC Server version 5.10.24.1 or later.
- ACC ES Recorders must run ACC Server version 5.10.24.1 or later.
- Avigilon video analytics appliances must run ACC Server version 6.0 or later.

  Set up failover connections before performing an upgrade to maintain a video connection during the update. This allows cameras to connect to a secondary or tertiary server while the primary server restarts. For more information, see *Failover Connections* on page 48.

  If your site is connected to ONVIF® Profile G cameras with SD cards that are recording video, the ACC Server can recover video that is missed during the upgrade when the server comes back online. For more information, see *Recovering Video from Profile G Cameras* on page 50.

  ONVIF is a trademark of Onvif, Inc.

Tip: Between each step during Site Upgrade, you can close the dialog box and continue regular operations.

1. Download the latest version of the ACC component installer from **avigilon.com**.
2. Install and run the latest version of the ACC Client software.
3. In the ACC Client software, log in to your site.
4. In the New Task menu ☰, click **Site Setup**.
5. Click the site name, then click **Site Upgrade**.
6. In the top-right corner, click **Upload** and open the downloaded installer.

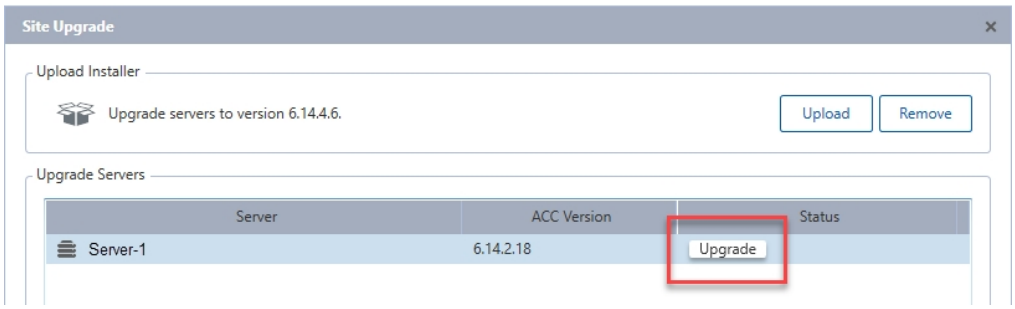
   Note: To upgrade camera firmware, download the `.fp` version of the firmware file from the **Cameras and Sensors** page on **avigilon.com**.

7. Confirm the correct installer was selected and click **OK**.

   The installer will be uploaded to one server and then distributed to other servers in the site. This process may take several moments.

   When the installer has been distributed throughout the system, the Status column will display an Upgrade button.

8. In the Status column, click **Upgrade**.



9. Click **OK**. The status bar displays the progress.

   If the component was a service, plugin, or firmware upgrade, the server will not reboot. You may need to open and close the Site Upgrade dialog to verify the ACC component version updated.

   If the component was a server upgrade, the server will reboot. During the reboot, the server will disappear from the list until it reconnects with the system. You may need to log back in to the site to see the progress.

   To maintain secondary or tertiary connections, wait for each server to complete its upgrade before starting another server.

10. Repeat steps 6 and 7 for each component you want to upgrade.

Removing an Upgrade Installer

If you've uploaded the wrong installer to the site, you can remove the installer before the upgrade is complete.

1. In the Site Setup tab, click .
2. Click **Remove**.
3. Click **OK**.

The upgrade installer will be deleted from the system.

Backing Up Site Settings

> **Note:** Backup files can only be restored on sites that are running the same or later version of the ACC Server software.

Back up site and server configuration settings to apply them to a second site, or restore them in the event of an unexpected system failure.

1. In the New Task menu , click **Site Setup**.
2. Click .
3. Select the server that you want to back up. Site settings are automatically included in the backup file.
4. Select the **Encrypt the backup file.** checkbox. Enter and confirm a password.

   If this encryption password is lost, the file will not restore any system settings.
5. Click **OK**.
6. Name and save the file.

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

Restoring Site Settings

Note:

- You cannot restore settings from your 5.2.2 or earlier version server through this version of the ACC Client software.
- Make sure the new site is licensed to run the same features as the previous site.

If you have a backup Avigilon Settings File (`.avs`), you can restore the settings after a server replacement or while setting up an independent site.

When you restore settings, existing settings are overwritten. When site settings are restored, the settings are merged with previous settings.

1. In the New Task menu , click **Site Setup**.
2. Click .
3. Select the `.avs` file that you want to restore.
4. If the backup file is encrypted, enter the password.
5. Select the settings you want to restore.
   - **Restore site and server settings** — Restores all settings in the site and the selected server.

     Note: Do not select this option if the server is part of a multi-server site. The site settings are maintained by the other connected servers.
   - **Restore server settings** — Restores all settings to the selected server.
   - **Use custom settings** — Lets you specify the settings that you want to restore.

     Some custom settings have dependencies that may cause unexpected issues if they are not supported by the server.

6. Select the server you want to restore.

   Only select servers from the Recommended Servers list. Servers in this list do not have any existing device connections. Restoring settings to a server not listed may overwrite existing device connections or cause the system to exceed its license and processing limits.

7. Click **OK**.

If you restored the site settings, settings will merge:

- 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 that are 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 that are 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.

Servers and Storage

Configure recording and archival settings to manage your storage usage. You can also configure the priority of failover servers.

Identity Data Retention

FOR ENTERPRISE EDITION

Note: These settings override protected bookmarks and video retention settings.

Depending on your privacy policy or regional regulations, you may only be able to retain identifying data for a specific amount of time.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Identity Data Retention** .
3. Select the checkbox next to each available feature and enter the maximum number of days to retain data.
4. Click **OK**.

Recording and Bandwidth

The Recording and Bandwidth settings define how long recorded video is stored. You can set the maximum record time for each camera connected to a server, and configure Data Aging settings.

Video Retention

The Total Record Time is estimated based on continuous recording and may not reflect the actual video retention.

The actual video retention is determined by the Max. Record Time setting and the average camera data rate. The actual retention time may exceed the Max. Record Time setting by 5 minutes.

Data Aging

Data aging is when ACC deletes videos based on their age in relation to the Max. Record Time setting. ACC prioritizes newer over older recorded video. By default, the Data Aging setting stores both high-resolution and low-resolution video until the Tier 1 storage is full. Once the storage is full, older video will be deleted.

ACC deletes older videos when any of the following occur:

- The Max. Record Time setting is set to the maximum value and the storage is full.
- A new camera is added and the storage is full.
- The Max. Record Time setting is set to X days and the stored videos are older than X days, even if the storage is not full.
- The slider is moved to the left and the change is saved; high-resolution videos are deleted based on the adjustment.

Video storage pertains to the data volume defined using the ACC Admin Tool.

To increase the amount of video stored when the Tier 1 storage is full, update the Data Aging setting to discard a percent of the high-resolution video. The system will discard the oldest high-resolution video and only store the low-resolution video to maximize storage. The oldest video stored will be low-resolution.

Note: Data Aging is shown in approximate days. It is applied as a percentage of the total footage. The number of Data Aging days is not guaranteed to change immediately after there are changes made to the system like adding cameras, or adjusting the Max. Record Time setting. ACC reviews stored recordings of all cameras and recalculates the predicted Data Aging days and Total Record Time. This may take a few days depending on the Data Aging and Max. Record Time settings, the number of cameras, and storage size.

The extent of data aging that is available depends on the cameras connected.

- For JPEG2000 or JPEG compression cameras, data aging is available at three rates:
  - **High Bandwidth** — Records at original quality.
  - **Half Image Rate** — Records half of the data to make room for new recordings.
  - **Quarter Image Rate** — Records a quarter of the original data, allowing you to still view older video.
- H.265 and H.264 cameras that support data aging, are available at two rates:
  - **High Bandwidth** — Keep the original high quality video and a secondary low resolution stream.
  - **Low Bandwidth** — Only keep the secondary stream of low resolution video.

    Note: Data aging only occurs when the secondary stream is enabled. Some cameras have a tertiary stream.
- For H.265 and H.264 cameras that do not support data aging, only the **High Bandwidth** video is kept.

Configuring Data Aging

Note: When using Data Aging with the Continuous Archive feature, make a note of the lowest data aging setting. The Continuous Archive settings should archive video at least one day less than the data aging setting to ensure video is archived before it is deleted. For more information, see *Continuous Archive* on the next page.

1. In the New Task menu, click **Site Setup**.
2. Select a server, then click **Recording and Bandwidth**.

   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.

3. In the Data Aging column, move the sliders to adjust the amount of video that 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.
4. 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 Total Record Time is significantly shorter than the Max. Record Time, the camera's actual recording time will be closer to the Total Record Time estimate. The total recording time assumes continuous recording, and will increase with a Recording Schedule.

5. Click **OK**.

Continuous Archive

FOR ENTERPRISE EDITION

The Continuous Archive feature automatically saves video to the archive directory in hourly blocks using the server's local time.

Archived video can be accessed as recorded video. For more information, see *Playing Recorded Video with the Timeline* on page 157.

Archived video can also be reviewed in the Avigilon Player software.

Enabling Storage Management

Before you can enable the Continuous Archive feature, you must enable Storage Management on your ACC Server and select the archive location:

- **Network video recorders:**
    1. In the ACC Admin Tool, select the Settings tab and click **Storage Management**.
    2. Select the **Enable Storage Management** checkbox and select the archive folder.
    3. Click **OK** to save.
- **Avigilon Hardened OS appliances:**
    1. In the New Task menu , click **Site Setup**.
    2. Select a server, then click **Server Management** and log in.
    3. Click **Network Storage Management**, then click **Enabled**.
    4. Select the protocol and enter the path to the preferred archive location. Enter the network location credentials if required.

- **CIFS** — Common Internet file system. The network path is typically in this format: *//<hostname or IP> / <path>*
- **NFS** — Network file system. The network path is typically in this format: *<hostname or IP> : <path>*

5. Click **Apply**.

Enabling Continuous Archive

Archiving should be configured along with Data Aging. By configuring both, you'll have a tiered storage configuration to manage the amount of video retained on your local server.

> **Note:** Set the Archive video older than: parameter to at least one day less than the Data Aging setting. This ensures that you always have high quality video of important events. For more information about Data Aging, see *Recording and Bandwidth* on page 42.

1. In the New Task menu, click **Site Setup**.
2. Select a server, then click **Storage Management** .
3. Select the **Enable Continuous Archive** checkbox.
4. In Camera(s) to Archive:, select the devices to include in the archive.
5. In Options, define the following:
   - **Archiving permitted:** — Specify the time frame when Continuous Archive is permitted. The time you select is the server's local time.

     If you want archiving operations to occur 24 hours each day (including retries), specify the time frame to be **00:00** to **23:59**.
   - **Archive video older than:** — The minimum number of days before recorded video is archived.

     Ensure this value is less than the number of days specified in Recording and Bandwidth for deleting High Bandwidth video on your local server. One fewer day is enough to account for network restricted retries.

     > **Tip:** Recorded video remains in the site until it is removed by data aging. For more information, see *Recording and Bandwidth* on page 42.
   - **Delete archived video older than:** — Automatically deletes recorded video older than the number of days specified. The maximum setting is 3650 days (10 years).

     If this setting is smaller than the Archive video older than: setting, video will be deleted immediately after it is archived.

- **Delete oldest archive when disk full**: — Automatically deletes the oldest archive files when the archive storage location is full.

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

6. Click **OK**.

   The Status area displays information about the last, current, and queued archive jobs.

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 or network issue occurs during the archiving process, the ACC system will automatically retry archiving.

Resetting Continuous Archive

The Continuous Archive feature will queue jobs after the last archive. To clear the archive queue, reset the continuous archive feature.

1. In the New Task menu , click **Site Setup**.
2. Select a server, then click **Storage Management** .
3. Click **Reset Continuous Archive**.
4. Click **OK**.

The next archive job will start at the beginning of the next hour, if permitted.

Manual Recording Setup

When manual recording begins 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 .
2. Define the following:
   - **Manual Recording Duration:** — How long before recording is triggered should the camera record.
   - **Pre-Trigger Record Time:** — How much time should be recorded before recording is activated.

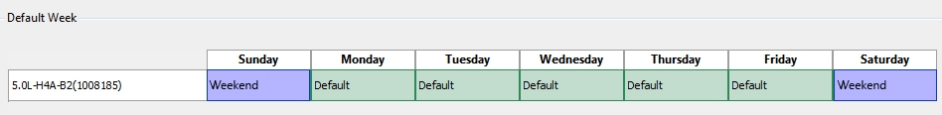
   Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
3. Click **OK**.

To learn how to start recording, see *Manually Recording Video* on page 157.

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 New Task menu , click **Site Setup**.
2. Select a server, then click **Recording Schedule** .
3. Select a template from the **Templates:** list. For more information, see *Recording Schedule Templates* below.
4. In Default Week, click the days your template will cover for each camera on your site.



5. Click **OK**.

Recording Schedule Templates

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

> **Note:** Recording templates are shared across a site.

Adding a Template

1. In the New Task menu , click **Site Setup**.
2. Select a server then, click **Recording Schedule** .
3. In the Templates: area, click **Add Template** .
4. Enter a name for the **New Template**.
5. Click the **Set Area** button, then click or drag the cursor across the **Recording Mode:** timeline to set the types of events cameras will record. Individual rectangles on the Recording Mode: timeline are colored when they have been selected.

   The **Recording Mode:** options include:

   - **Continuous** — Records video constantly.
   - **Motion** — Records video when motion is detected.
   - **Digital Inputs** — Records video when a digital input is activated.
   - **Alarms** — Records video when an alarm is activated.
   - **POS Transactions** — Records video when a point of sale (POS) transaction is made.
   - **License Plates** — Records video when a license plate is detected.
6. To disable recording in parts of the template, click **Clear Area**, then click or drag the cursor across the timeline to remove set recording periods.

7. 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:** checkbox and set the time between each reference image.

Editing and Deleting a Template

1. In the Setup tab, select the server you want to edit and click .
2. 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**.

Failover Connections

FOR ENTERPRISE EDITION

When connecting devices, you have the option to assign a failover connection to a backup server. This connection allows a device to continue recording if connection to the primary server fails. The Failover connection does not activate when a camera goes offline.

> **Note:** Failover connections can only be made between servers within the same multi-server site. When a failover connection is made, a single failover license is required for each camera. Regular camera channel licenses and failover licenses can be used on a failover server.

Each device can be connected to multiple servers. The Connection Type: determines when the device will connect.

- **Primary:** — Devices automatically connect to this server when on the same network.
- **Secondary:** — When the Primary server is not available, the device will connect to this server when on the same network.
- **Tertiary:** — When the Secondary server also fails, the device will connect to this server when on the same network.

The **License Priority:** sets the order that devices will connect to a server — **1** is highest and **5** is lowest. If the server does not have enough camera failover licenses, low priority devices may not connect.

The prerequisites for failover connections are as follows:

- ACC Enterprise Edition on all servers.
- Two or more servers merged into one multi-server site (does not apply to a Parent-Child site configuration).
- Have all the servers on the same switch or on the same network.

- All IP cameras should be accessible by all servers. Avigilon cameras and third-party cameras are supported.
- Make sure that the servers are licensed to accommodate the additional camera connections in the event of a failure.

Editing Failover Connections

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Connect/Disconnect Devices** .
3. Select a connected device, then click **Edit...**.
4. Select the relationship you want to edit in **Change on server:**.
5. Update the **Connection Type:** to Primary, Secondary, or Tertiary.

   > **Note:** If you select Secondary or Tertiary, update the **License Priority:**.

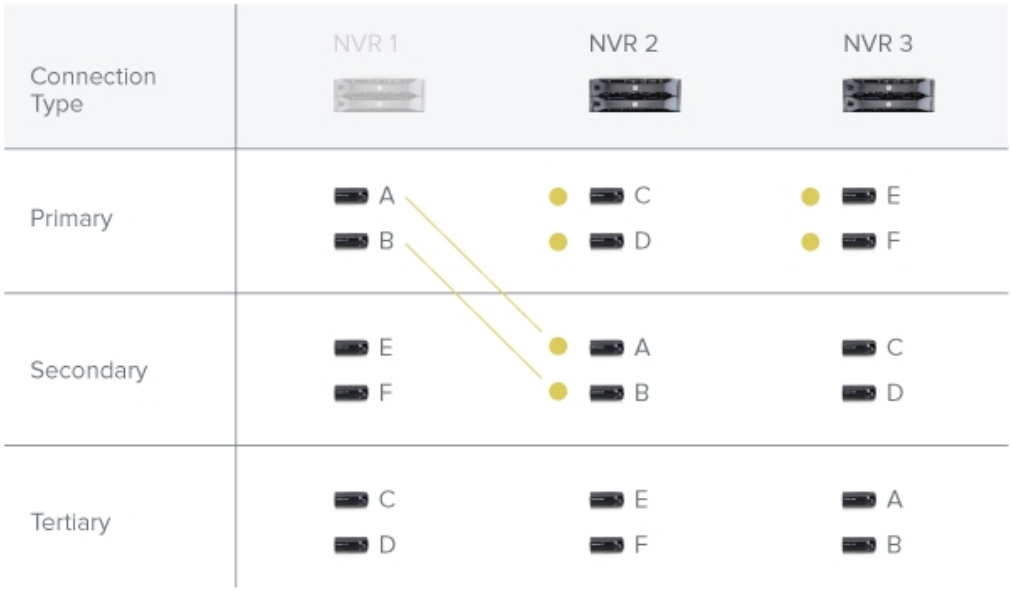
6. Click **OK**.

Failover Examples

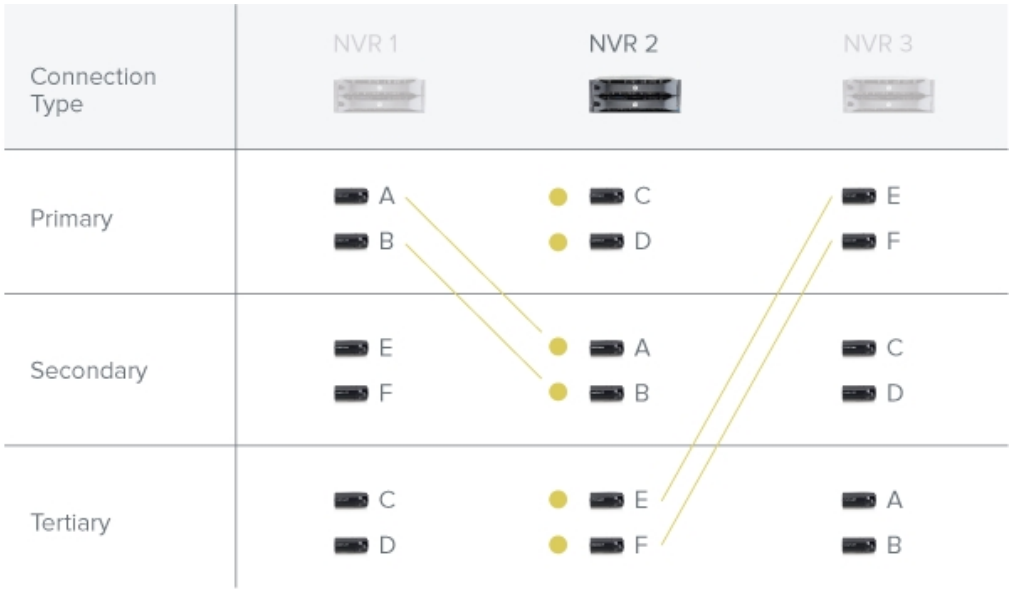
Cameras A, B, C, D, E and F have failover connections set to two different servers. For this example, the site has 6 camera channel licenses with 4 failover licenses, and the license priority is set to 1 for each connection.

Connection Type	NVR 1	NVR 2	NVR 3
Primary	A B	C D	E F
Secondary	E F	A B	C D
Tertiary	C D	E F	A B

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



When NVR 3 fails, cameras E and F automatically connect to their Tertiary server, NVR 2. If NVR 1 was online, the failover connection would have been the Secondary server, NVR 1.



When the Primary and Secondary NVRs come back online, the cameras automatically connect to those servers again.

Recovering Video from Profile G Cameras

Note: The camera's time must be synchronized with the ACC system time to avoid losing video.

After a network connection or server issue is resolved, the system can recover the video from an ONVIF Profile G camera that has an SD card recording video.

You can limit how quickly the server recovers video.

1. In the New Task menu , click **Site Setup**.
2. Select a server, then click **Recovery Configuration**.
3. Enter the following:
    - **Maximum streams to recover:** — The number of streams to recover at a time. The limit is 200 streams.
    - **Limit recovery rate:** — Select this checkbox to limit recovery speed to 1 minute of video over 1 minute of time. If cleared, the system performance may decrease.
4. Click **OK**.

Server Management

View the operational status and configuration of your Avigilon Hardened OS appliance, which is pre-installed with the ACC Server.

1. In the New Task menu , click **Site Setup**.
2. Select a server and click **Server Management** and log in.
3. View the operational status in the web interface for your appliance. Depending on your appliance, this may include the ACC Server name and license, System information, Storage disk, Network uplink ports, and PoE ports. For more information, see the Avigilon appliance documentation.

Devices

Discover, connect, and manage devices.

Discovering a Device

Avigilon and ONVIF-compliant devices that connect to the same network as the ACC Server will be 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 must be manually discovered.

Note: For third-party ONVIF-compliant devices:

- Update the ONVIF-compliant firmware. Some firmware versions may require an update to your ACC Server software.
- Configure the date and time details in the device's web interface.
- After the date and time details are entered, synchronize the device to an NTP server. The ACC Server has a built-in NTP server using IP port 38884 UDP.

1. In the site Setup tab, click .
2. In the top-left corner, click **Find Device...**.
3. Fill the following fields to find a device:
   - **Search From Server:** — Selects a server to connect to.
   - **Search Type:**
     - **IP Address** — Discover the device by IP address or hostname. The device and server's gateway IP must be set correctly for the device to be found.
     - **IP Address Range** — Discover the device by searching within an IP address range.
   - **Device Type:** — Select the device brand.

     Tip: Selecting ONVIF will discover ONVIF compliant devices.

   - **Control Port:** — Enter the device control port. The default port number is 55080.
   - **Apply credentials to all uninitialized devices.** checkbox — Enter the password for the `administrator` username, or create a username and set a new password.

     Note: When discovering Avigilon devices in the factory default state, ACC prompts to enter the password again in the **Confirm Password** field to create login credentials for the uninitialized Avigilon device in the factory default state.

     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**.

Added devices automatically appear in the Discovered Devices list. You can now connect the device to a server.

Connecting a Device

Note: Some features are only available if the site has the required license, and if you have the required user permissions.

To access a device, it must be connected to a server within your site. After a device has been discovered on the network, it can be connected to the server. If you can't see your device, see *Discovering a Device* on page 51.

1. In the New Task menu , click **Site Setup**.
2. Click .
3. To display only devices in uninitialized state, select the **Uninitialized devices** checkbox. The devices are displayed in the Discovered Devices area.
4. In the Discovered Devices area, select the devices and click **Connect...**.

   Tip: You can also drag devices to a server in the Connected Devices area.

   Note: To connect multiple devices, all cameras must use the same connection settings. To ensure you can enter login credentials for uninitialized devices, do not select a mix of non-factory default devices and factory default devices.
5. Select which server will connect to the devices.
6. Connect third-party devices using their native drivers. In the **Device Type:** drop-down list, select the device's brand name. The system may only support one type of driver from the device.
7. In the **Connection Type:** drop-down list, select **Primary**. The device will automatically connect to this server if they are in the same network.

   For more information about Secondary or Tertiary connection types, see *Failover Connections* on page 48.
8. In the **License Priority:** drop-down list, select the license priority — **1** is highest and **5** is lowest.

   This defines the order that devices will connect to the server. If the server does not have enough camera channel licenses, low priority devices may not be connected. Camera channel licenses are only used when the device connects to the server.

9. If the camera supports a secure connection, the **Device Control:** drop-down list is displayed. Select one of the following options:
    - **Secure** — This default protects and secures the camera configuration and login details.
    - **Unsecure** — The camera configuration and login details may be accessible to users with unauthorized access.

    Cameras with a secure connection are identified with the icon.
10. In the **Network Type:** drop-down list, select **LAN** (local area network) or **WAN** (wide area network).

    Select the **WAN** network type to connect cameras on your local network if the Internet Control Message Protocol (ICMP) is blocked or disabled.
11. 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.
12. In the Site View Editor, choose where to display your device in the System Explorer. If it is not displayed, click .
    - If your site includes folders, select a location for the device in the left pane.
    - In the right pane, drag devices to set where they are displayed.
    - If you are connecting multiple devices at the same time, the devices must be assigned to the same location.

    Tip: If your preferred site is not listed, temporarily connect the device to a different server that is connected to the site you want.
13. Click **OK**.

Enabling FIPS Cryptography for Avigilon Devices

When an encrypted connection is selected for your Avigilon device, your device may support a choice of FIPS 140-2 cyptography technologies as an option to the standard OpenSSL cryptographic engine for encrypting communications between the camera and the ACC Server.

The FIPS 140-2 Level 1 option for a supported Avigilon device, switches from OpenSSL cryptography to a FIPS 140-2 Level 1 (software) cryptographic engine. Note that this requires a CAM-FIPS license for the device, to be activated on the ACC site.

CRYPTR FIPS 140-2 Level 3 (tamper protected) cryptography can be enabled by installing a CRYPTR card in a supported Avigilon device. The license for this engine is included with the CRYPTR card, so no CAM-FIPS license is required for this mode.

To select a cryptography option to be used on an Avigilon device:

1. In the New Task menu , click **Site Setup**.
2. Select a device, then click **Network** .
3. Select **FIPS 140-2 Level 1** or **CRYPTR FIPS 140-2 Level 3** from the Encryption Mode: list to enable encrypted communications for the device.

   Enabling FIPS 140-2 Level 1 or CRYPTR FIPS 140-2 Level 3 may cause your device to reboot.

   Important: The CRPYTR card stores the certificates and keys inside its tamper-proof memory. New certificates and keys must be created after installing the CRYPTR card and switching to the CRYPTR FIPS 140-2 Level 3 mode. The Camera Configuration Tool (CCT) can be used to request a new Certificate Signing Request (CSR) from the CRYPTR card and to upload the new certificate after being signed by the Certificate Authority (CA) into the CRYPTR card. For more information, see the *Camera Configuration Tool User Guide*.
4. Click **OK**.

Device Network Settings

Change the IP address of each device after connecting it to ACC site. Then remove the device's default IP address from the server's network ports.

Note: If the device has a Zeroconf IP address of 169.254.x.x with subnet mask of 255.255.0.0, change its IP address to a unique static private IP address in the same IP subnet as the server network interface card (NIC).

For example:

- Server NIC IP Address / Subnet Mask : 192.168.10.10 / 255.255.255.0
- Current device IP Address / Subnet Mask: 169.254.123.140 / 255.255.0.0
- New device IP Address / Subnet Mask : 192.168.10.100 / 255.255.255.0

1. In the New Task menu , click **Site Setup**.
2. Select a device, then click **Network** .
3. Select how the device obtains an IP address:
    - **Obtain an IP address automatically:** — The device will 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:** — Manually assign a static IP address to the device.

      Enter the **IP Address:**, **Subnet Mask:**, and **Gateway:** you want the device to use.
4. Select the **Control Port:** for connecting to the device. This port is also used for manually discovering the device on the network.
5. For cameras, select the **Enable Multicast** checkbox to enable multicast streaming from the device. This is required to set up redundant recording to multiple servers.

   Use the default generated **IP Address:**, **TTL:**, and **Base Port:**, or enter your own values.
6. Click **OK**.
7. For Rialto Video analytics appliances, allow the system to restart the device.

Disconnecting a Device

1. In the site Setup tab, click .
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.

Replacing a Device

Important: Only permanently damaged or defective devices should be replaced.

Note: For regularly scheduled maintenance, instead of replacing the device, disconnect it and connect a temporary replacement. For more information, see *Disconnecting a Device* above and *Connecting a Device* on page 53.

You can replace a device with a similar one and transfer its recorded video in the ACC system.

Replacement devices should have:

- The same username and password as the original device.

  If the credentials are different, you may be locked out of the device.

- The same or similar capabilities as the original device.

  For example, if a fisheye camera malfunctioned, you could install a new fisheye camera in its place. After installation, 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 will appear warped.

The replacement device will take the place of the original device for the following features:

- Recorded and archived video
- Saved Views
- 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. Configure the replacement device with:
   - The same username and password as the original device.
   - A temporary IP Address. This can be changed after the replacement.
3. In the New Task menu , click **Site Setup**.
4. Click the site name, then click **Connect/Disconnect Devices** .
5. In the Discovered Devices area, select the replacement device then click **Replace**.
6. Select the disconnected device you want to replace.
7. 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. Failover level and license priority are maintained.

Always uninstall the original device before replacing it in the ACC system. If you replace a device 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* on page 53.

Rebooting a Device

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

1. In the device Setup tab, click .
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 will automatically reconnect with the server.

Upgrading Camera Firmware

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

While a camera is being upgraded, is displayed beside the camera name. During the upgrade, video will not display.

After the upgrade is complete, the System Explorer will display again and video from the camera will resume.

> **Tip:** You can also upgrade camera firmware manually for cameras that need firmware upgrade. In the Site Health tab under Devices:, the Hardware column shows the firmware version and serial number of devices. The icon is displayed if a device requires a firmware upgrade. To upgrade camera firmware manually, see *Upgrading Your Site Remotely* on page 37 for more details.

Changing from LAN to WAN

The ACC Server will not be able to detect connected cameras in local area network (LAN) mode if the Internet Control Message Protocol (ICMP) on your network is disabled or blocked.

Change the camera's network type to wide area network (WAN) mode before disabling ICMP to keep cameras connected to the server.

Selecting WAN mode will encrypt communications with your device.

1. In the site Setup tab, click .
2. Select the device connections you want to edit from the Connected Devices list.
3. Click **Edit...**.
4. In the Network Type: drop-down list, select **WAN**.
5. Click **OK**.

Device Configuration

Update compression and display settings, add privacy zones, and configure linked devices.

Setting a Device's Identity

In a device's General settings, you can give the device a name, describe the location, and give the device a Logical ID. Logical IDs allow easier keyboard and joystick control.

> **Note:** Certain options are only available if supported by the device.

1. In the New Task menu , click **Site Setup**.
2. Select a device and click .
3. In the **Device Name:** field, enter a meaningful name to easily identify it. By default, the device name is its model number.
4. In the **Device Location:** field, describe the device location.
5. In the **Logical ID:** field, enter a unique number to allow the ACC 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 Logical IDs** is enabled in ACC Client Settings, the device's Logical ID will appear beside the device's name in the System Explorer.

6. To disable the LEDs on a camera, select the **Disable device status LEDs** checkbox. This may be required if the camera is installed in a covert location.
7. Click **OK**.

Changing the Camera Operating Priority

> **Note:** Certain options are only available if supported by the device.

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

Choose what the camera should prioritize during normal operations.

1. In the device Setup tab, click .
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, Unusual Motion Detection, Wide Dynamic Range (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**.

Compression and Image Rate

Use the camera Compression and Image Rate settings to modify the camera's frame rate and image quality sent over the network.

For more compression and image rate options, see *Enabling HDSM SmartCodec™ Technology* on page 63, *Enabling Idle Scene Mode* on page 64, and *Manually Adjusting Video Streams for Recording* on the next page.

> **Note:** Certain options are only available if supported by the device.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Compression and Image Rate** .

   Total Camera Bandwidth: gives an estimate of the bandwidth used by the camera with the current settings.

   > **Note:** For cameras capable of maintaining multiple streams, these settings only affect the primary stream.
3. In the **Format:** drop-down, select the preferred streaming format.

4. In the **Stream Mode:** drop-down, select the number of streams. **Single Mode** (HDSM 2.0) enhances the resolution and quality from applicable cameras, but may reduce performance in integrated third-party software. Use **Dual Mode** in this case. Dual Mode uses a primary and secondary stream to manage bandwidth usage.
5. Move the **Image Rate:** slider to select the number of images per second (ips) you want the camera to stream. A higher Image Rate results in better video quality but more storage and network bandwidth usage.

   For H.265 and H.264 cameras and encoders, the image rate 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.
6. In the **Image Quality:** drop-down list, select an image quality setting. An image quality setting of **1** will produce the highest quality video, require the most bandwidth, and use more storage. The default setting is **6**.
7. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in kilobits per second (kbps).
8. In the **Resolution:** drop-down list, select the preferred image resolution.
   For thermal cameras, use the default resolution for enhanced video quality.
9. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe.

   It is recommended to have at least one keyframe per second. For example, if the Image Rate is 20 images per second (ips), set the Keyframe Interval: to 20. This results in 1 keyframe per second.

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

    When enabled, the lower resolution video stream is used by the HDSM™ technology feature to enhance bandwidth and storage efficiencies.
11. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
12. Click **OK**.

Manually Adjusting Video Streams for Recording

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

For the following cameras, you can manually adjust the primary and secondary video stream or allow the system to use HDSM technology to automatically adjust video bandwidth to meet your requirements:

- 2 MP Avigilon H5A cameras
- 1-3 MP Avigilon H4 HD cameras
- 1-2 MP Avigilon H4 IR PTZ cameras

If local regulations require a specific video stream be recorded or have a minimum resolution, you can manually adjust the settings or use the HDSM Flexible setting.

> **Note:** If a camera is connected to multiple servers (including failover), the following settings must be the same at each server connection. Otherwise, settings may overwrite each other, and the camera will not record with the correct stream settings.

1. In the New Task menu, click **Site Setup**.
2. Select a camera, then click **Compression and Image Rate**.
3. Select the **Enable Low Bandwidth Stream** checkbox.
4. In the **Recording Profile:** drop-down list, select one of the following:
   - **Record High Bandwidth** — *Third-party ONVIF-compliant cameras only*. Records video on the high bandwidth stream. Live video can use either the high or low bandwidth stream.
   - **Record Low Bandwidth** — *Third-party ONVIF-compliant cameras only*. Records video on the low bandwidth stream. Live video can use either the high or low bandwidth stream.
   - **HDSM Auto** — *Applicable Avigilon cameras only*. Records video from both the high and low bandwidth streams and uses HDSM technology to automatically adjust bandwidth and storage.
   - **HDSM Flexible** — *Applicable Avigilon cameras only*. Records video from both the high and low bandwidth streams and uses HDSM technology to automatically adjust bandwidth and storage, but allows manual configuration of the low bandwidth stream for live and recorded video.
   - **Manual** — *Applicable Avigilon cameras only*. Records video using the manually configured settings.
5. Adjust the stream settings as needed. For more information, see *Compression and Image Rate* on page 60.

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

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

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

7. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
8. 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 HDSM SmartCodec™ Technology

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. Higher quality image is retained for non-static objects of interest in the foreground while reducing bandwidth for static objects in the background. When there is no motion in the scene, the HDSM SmartCodec feature switches the camera into idle scene mode to increase bandwidth savings.

The 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 Events* on page 123.

1. In the New Task menu, click **Site Setup**.
2. Select a camera, then click **Compression and Image Rate**.
3. Select the **Enable HDSM SmartCodec** checkbox.
4. If it is not displayed, click to display the HDSM SmartCodec settings.
5. In the **Bandwidth Reduction:** drop-down list, select Low, Medium, High, or 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 involves more movement, 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in this mode.

11. 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.

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

Enabling Idle Scene Mode

> **Note:** Only available to cameras that support this feature.

Idle scene mode records video at a different frame rate and quality if there are no motion events detected in the scene. This lowers the bandwidth and storage used when the scene is idle. When motion events are detected, the camera automatically switches back to standard streaming mode.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click .
3. Select the **Enable Idle Scene Mode** checkbox.
4. 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.
5. Move the **Image Rate:** 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.
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 and Display Settings

> **Note:** Certain options are only available if supported by the device.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Image and Display** .
3. Use the focus controls to focus the camera. For more information, see *Zooming and Focusing the Camera Lens* on page 114.
4. Click to toggle the Auto Contrast Adjustment. This change does not affect recorded video or video displayed in other views. By default, Auto Contrast Adjustment is off.
5. If the camera supports day/night control, select one of the following options from the **Day/Night Mode:** drop-down list:
   - **Automatic** — The camera controls the infrared (IR) 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 monochrome and the IR cut filter is enabled.

   Note: The camera bandwidth may vary depending on the mode.
6. Select the **Disable IR filter in Night Mode** check box to disable the IR filter when Day/Night Mode: is set to Night Mode. If the IR filter is disabled, the camera will stream in color.
7. If available, move the:
   - **Day/Night Threshold:** slider to set the exposure value (EV) when the camera changes from day to night mode.
   - **Night/Day Threshold:** slider to set the exposure value (EV) when the camera changes from night to day mode.

   Note: The H5 Hardened PTZ camera supports the installation of a narrow spot illuminator that can be controlled from the ACC Client. See *Using the H5 Hardened PTZ Illuminator* on page 166.
8. 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: Maximum Exposure:, **Maximum Gain:**, and **Priority:** control low light behavior.

Option	Description
Synchronize Image Settings with All Heads	Apply the same image settings to all camera heads. Zoom and focus settings must be set individually.

Option	Description
Exposure:	Let the camera control the exposure by selecting **Automatic**, or set a specific exposure rate. Increasing the manual exposure time may affect the image rate.
Iris:	Let the camera control the iris by selecting **Automatic**, or manually set it to **Open** or **Closed**.
Maximum Exposure:	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:	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:	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:	Select **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera maintains 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 maintains the exposure setting as the priority and overrides 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, reduce the effects 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 checkbox to enable automatic color adjustments through Wide Dynamic Range (WDR). This allows the camera to adjust the video image

Option	Description
	to accommodate scenes where bright light and dark shadow are clearly visible.
Enable Adaptive IR Compensation	Select this checkbox to enable automatic IR adjustments through Adaptive IR Compensation. This allows the camera to automatically adjust the video image for saturation caused by IR illumination.
Saturation:	Move the slider to adjust the video's color intensity until the video image meets your requirements.
Sharpening:	Move the slider to adjust the video sharpness to make the edges of objects more visible.
Image Rotation:	Change the rotation of captured video by 90, 180, or 270 degrees clockwise.
White Balance	Control white balance settings to adjust for differences in light. To let the camera control the white balance, select **Automatic White Balance**, or select **Custom White Balance** to manually set the **Red:** and **Blue:** settings.

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

9. Click **OK**.

Image Dimensions

> **Note:** This feature is only available for JPEG2000 cameras.

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.

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**.

Privacy Zones

You can block the camera's field of view to protect privacy and personal information in live and recorded video. A privacy zone is like blind spot for a camera. The area covered in the privacy zone cannot be used for viewing, recording, motion detection, and analytics.

Adding a Privacy Zone

1. In the New Task menu , click **Site Setup**.
2. Select a camera and click **Privacy Zones** .
3. Click and resize the green privacy box.
4. Click **OK**.

Editing Privacy Zones

1. In the New Task menu , click **Site Setup**.
2. Select a camera and click **Privacy Zones** .
3. Click on a privacy zone and adjust the green box, or click to delete the zone.
4. Click **Apply** to refresh the view and **OK** to finish editing.

Configuring PTZ

> **Note:** Certain options are only available if supported by the device.

Use the camera General settings to enable and configure the motorized Pan, Tilt, Zoom (PTZ) for Avigilon cameras. PTZ devices are connected to Avigilon cameras through RS-485 inputs.

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

1. In the camera Setup tab, click .
2. Select the **Enable PTZ controls** checkbox.

   > **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 162.

Configuring Digital Inputs

FOR STANDARD AND ENTERPRISE EDITION

> **Note:** Certain options are only available if supported by the device.

1. In the device Setup tab, click .
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**.

Configuring Digital Outputs

FOR STANDARD AND ENTERPRISE EDITION

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 175.

> **Note:** Certain options are only available if supported by the device.

1. In the device Setup tab, click .
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 the Device Microphone

FOR STANDARD AND ENTERPRISE EDITION

Use the Microphone settings for any microphone 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:** Certain options are only available if supported by the device.

1. In the device Setup tab, click .
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.
4. Enter a name for the microphone. Default names are 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.

   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**.

Configuring the Device Speakers

FOR STANDARD AND ENTERPRISE EDITION

Use the Speaker settings for speakers connected to a device or Avigilon video analytics appliance. You can also link the audio output to other devices.

Speakers must be connected to the device and a microphone must be connected to your local ACC Client.

> **Note:** Certain options are only available if supported by the device.

1. In the device Setup tab, click .
2. If multiple **Speaker Outputs:** are listed, select the one you want to edit.
3. Click the **Speaker Off** toggle to enable audio broadcasting. Speakers connected to the device will broadcast audio from the microphone that is connected to the local ACC Client.
4. Select the **Record:** checkbox 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**.

Video Intercom

FOR STANDARD AND ENTERPRISE EDITION

Before an Avigilon Video Intercom device can start a call session, you need to enable the microphone and speaker on the device in the ACC Client software, see *Configuring the Device Microphone* on page 70 and *Configuring the Device Speakers* on the previous page.

Adding Rule to Answer Calls

Note: Push notifications are available for ACC Mobile 3 users using ACC Server version 7.6 or later. If you upgraded from a previous version of the ACC Server software, remove and then re-add users or groups in your Video Intercom rule to enable push notifications.

Tip: To have a call open up in one large image panel, create a Saved View with one image panel. Select this View when specifying the rule actions.

To authorize ACC operators to receive calls from a Video Intercom, create a rule.

The following example is a rule which specifies that when a call button is pressed on any intercom device, multiple users receive the video call until one answers.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Rules** .
3. Click **Add**.
4. Select the **Device Events** > **Digital Input Activated** checkbox, then click **any digital input**.
5. Select **Any of the following digital inputs:** and select the call button digital input for each Avigilon Video Intercom device.
6. Click **OK**, then click **Next**.
7. Under Monitoring Actions, select the **Open a saved view** and **Video intercom call** checkboxes.

   Note: If the device uses the Session Initiation Protocol (SIP) to send calls directly to a phone, do not select the **Video intercom call** checkbox.
8. Click the blue text to specify the Saved View, linked cameras, and users.
9. Click **OK**, then click **Next**.

For instructions on how to add and edit rules, see *Adding a Rule* on page 126.

For information on answering calls, see *Using Video Intercom* on page 174.

If you experience voice echoing during calls, configure the intercom in the device's Web Interface to ignore the operator's voice. We recommend having operators use a headset.

Recording Video during a Call

To conserve video storage, use recording schedule templates to record only when a the call button is pressed.

1. In the New Task menu , click **Site Setup**.
2. Click the server, then click **Recording Schedule** .
3. Click **Add Template**.
4. Enter a name and specify the **Digital Inputs** recording schedule. This specifies when to record video if the call button is pressed.

   For more information, see *Recording Schedule Templates* on page 47.
5. Ensure the template is selected in the Templates: list.
6. 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 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 46.
7. Click **OK**.

Avigilon Presence Detector™ Sensors

The Avigilon Presence Detector (APD) sensor is a short-range radar that detects fine motion up to 9 meters, or 30 feet. These devices complement cameras to detect breathing or heartbeats that a camera may not detect reliably. For locations where cameras are impractical or not allowed, the APD™ sensor can indicate loitering.

The APD sensor does not use a camera channel when connecting to an ACC site.

The APD sensor works by detecting a person in range and sending a Presence Detected notification. Presence is indicated in the event timeline, and the system starts counting down the preconfigured Dwell Time. If the person moves out of range, a Presence Ended event is recorded. If the person lingers in range too long, a Presence Dwell Time Exceeded notification is triggered. Once they finally move, the Presence Dwell Ended and Presence Ended event notifications are sent. To review these presence events, see *Searching Events* on page 182.

Note: The APD sensor only detects the presence of moving objects within its range. It cannot identify or count any objects detected.

1. In the device Setup tab, click .
2. Move the **Range:** slider to define the range within which motion can be detected. Enter the distance from the sensor to the furthest edge of the floor or space. Accurately setting range is critical to avoid detecting motion on the other side of walls or barriers, or detecting a specific distance in a lobby or large space.
3. Set the **Dwell Time:** for define how long the APD sensor must detect motion before a Presence Dwell Time Exceeded event is generated. Longer dwell times are best for detecting loitering, so that normal activities in range do not generate events. Shorter dwell times are best for detecting activity in restricted areas.
4. Move the **Sensitivity:** slider to define how sensitive the APD sensor is to fine movement, such as breathing. Lowering the sensitivity helps prevent false detections.

Analytics

Configure and optimize video analytics settings for cameras and Avigilon video analytics appliances.

Enabling Analytics

You can enable and disable server-based analytics on cameras throughout your site to manage the server's analytics load.

1. In the New Task menu , click **Site Setup**.
2. Select a server, then click **Server Analytics** .

   Important: If your site is connected to an AI Appliance to provide analytics processing on the video streams from non-analytics cameras, expand the site and then click on the **Server Analytics** .
3. Select an analytics feature tab and then select the cameras to enable the feature on.

   Only cameras that you have access to that have the prerequisite analytics enabled are displayed in each tab.

   Tip: If you do not see one of the tabs, check that you have the required license. Appearance Search and No Face Mask Detection need ACC Enterprise, while Face Recognition requires a separate license.

As you enable (or disable) analytics for cameras, the bars at the bottom update to display the server's capacity. The percent usage of each analytics feature is displayed using the color of the analytics feature tab.

To exit the Server Analytics panel, click **Close**.

Configuring Data Retention

To set how long the ACC system stores appearance signatures, see *Identity Data Retention* on page 41.

Disabling Analytics

You can enable and disable server-based analytics on cameras throughout your site to manage the server's analytics load.

1. In the New Task menu , click **Site Setup**.
2. Select a server, then click **Server Analytics** .
3. In the **Server Analytics** panel (for each server), select an analytics feature tab and then select the cameras to disable the specific feature on those cameras.

   > **Tip:** You can either individually deselect specific cameras to disable an analytics feature on them or click **Clear All** to deselect all cameras at once for a specific feature. To fully disable server-based analytics for the entire site, including the storage of appearance signatures, ensure that all cameras are disabled in each of the feature tabs within the **Server Analytics** panel.

4. For multi-server sites, repeat the above steps.

As you enable (or disable) analytics for cameras, the bars at the bottom update to display the server's capacity. The percent usage of each analytics feature is displayed using the color of the analytics feature tab.

To exit the Server Analytics panel, click **Close**.

Configuring Data Retention

To set how long the ACC system stores appearance signatures, see *Identity Data Retention* on page 41.

Configuring Camera Analytics

Cameras with Classified Object Detection video analytics and cameras connected to Avigilon analytics appliances can be configured to improve classified object detection accuracy.

> **Tip:** You can configure these settings for multiple cameras using the Camera Configuration Tool available on **avigilon.com/support**.

> **Note:** Certain options are only available if supported by the device.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Settings** .
3. Edit the analytics settings. Each setting is described below.
4. Click **Apply**.

Next, you can enable self-learning and configure analytics events. For more information, see *Self-Learning* on page 79 or *Analytic Events* on page 118.

Analytic Settings

Setting	Description
Camera Type:	Select the type of camera that has been connected. • **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.
Analytics Scene Mode:	Select the location that best describes where the camera is installed. • **Outdoor** — suitable for most outdoor environments. This setting optimizes the camera to identify vehicles and people. • **Large Indoor Area** — only detects people and is optimized to detect people around obstructions, like chairs and desks, if the head and torso are visible. • **Indoor Overhead*** — optimized for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera field of view. Any movement is assumed to be human. Use in areas with limited space but with high ceilings, or to monitor doors. Do not use with the Avigilon Appearance Search feature, Face Recognition, the Self-Learning feature, or to detect people traveling against the crowd. • **Outdoor High Sensitivity*** — optimized to run with higher sensitivity for detecting people and vehicles in challenging outdoor scenes. This option may generate more false positives. Only use this option if you require the system to be more sensitive than the Outdoor setting. • **Long Range Night*** — prioritizes outdoor long-range object detection at night over object classification and tracking during the day. Uses external IR illumination rather than built-in IR illumination from the camera. Object classification and tracking accuracy during the day is reduced compared to other outdoor modes. Available for H4A cameras only.

Setting	Description
	* These modes are not available for H5A cameras. **Note:** The H5A Fisheye camera does not support video analytics when installed on a wall or on a floor. It must be installed on a ceiling to support video analytics. When a camera is installed on a ceiling, also ensure that the camera View Perspective: is set to Ceiling. For more information, see *Dewarping Fisheye Displays* on page 113.
Enable Noise Filter	Select the checkbox if the camera is too sensitive and falsely detects motion as classified objects.
Display Classified Objects	Select the checkbox to display bounding boxes around classified objects in recorded video.
Enable Tampering Detection	Select the checkbox to enable tampering detection. If cleared, the device will no longer send tampering events.
Sensitivity:	Enter a value between 1-10 to select how sensitive a camera is to tampering events. Tampering is 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.
Trigger Delay:	Enter a value between 2-30 to define how many seconds the camera will wait before sending tampering events. The default value is 8. 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.
Enable Self Learning	Select the checkbox to enable self-learning. If you clear this checkbox, more classified objects may be falsely detected.

Configuring Skin Temperature Thresholds

Configure the thresholds for detecting skin temperatures on faces in live video.

Note: The following button is supported only for the Avigilon H4 Thermal Elevated Temperature Detection camera.

1. In the New Task menu , click **Site Setup**.
2. Select a thermal camera and click **Temperature Settings** .
3. In the **Temperature Settings** dialog box, edit as needed:
   - **Elevated Temperature Threshold (°C)** or **(°F)**: The threshold above which a person may need further screening. Default is the calibrated value from the thermal camera.

     If an elevated temperature at or above the threshold is detected, and a red bounding box are displayed over the face in the live video.

   - **Lower Temperature Threshold (°C)** or **(°F)**: The threshold below which a person may need further screening. Default is the calibrated value from the thermal camera.

     If a lower temperature at or below the threshold is detected, and a white bounding box are displayed over the face in the live video.

   Any temperature detection that falls between the specified thresholds is considered within the acceptable range. If a temperature is detected, and a green bounding box are displayed over the face in the live video.
4. Click **Restore Defaults** to restore the calibrated value from the camera, if needed.
5. Click **OK** to apply the settings and exit, or click **Apply** to apply the settings without exiting.

Next, you can configure analytics events. For more information, see *Analytic Events* on page 118.

Toggling Degrees Celsius and Fahrenheit

Toggle the temperature unit that displays next to the bounding box on faces in live video and in related temperature detection activity events.

1. In the Windows Control Panel, select **Region** and **Additional settings**.
2. Select the unit in **Measurement system**.
3. Click **OK**. The temperature unit takes effect immediately.

Unusual Motion and Unusual Activity

Unusual Motion Detection and Unusual Activity Detection both detect unusual events, but use different algorithms to determine what is unusual.

	Unusual Motion	**Unusual Activity**
Algorithm:	Analyzes motion-based activity and learns to identify rare events	Analyzes unusual events performed by detected people or vehicles
Supported on:	Cameras with Unusual Motion Detection	Cameras with Next-Generation Video Analytics
Video Analytics Mode:	Unusual Motion	Classified Object
Available in:	Timeline, Focus of Attention interface, Event search, Rule triggers	Timeline, Focus of Attention interface, Event search, Rule triggers

	Unusual Motion	Unusual Activity
Initial Learning Period:	2 weeks, but events are reported while the device is learning	1 week, but events are reported while the device is learning

Video Analytics Mode

If your device supports Unusual Motion Detection, you can enable Classified Object or Unusual Motion mode for a video analytics device.

> **Tip:** If your device is connected to a server that provides Classified Object Detection, you can enable both analytics modes simultaneously. In the device Setup tab enable Unusual Motion mode. In the server Setup tab enable server-based analytics. See *Enabling Analytics* on page 74.

1. In the New Task menu , click **Site Setup**.
2. Select a device, then, click **General** .
3. In the **Video Analytics Mode:** drop-down list, select one of the following:
   - **Classified Object** — Detect and classify people or vehicles.
   - **Unusual Motion** — Detect unusual pixel motion based on typical speed and direction of movement in a scene.
   - **None** — Do not use analytic capabilities.
4. Click **OK**.

Self-Learning

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. Enable self-learning for all video analytic devices, except if:

- People or vehicles are not expected in the device's field of view.
- Objects move at different heights. For example, overhead pedestrian bridges, train platforms, hills and underpasses.
- The device is in Indoor Overhead mode. Self-learning is not used, even if enabled. All detected objects are classified as people. The Progress Bar will display 100% and cannot be reset.

For information on enabling self-learning, see *Configuring Camera Analytics* on page 75.

Self Learning Progress Bar

A progress bar displays in the device's Analytics Settings. The following table describes each phase of 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.

Learning progress depends on the amount of activity in the scene. Approximately 200 high-confidence detections are required for optimal self-learning calibration. If the camera is moved or adjusted, reset it's learning progress. For more information, see *Resetting the Learning Progress* below.

Self-learning requires full-body detections. The learning progress may never reach 100% if only partial bodies are detected in the device field of view. However, if the upper half of the body moves as expected, Classified Object Detection will not be affected.

Teach By Example can be used, even if the Self Learning progress bar is not at 100%.

Resetting the Learning Progress

Note: Always reset the learning progress for Self Learning, Unusual Activity Detection and Unusual Motion Detection after a camera is physically moved or adjusted, or if the focus or zoom level is changed. Any change in the camera's field of view affects the video analytic results.

Cameras with Avigilon self-learning video analytics, Unusual Activity Detection, or Unusual Motion Detection learn the scene.

When the learning progress is reset, all learning data is cleared and the device to re-learns the scene. This prevents missed and false detections based on old data.

1. In the New Task menu , click **Site Setup**.
2. Select a device, then click **Settings** .
3. Under the learning progress bar, click **Reset**.
4. Click **Yes**.

   The learning progress is reset.

Tip: If you reset the Self Learning progress, you do not need to reset the Unusual Activity or Unusual Motion learning progress. If you disable the Self Learning feature, we recommend resetting the Unusual Activity or Unusual Motion progress.

Teach By Example

Teach By Example helps Avigilon video analytics cameras learn the scene to improve classified object detection accuracy.

Teach By Example collects feedback by applying assigned Teach Markers in recorded video. While any user can assign the markers, administrators decide which markers are most useful considering the environment, lighting, and field of view for each camera. Teach By Example is not required for video analytics cameras, but will help reduce the number of false alarms after self-learning is complete or disabled.

Assigning Teach Markers

True and False markers can be applied by operators. The easiest way to apply these markers is to conduct a classified motion search.

1. In the New Task menu , click **Motion** .
2. Select the camera you want to teach and select **Classified Object Motion**.
3. Adjust the search region of interest to be slightly larger than the region of interest typically used for analytic events from that camera.
4. Click **Search**.
5. Select a result and play the event.

   When motion is detected, a bounding box will appear around the detected motion.
6. Click inside the bounding box and mark the motion as either a **True** or **False** person or vehicle. Teach markers do not differentiate vehicle types.
7. Repeat until at least 30 true and 30 false markers have been assigned.

   Tip:
   - Include True and False examples from scenes with different lighting.
   - To find False markers, search for events longer than 2 seconds with a confidence level greater than 20%.

Editing and Removing Teach Markers

1. In the New Task menu , click **Site Setup**.
2. Select a video analytics camera, then click **Teach By Example** .
   - Click inside the bounding box to change if the marker is True, False, or Not Used to remove the marker.
   - Click **Clear All Markers** to remove the assigned markers. This will not remove markers that were already applied to the camera.

- Click **Restore to Factory Default** to remove all applied markers.

> **Note:** Always restore factory default settings after a camera is moved or adjusted, or if the zoom or focus have changed.

3. Apply the teach markers or close the Teach By Example tab.

Applying Teach Markers

After at least 30 True and 30 False markers are assigned, they can be applied. Once applied, the teach markers will remain on the camera even if the camera changes servers. Each camera can have a maximum of 200 True and 200 False markers.

1. In the New Task menu , click **Site Setup**.
2. Select a camera with assigned markers and click **Teach By Example** .
3. Click **Apply**.

The assigned markers list is empty because the markers have been applied to the device. You can verify that the device was updated by checking the Teach Marker status.

Teach Marker Status

Review the camera's Teach Marker status to know when they were last applied or restored to factory default.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Settings** .
3. In the Self Learning section, the **Teach Markers Applied:** area displays the date that markers were last applied or if the camera is in its Factory Default state.

> **Note:** For cameras connected to a Rialto video analytics appliance, the Teach Markers Applied: field will display **Unknown**.

Disabling Tampering Detection

You can disable tampering notifications for cameras with Classified Object Detection.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Settings** .
3. Clear the **Enable Tampering Detection** checkbox.
4. Click **Apply**.

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, ensure the cameras are physically connected to each camera channel before connecting the appliance 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.

1. In the New Task menu , click **Site Setup**.
2. Select the appliance, then click .
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 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. Configure the available analytics settings. For more information, see *Configuring Camera Analytics* on page 75.
5. Click **Apply** to save your settings.
6. If you are prompted, allow the device to reboot.

   You can now enable self-learning or configure video analytic events.

   For more information, see *Self-Learning* on page 79 or *Analytic Events* on page 118.

Users, Groups, and Permissions

Manage users, permission groups, and set up your corporate hierarchy.

Tip: Changes to users, groups, and permissions can be viewed in the Site Logs.

Best Practices for Large Organizations

FOR ENTERPRISE EDITION

When you have a large organization, you need detailed access permissions to manage system use.

The Avigilon Control Center software has several ways to manage large organizations.

- **Active Directory Support** — Synchronize with Windows Active Directory to quickly import users. For more information, see *Importing Active Directory Users* on the next page.
- **Group Privileges:** — Users are added to at least one group to define their access to features and devices within the system. Users with the Setup user and group settings permission can create and edit groups. For more information, see *Adding Groups* on page 89.

These features help manage groups across your system:

- **Corporate Hierarchy** — Create a Corporate Hierarchy to assign group control and access. For more information, see *Corporate Hierarchy* on page 95.
- **Site Families** — Connect multiple child sites to an Enterprise parent site and control group settings from the parent site. For more information, see *Site Families* on page 97.

Best Practices

We recommend the following practices for maintaining a secure system:

- Use a strong administrator password to protect your site from unwanted access.
- Add a secondary ACC Administrator user with identical privileges as a backup. A secondary, well guarded user can maintain access if the primary account's password is forgotten or the site is compromised. Create a secondary Administrator user on your Windows server as well.
- Assign all groups a rank. Any groups that are Unranked will have access over all other groups. The default administrators group is Unranked automatically, but you are free to create a group for admins. For more information, see *Corporate Hierarchy* on page 95.
- Limit the number of users in the default Administrator group. The Administrator group should be used only for system maintenance.
- Consult your Information Security office or IT administrator for password strength and expiry recommendations.
- Confirm that 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.
- Check group access permissions after a new server has merged into the site.
    - If groups have the same name, the previous site settings are used and users from both the site and server are added to the group.
    - New groups to the site and server automatically receive access to all connected devices.

- Always check access permissions after new users and groups settings are imported into the site.
    - Groups with the same name with share import settings, adding users from both the import file and the current site are added to the same group.
    - Groups added from the import file automatically gain access to all new devices that were added since the settings were exported.

Importing Active Directory Users

FOR ENTERPRISE EDITION

Importing Active Directory groups and users allows users to log in with their existing credentials. Members of an initially imported Active Directory group are automatically added as users to the site.

Changes to users in the Active Directory are synchronized manually with groups in the ACC software.

Note: User information, including credentials, is maintained by the Active Directory. You can only disable an imported user, assign the user to a group, or configure the user's Login Timeout in the ACC software.

Important: If your site is connected to an ACM appliance, enabling Active Directory will disable previously imported ACM roles. To use Active Directory, an ACM administrator must configure remote authentication from external domains in the ACM appliance first. For more information, see the ACM help files.

Enabling the Active Directory

Before you can import users and groups, you need to enable and log in to Active Directory.

Note: The default IP port is 389 UDP. Ensure that this IP port is open between each ACC Server and all Active Directory servers used for ACC authentication.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. In the External Directory tab, select **Active Directory** from the drop-down list.
4. Click **Edit**.

- **Windows only sites:** Select the **Use ACC service account** checkbox to use the ACC service account credentials, or enter your domain credentials.

  The ACC service account is either the Local System account or the account specified in Windows Service under the Avigilon Control Center Service Properties in the Log On tab on the computer running the ACC Server software.

- **Avigilon Hardened OS appliances only sites:** Enter your domain, username (for example, `john.smith@domain.com`), password, and domain controller URL (for example, `ldap:\\dc-server.domain.com`).
- **Mixed Windows and Avigilon Hardened OS appliance sites:**
  - In the Windows server settings, enter your username (for example, `john.smith@domain.com`) and password. Clear the **Use ACC service account** and **Enable nested groups** checkboxes.
  - The Avigilon Hardened OS appliance Active Directory settings can be left blank. After the Avigilon Hardened OS appliance is added to the site, it will inherit the site settings. If Active Directory settings were configured on the appliance, the appliance domain must match the domain of the site. For more information, see *Multiple Server Sites* on page 18.

> **Tip:** The validity of the currently stored Active Directory credentials in ACC may be in an *Unknown* or *Invalid* state. This may happen because of administrative changes to Active Directory user accounts or incorrect user credentials. To validate the currently stored credentials on the server, click **Check Credential**. If the credentials are invalid, click **Edit** and enter valid credentials again.

5. Click **OK**.

Nested Groups

FOR WINDOWS SERVERS ONLY

With ACC version 7.8 or later, nested Active Directory groups are imported by default if the Windows user is part of the parent group.

However, some Active Directory group configurations are very complicated and even recursive. If you experience long log in times or nightly directory sync errors, you may need to disable nested group support.

- In the External Directory tab, clear the **Enable nested groups** checkbox.

Importing Groups

After Active Directory is enabled, you can import groups and nested groups from trusted domains within the same forest. All users in the initially imported group are automatically imported, and will belong to the permissions group.

1. Click **Add Group**.
2. Select a permission group template and click **OK**. You can change the group's permissions later.
3. To import a group from a different domain, click **Locations...** and select a domain.
4. Enter the name of the Windows group or click **Advanced...** to search for the group.
5. Click **OK**. All users in the group are automatically imported.
6. Update the imported group's settings and permissions. For more information, see *Adding Groups* on page 89.

Importing Users

After Active Directory is enabled, you can import users from trusted domains within the same forest.

1. Click **Add User**.
2. To import a user from a different domain, click **Locations...** and select a domain.
3. Enter the name of the Windows user or click **Advanced...** to search for the user.
4. Click **OK**.
5. Assign the imported user to an ACC group:
    a. In the Users tab, select the imported user and click **Edit User**.
    b. Select the **Member Of** tab.
    c. Select the access group checkboxes to assign the user to that group.
    d. Click **OK**.

Adding a User

Add users to monitor and manage your site.

You can also add users through Active Directory. Ensure all user accounts are unique. For more information, see *Importing Active Directory Users* on page 85.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. Click **Add User**.
4. Complete the User Information area.
5. Select the **Disable user** checkbox to create an account, but prevent access.
6. In the Login Timeout area, select the **Enable login timeout** checkbox 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.

7. Select the **Member Of** tab to assign the user to a group.
    a. Select access group checkboxes to assign the user to that group.

    > **Tip:** Click an access group to display the group's privileges and access rights.

    b. Return to the **General** tab.
8. In the Password area, complete the following fields:
    - **Password:** — The password the user will use to gain access.
    - **Confirm Password:** — Re-enter the password.

      The password must meet the minimum strength requirements, defined by how easy it is for an unauthorized user to guess.

      > **Tip:** 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** — The user must replace the password after the first login.
    - **Password Expiry (Days):** — The number of days before the password must be changed.
    - **Password never expires** — The password will never need to be changed.
9. To enable access to Avigilon Cloud Services, ensure the correct email address is entered and select the **Connect** checkbox.

    The user will receive an email invitation after the site is connected to the Avigilon Cloud Services.
10. Click **OK**.

Editing and Deleting a User

Edit and delete users as needed. If a user has access to more than one site, the changes to the user need to be made on each site.

> **Note:** You cannot edit or delete users that are above, or in the same ranked group as you. You cannot edit your own user account unless you belong to an Unranked group.
>
> You can only change the Login Timeout, assign a group, or disable users imported from an External Directory. All other settings are maintained by the External Directory.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. 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 options, see *Adding a User* on page 87.
    - If Two-Factor Authentication is enabled, and a user has lost their verification code, click **Reset Two-Factor Key**. On their next login, a new QR code will display.
    - To delete the user, click **Delete User**.

Adding Groups

Groups define which features users can access. You can further define privileges by assigning each group a rank, and setting rules on what a group can access. For more information, see *Corporate Hierarchy* on page 95.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. In the Groups tab, click **Add Group**.
4. Select an existing group to use as a template for your new group, then click **OK**.
5. Add the following details in Edit Group:
    a. Enter a group name.
    b. Select a rank from **Rank:**. To edit or view the entire Corporate Hierarchy, click .
    c. Move the **Min Password Strength:** slider to define how strong each user's password must be.
    d. To enable Two-Factor Authentication, select the **Required** checkbox.

    Users will need an authenticator app on their mobile device to scan a QR code before they can log into a site.

    Ensure your servers sync to a real-time source. If the time on the user's device does not match, they will not be able to log in. Verification codes are only valid within 5 minutes.

    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: Users with Two-Factor Authentication enabled will not be able to use the ACC Mobile 3 app or the ACC Virtual Matrix software.

    e. To enable Emergency Privilege Override, select the **Enabled** checkbox. For more information,

see *Emergency Privilege Override* below.

f. Select the required **Group Privileges:** and **Access Rights:** for the group. For more information, see *Group Privileges* on the next page.

6. Click **Enable Dual Authorization** to configure Dual Authorization settings. When enabled, users cannot review recorded video without permission from the authorizing group.
   a. Click the toggle to enable Dual Authorization. Click again to disable Dual Authorization.
   b. Select which groups can authorize users.
   c. Click **OK**.
7. In the **Members** tab, add users to the group.

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

   a. Click **Add User**.
   b. Select the users from this site to include in this group or use Search... to refine results.
   c. Click **Add**. The users are added to the Members list.
8. Click **OK** to save the new group.

Editing and Deleting a Group

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

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. In the Groups tab, select a group and do one of the following:
   - To edit the group, click . For details about the configurable options, see *Adding Groups* on the previous page.
   - To delete the group, click .

     Default groups cannot be deleted.

Emergency Privilege Override

Emergency Privilege Override is a group permission that gives operators access to the following privileges without needing dual authorization:

- View high-resolution images
- View live images
- View recorded images
- View images recorded before login
- Use PTZ controls
- Broadcast to speakers
- Listen to microphones

Create a new group to manage who has Emergency Privilege Override permissions.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. In the Groups tab, click **Add Group**.
4. Select an existing group to use as a template for your new group, then click **OK**.
5. Next to Emergency Privilege Override:, select the **Enabled** checkbox.
6. Enter a name and in the Members tab, select users to add to the group.
7. Click **OK** to save the group.

Users assigned to groups with this privilege can enable Emergency Privilege Override. For more information, see *Enabling Emergency Privilege Override* on page 191.

Group Privileges

To learn how to add a group, see *Adding Groups* on page 89.

Group Privileges	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.
Receive live events with identifying features	Allows users to receive the following alarms and live events, if configured: • Face Watch List Matches • LPR
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.
Export images	Allows users to export recorded images.
View images recorded before login	Allows users to view images recorded before

Group Privileges	Description
	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.
Licensed search for identifying features	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.
View Maps	Allows users to view Maps if applicable.
Manage maps	Allows users to add and edit maps and Maps if applicable.
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 audio from a camera microphone.
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 compression and image rate settings	Allows users to edit the Compression and Image Rate dialog box.
Setup dewarping settings	Allows users to edit the Dewarping dialog box.
Setup image dimension settings	Allows users to edit the Image Dimensions dialog

Group Privileges	Description
	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 camera's microphone settings for listening to audio.
Setup speaker settings	Allows users to edit the camera's speaker settings for broadcasting audio.
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 general settings	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 Privileges	Description
Setup LPR settings	Allows users to edit the License Plate Recognition dialog box.
Setup LPR watch lists	Allows users to edit license plate watch lists.
Setup external notification settings	Allows users to edit the External 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.

Resetting a Password

Only administrators can reset a user's password.

> **Note:** To maintain strict security, administrator passwords can only be reset by Avigilon Technical Support.

1. In the New Task menu, click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. In the **Users** tab, double-click a user.
4. Click **Change Password** and enter a new password.
5. Click **OK** to save the new password.

> **Tip:** Select the **Require password change on next login** to let the user update their credentials after they log in.

6. Click **OK**.

Managing User Connections

If an operator leaves themselves logged in, or if there are too many users logged in at one time, you can log them out.

1. In the New Task menu, click **User Connections**.
2. Select a site from the System Explorer to display all current users on the right.
   - Users that share login credentials are separated by User Name and Machine Name
   - The Login Duration displays how long that user has been logged in to the site.
3. Select a user to log out and then click **Log Users Out**.

Corporate Hierarchy

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

Rank groups to help define what group members 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. For more information, see *Ranks* on the next page.

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. For more information, see *Site Families* on page 97.

Setting Up a Corporate Hierarchy

Assign ranks to users and groups to establish a Corporate Hierarchy.

Ranks are also assigned to sites when organized into families. For more information, see *Site Families* on page 97.

1. In the New Task menu, click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. In the Group tab, select a group and click **Edit Group**.
4. To create a rank, click .

   If you have not yet created a Corporate Hierarchy, you will be prompted to create one. Click **Yes**.

   The default and highest rank is Global. It can be renamed, but not deleted.
5. Select a rank, then click **Add** to add a subordinate rank below it in the hierarchy.

6. To rename a rank, double-click the name and enter the new one. Clicking outside the text field will save the change.

   > **Note:** Ranks cannot be moved within the Corporate Hierarchy.

7. To delete a rank, select it and click **Delete**. Any subordinate ranks will be deleted.
8. Click **OK** to save your changes.

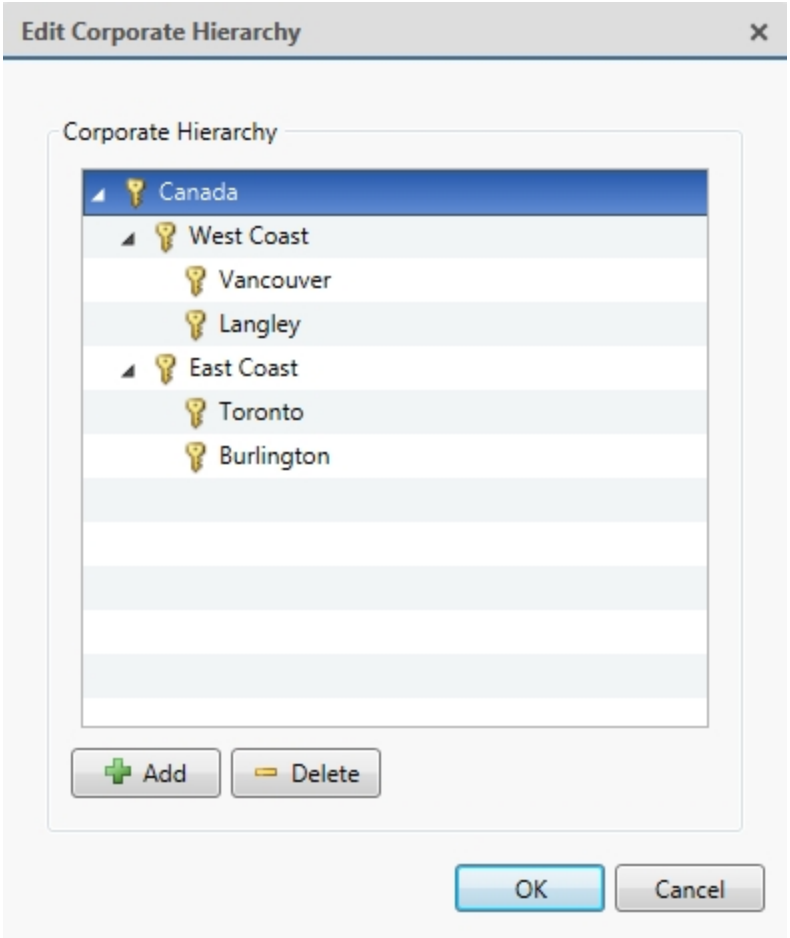
You can now assign ranks to groups. For more information, see *Adding Groups* on page 89.

Ranks

Ranks within Corporate Hierarchy represent the permission levels of your organization. For more information, see *Corporate Hierarchy* on the previous page.

Global is the default, and also highest rank in the Corporate Hierarchy.

To further explain ranks, we'll use this example. **Canada** is the highest, Global rank while **West Coast** and **East Coast** are equal rank, below **Canada**. Users in **East Coast** cannot edit ranks below **West Coast**.



Unranked Groups

The Unranked groups are outside 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.

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 the lowest rank possible. Those users are 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 will retain basic privileges.

Deleting a rank will delete all subordinate ranks. Remotely synchronized users and groups may become inaccessible.

Ranked Site Families

Ranks can be applied to sites 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 tied to the Global. For more information, see *Site Families* below.

Site Families

FOR ENTERPRISE EDITION

Independent sites can be connected to create a site family. User, rank, and group information is centrally managed by the parent site while the child sites can define local users and groups.

For more information, see *Corporate Hierarchy* on page 95.

Connecting Site Families

Each parent site can have up to 1 Core site, 24 Standard sites, and unlimited Enterprise sites as child sites. Each site should be running the same version of ACC software.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Manage Site**.
3. Select the site you want to connect as a child.
4. In the bottom-right corner, click **Connect to Parent Site**.

   Tip: To connect a single server to a different site, click the server , then click **Connect to Site...**.

5. In the **Connect to:** drop-down list, select a parent site.

6. In the **Rank:** drop-down list, assign a rank for the child site. For more information, see *Corporate Hierarchy* on page 95.
7. Click **OK**, then click **Yes**.

Disconnecting Site Families

You can dismantle a site family by removing the child site from your Corporate Hierarchy. Removed sites function independently, or can be connected to another parent site.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Manage Site**.
3. Select the parent or child site you want to disconnect.
4. In the bottom-right corner, click **Disconnect Child Site...** or **Disconnect from Parent Site...**.
5. Click **OK**.

> **Note:** Network issues may require revoking access from the parent site.

Restricting Login to Parent Sites

If you specify users on a parent site and synchronize them to a child site, to prevent the synchronized users from the child site to be able to log into the parent site:

1. In the parent site Setup tab, click **General**.
2. Select the **Restrict login to only Global and Unranked users** check box.
3. Click **OK**.

Avigilon Cloud Services

Avigilon Cloud Services (ACS) enables a modern cloud-connected user experience, accessible from a web browser or the ACC Mobile 3 app.

With ACS, you can:

- View live and recorded video.
- Access Saved Views. Only the first 9 cameras are available when opening a Saved View in the web client.
- Create custom Saved Views. These are only available in the ACS web client and cannot be shared between users.
- Control PTZ cameras using mouse controls. Activate existing PTZ presets and tours from the web client. New presets and tours created in the web client will be saved to the ACC site.
- Activate digital outputs. If a digital output is associated with a camera in the ACC client, it can be triggered from the cloud platform.

- Create, view, and manage bookmarks in the web client. Changes are synchronized between the ACC site and web client.
- Download MP4 video clips and snapshots to a local drive.

For more information about using the ACS platform, see **help.avigilon.com/cloud**.

Connecting to the Cloud

For the latest instructions, see **help.avigilon.com/cloud**.

Before Connecting Your ACC Site

- Ensure your ACC site has Internet access.
- Ensure that each ACC Server is version 7.12 or later and that the same version of the ACC Web Endpoint Service is installed and running.
- If you have a multi-server site, add all servers to the site before connecting to Avigilon Cloud Services. Otherwise you will have to disconnect the standalone servers from Avigilon Cloud Services before adding them to your single ACC site.
- Ensure each server has the correct time zone, date, time, and daylight saving time settings. For a multi-server site, ensure the servers are synchronized to a network time protocol (NTP) server.

Registering Your Organization

Administrators should register their organization in Avigilon Cloud Services. This organization can include one or more ACC sites and provides users with access to cameras across all sites.

1. In your browser, go to **cloud.avigilon.com**.
2. Select a **region*** then click **Not registered? Sign up**.
3. Enter the organization name and your contact information. Click **Submit**.
4. If Google™ reCAPTCHA is not supported, you will be directed to contact **support@avigilon.com**.
5. A registration email will be sent. Complete your registration:
    a. In the email, click the registration link. This link is only valid for 24 hours.

       If the link expires, register your organization again.

       If the link expires, contact *AvigilonCloud Services Support* to resend the link.

    b. Create a password. This password is unique to Avigilon Cloud Services and does not need to match your ACC password.

       Your password must contain 8-50 characters and include at least one:

       - Uppercase letter
       - Lowercase letter
       - Number
       - Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

       Your password cannot include the word "Password".

If you are a federated user, you are not prompted to set a new password. Avigilon Cloud Services will use your identity provider credential, such as a Microsoft account.

c. Select your **Preferred communication language**. This sets the language for emails from Avigilon Cloud Services.

d. Click **Submit**, then click **Sign in** and enter your credentials.

e. Review and accept the End User License Agreement.

Adding a Site to Your Organization

1. After the organization has been created, get an activation code in Avigilon Cloud Services:
   a. In the Sites tab, click **Add site**.
   b. Enter the site name, address, and select a Primary Contact who will receive email notifications about the site.
   c. Click **Add**. A code is displayed.
2. Copy the code and enter it in the ACC Client software:
   a. In the New Task menu , click **Site Setup**.
   b. Click the site name, then click **Avigilon Cloud Services** .
   c. Click **If you have an activation code, click here.**.
   d. Enter the activation code and click **Connect**.

   The system should connect shortly. If the system takes more than 15-20 minutes to finalize the connection, disconnect your site and try again.

Adding Users to Avigilon Cloud Services

After the ACC site is connected, an ACC administrator can enable users to access Avigilon Cloud Services. Users imported from Active Directory or ACM™ can also be enabled, however these users will have a unique password for Avigilon Cloud Services that may differ from their ACC password.

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. Select a user, then click **Edit User**.
4. Enter an email address if not already specified. This will be the username in Avigilon Cloud Services.
5. Select the **Connect** checkbox and click **OK**.
6. Click **Yes** to confirm the email address.

   The user will receive an email invitation with a registration link that expires within 24 hours. If the email does not appear, check the junk or spam folder.

Signing In to Avigilon Cloud Services

Users can sign in with their Avigilon Cloud Services credentials at **cloud.avigilon.com** and on the ACC Mobile 3 app.

Giving Users Additional Privileges

Avigilon Cloud Services administrators can manage sites, users, and view the System Health dashboard. Avigilon Cloud Services managers can also view dashboards without site or user management privileges. You can elevate users to be an administrator or manager.

In Avigilon Cloud Services:

1. On the Organization Management page > Users tab, select a user.
2. In the **Role** drop-down list, select Administrator or Manager.
3. Click **Save**.

* Avigilon Cloud Services Regions

Selecting the default region or USA will host your organization and accounts on Microsoft Azure servers in the United States. Selecting Asia Pacific or Oceania will host your account in Australia. All other options will host your account in Canada. Note that all users must select the same region to log in to their accounts.

Disconnecting from the Cloud

You can disconnect your site from Avigilon Cloud Services at any time. Cloud users will no longer have access to cameras or video from the site.

1. In the New Task menu, click **Site Setup**.
2. Click the site name, then click **Avigilon Cloud Services**.
3. Click **Disconnect**.
4. To confirm, click **Yes**.

   A success message is displayed and your site is disconnected.

   Synchronized cloud users are deleted from the ACC site.
5. Click **Close**.

You can confirm the status of your connection on the Site Health page. For more information, see *Site Health* on page 20.

ACM™ Appliances

FOR STANDARD AND ENTERPRISE EDITION

A site can connect to a single Access Control Manager (ACM) appliance. Once connected, you can import ACM roles, link cameras to doors, and add rules for ACM events.

Before Adding an ACM Appliance

FOR STANDARD AND ENTERPRISE EDITION

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
    - Doors Grant
    - 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** checkbox 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 a Lightweight Directory Access Protocol (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 the ACM appliance 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 Avigilon Hardened OS 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 an ACM Appliance to an ACC Site

FOR STANDARD AND ENTERPRISE EDITION

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.

Note:
Make sure you have the following before you begin.

- The hostname or IP address of the ACM appliance.
- The ACM port number is 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 New Task menu , click **Site Setup**.
2. Click .
3. Enter the required credentials.
4. Click **OK**.

   Confirm that the listed SHA-256 fingerprint ID is the same. Fingerprint information is typically listed on the Appliance:Edit page, under the SSL Certificate tab.
5. If the fingerprints are the same, click **Trust**.

   If they do not match, contact your system administrator.

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

Importing ACM Roles

FOR STANDARD AND ENTERPRISE EDITION

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

Note:

- Importing ACM Roles to a site will disable all Active Directory users in the ACC software. To continue using Active Directory with ACM Roles, configure remote authentication from external domains in the ACM appliance first. Then import Active Directory users in the ACC software.
- If your ACM appliance is partitioned, ensure identities are members of the appropriate partitions so they can access unification features in the ACC Client.

Import Roles from the ACM appliance to give users access to cameras and doors. When you import a role, you also import the identities that are assigned to the role. Only identities with a username and password in the ACM appliance will be imported.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. In the External Directory tab, select **Avigilon Access Control Manager** from the drop-down list.
4. Click **Add Group**.
5. Select an existing group to use as a template then click **OK**. You can edit the permissions for the group later.
6. Select all the roles that you want to import.

   You can use the search bar to find specific roles.
7. Click **OK** to add the roles.

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

Imported roles can be edited for ranks, feature privileges, and device access rights to the imported role. 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.

Linking Doors to Cameras

FOR STANDARD AND ENTERPRISE EDITION

Note: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. Contact your ACM administrator to update your permissions.

Doors that are installed and connected to installed panels or subpanels can be linked to any number of cameras in your site. Once a link is created, authorized users can monitor doors, identities, and configure rules in the ACC software.

Contact your ACM administrator to configure the doors you want to link.

Adding a Link

1. In the New Task menu , click **Site Setup**.
2. Select the ACM appliance, then click .
3. Click **Create Link**.
4. In the **Select a door** drop-down list, select the checkbox beside a door.

   > **Note:** The available doors depend on your permissions in the ACM appliance. Contact your ACM administrator to update your permissions.

5. In the **Select one or more cameras** drop-down list, select the checkbox beside all the cameras that you want to link to the door.
6. Click **OK**.

Editing and Deleting a Link

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

1. In the New Task menu , click **Site Setup**.
2. Select the ACM appliance, then click .
3. Select a link then click **Edit Link**, or **Delete Link**.
4. Click **OK**.

Adding Rules for ACM Appliance Events

FOR STANDARD AND ENTERPRISE EDITION

> **Note:** To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. Contact your ACM administrator to update your permissions.

You can create rules in the ACC software that are triggered by ACM appliance events. These events can include attempts at door access and badge readers, and can trigger live video that immediately displays on all user's screens.

For a complete list of rules, actions, and conditions for access control events, see *Rule Events and Actions* on page 128.

1. In the New Task menu , click **Site Setup**.
2. Click , then click .
3. 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. 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. 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. Enter a **Rule Name:**, **Rule Description:**, and assign a **Schedule:**. For more information, see *Scheduling Rules* on page 126.
7. Click to save the new rule.

Customizing ACC

Create custom events, notifications, and alarms to enhance your site's security. Configure camera and display settings and manage licensed features like license plate recognition, maps, and the ACC Virtual Matrix.

Application Settings

You can select a theme, language, and other settings for the ACC Client software.

Automatically Logging In to Sites

You can log in to all sites that you have access to under the same credentials.

1. In the top-right corner, click > **Client Settings**.
2. Select the **Automatically log in to sites:** checkbox and select one of the following:
    - **Using Windows Authentication** — use your Windows credentials.
    - **Using saved user name and password:** — use your ACC credentials.
3. Click **OK** to save.

Changing the Theme

You can adjust whether the application display uses a light or dark theme. By default, the light theme is used.

Use a dark theme to reduce eye strain when using the software in a dark room.

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Display tab, select a theme.
3. Click **OK** to save your changes.

Changing the Language

You can change the language of the ACC Client.

1. In the top-right corner, click > **Client Settings**.
2. Select a **Language** from the dropdown list or select **Windows Default** to use the same language as the operating system.
3. Click **OK** to save.
4. Restart the ACC Client to see the change.

Saving the Layout

You can set the system to remember your layout preferences after closing and opening the ACC Client, as long as you keep the tabs open.

1. In the top-right corner, click > **Client Settings**.
2. Select the **Save/restore window layout** checkbox to remember your layout preferences. Select the **Automatically launch full screen** checkbox if desired.
3. Click **OK** to save.

Setting the Maximum Incoming Bandwidth

You can set how much bandwidth is received by the ACC Client. This includes video streaming.

1. In the top-right corner, click > **Client Settings**.
2. In the Maximum Incoming Client Bandwidth: area, select **Unlimited** or **Other:** to specify the maximum bandwidth allowance in kilobits per second (kbit/s).
3. Click **OK** to save.

Displaying System Messages

System messages appear in the top-right corner of the application window. The notification color represents the severity of your most recent message.

You can specify whether the client should show or hide the system messages.

1. In the top-right corner, click > **Client Settings**.
2. Select or clear the **Display Notifications** checkbox.
3. Click **OK** to save.

Display Settings

You can update the Site View to change the order of the System Explorer and configure how the ACC Client software displays video.

Editing the System Explorer

By default, all cameras are listed in alphabetical order by site in the System Explorer. You can organize the System Explorer to display cameras by location and group items for convenience. You can also hide cameras that are not relevant to an ongoing investigation. Each camera grouped under a folder shows up grouped in the *Focus of Attention* on page 166 module.

The site cannot be moved or re-organized.

> **Note:** These settings only affect the System Explorer in the View tab.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Site View Editor**
3. Edit your layout.
    - To add a folder, click . Folders are only visible in the View tab.

      Double-click the folder to change its name.
    - Click and drag items to move their location.
    - Use to move one element at a time.
    - To sort the layout alphabetically, click . To sort a single folder, select an element within the folder then click .
    - To delete a folder, select the folder and click . The elements inside the folder will move to the bottom of the layout.
    - Expanded or collapsed folders will appear that way when users log in to the site. Users can still collapse or expand folders in the System Explorer.
4. Click **OK** to save your changes.

When you open a new View tab, the System Explorer displays your latest changes.

Changing the Video Display Settings

There are multiple settings that impact color and quality of the image displayed from a camera. These settings do not impact quality or image rate on the server.

1. Click > **Client Settings** > **Display**.
2. Update any of the following settings.
    - **Display Deinterlaced Images** — Smooths the blur occasionally seen in analog video.
    - **Display Logical IDs** — Displays the Logical ID next to the device name in the System Explorer.
    - **Display Device Preview** — Displays live video while hovering over a device in the System Explorer.
    - **Display Quality:** — Adjusts image quality based on bandwidth or processing power. Increasing the quality allows you to make out objects and faces while lowering quality is better for viewing moving events.
    - **Display Adjustment Settings:** — Changes the levels of contrast and brightness or restores the factory default. Make small changes at a time. If video is displayed in a View tab, the new

settings will not take effect until the **Restore Defaults** option is selected in the image panel.

> **Tip:** You can adjust these settings per image panel by right-clicking and selecting **Display Adjustments...**.

3. Click **OK** to save.

Video Overlays

Overlays display additional contextual information over video.

1. In the top-right corner, click > **Client Settings** > **Overlays**.
2. Enable any of the following overlays.
    - **Device Name** — Displays the device's assigned name.
    - **Device Location** — Displays the custom location of the device.
    - **Playback Timestamp** — Displays either the device's local timestamp or your local timezone during recorded playback.
    - **Live Timestamp** — Displays either the device's local timestamp or your local timezone during live playback.
    - **Record Indicator** — Displays recording status.

      > **Note:** Record Indicator must be displayed to enable manual recording. For more information, see *Manually Recording Video* on page 157.

    - **Motion Activity** — Highlights motion.
    - **Video Analytics Activity** — *For video analytics devices*. Highlights people and vehicles in live and recorded video.
    - **Live Video Analytics Activity:** — *For video analytics devices*. Select when overlays are displayed in live video.
        - **Off** — Hides video analytic overlays.
        - **Motion Only** — For H5A cameras, highlights only moving objects. For all other video analytics cameras, highlights people and vehicles.
        - **All** — For H5A cameras, highlights stationary and moving objects. For all other video analytics cameras, highlights moving objects only.

          When set to **Off** or **Motion Only**, overlays will still appear when hovering over detected objects in live video.
    - **License Plate** — Shows detected license plates during live video.
3. Click **OK** to save.

Configuring Standby Mode

FOR STANDARD AND ENTERPRISE EDITION

If a person does not agree to be under surveillance due to privacy concerns, you can put a device on Standby. When on Standby, the device does not stream or record video and operators will see that video has been Paused.

Create rules to enable and disable Standby mode. For example, you could set up a rule to trigger Standby when motion is detected and a digital input is activated.

Adding a Rule to Enable Standby

1. In the New Task menu , click **Site Setup**.
2. Click .
3. Click and select the events that will trigger the rule. Click .
4. Select **Pause device**. Click .
5. Select one or more conditions that will cause the rule to run. To always run the rule, clear all conditions. Click .
6. Enter a descriptive **Rule Name:** and **Rule Description:**.
7. Click to save the new rule.

Adding a Rule to Disable Standby

1. In the New Task menu , click **Site Setup**
2. Click .
3. Click and select the events that will trigger the rule. Click .
4. Select **Resume device**. Click .
5. Select one or more conditions that will cause the rule to run. To always run the rule, clear all conditions. Click .
6. Enter a descriptive **Rule Name:** and **Rule Description:**.
7. Click to save the new rule.

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 infrared (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.

Alternatively, in the Image and Display dialog box, set Day/Night Mode: to either Automatic, Day Mode or Night Mode.

Select the **Disable IR filter in Night Mode** check box to disable the IR filter when Day/Night Mode: is set to Night Mode. If the IR filter is disabled, the camera will stream in color.

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 rain, mist, or foggy conditions. Digital defog is disabled by default.

The digital defog levels in the image panel are applied to all user views and will be seen in recorded video.

- 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.

Dewarping Fisheye Displays

> **Note:** Images from Avigilon fisheye cameras are automatically dewarped. The following setting is for third-party cameras.

If your camera uses a fisheye or panomorph lens, you can dewarp the image from the ACC Client software.

1. In the New Task menu, click **Site Setup**.
2. Select a camera, then click **Dewarping**.
3. Select the **Enable Dewarping** checkbox.
4. Select the **Lens Type:** if applicable and the **View Perspective:**

- **Floor** — The camera is looking up.
- **Ceiling** — The camera is looking down.
- **Wall** — The camera is looking towards the horizon.

5. *Optional.* If the default dewarped view needs further adjustment, select the **Adjust Image** checkbox. A green overlay is displayed on top of the camera image.
   - Drag and resize the overlay to fit the camera field of view.
   - Use the **Left**, **Right**, **Top**, **Bottom** sliders to position the overlay.
   - Use the **Horizontal Stretch** and **Vertical Stretch** sliders to determine the size of the overlay.
   - Clear the **Adjust Image** checkbox to lock the changes and hide the overlay.
6. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
7. Click **OK** to finish editing.

After the settings are applied, we recommend creating a View with different portions of the dewarped image.

Save this View. For Enterprise and Standard Editions, see *Saving Views* on page 177. For Core Edition, select > **Client Settings** > **Save/restore window layout**.

For example, use a layout with 6 panels to display different directions from the same fisheye camera. Use the zoom and pan tools to display the appropriate portion of the video. For more information, see *Zooming and Panning* on page 161.

Zooming and Focusing the Camera Lens

If the camera has remote zoom and focus capabilities, they can be controlled through the Image and Display settings.

1. In the camera Setup tab, click .
2. If the camera has a built-in auto-focus feature, choose one of the following:
   - **Continuous Focus** — The camera will automatically focus itself whenever the scene changes. Skip the remaining steps.
   - **Manual Focus** — You can manually focus the camera through the Focus: buttons.
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.

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

> **Tip:** For pixel guidelines, refer to Designing a *Site with Avigilon Video Analytics and H3 LPC Camera Kit* and *ACC 6 License Plate Reader Engine Site Design* on **avigilon.com.**

> **Note:** Fisheye cameras and cameras connected to a video analytics appliance are not supported.

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 field of view. The live video is paused so you can measure the number of pixels an object of interest covers within the field of view.

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.

Configuring Infrared LEDs

You can enable or disable IR LEDs on the H4 Multisensor camera's exterior from the ACC Client software. Disable IR LEDs to prevent reflections off nearby objects 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**.

Displaying Video Analytics Activity

> **Note:** Certain options are only available if supported by the device.

When adding Avigilon self-learning video analytics cameras, you can choose to display the bounding boxes that highlight video analytics activity. By default, this setting is enabled, and bounding boxes will appear around detected objects and in AVI video export. When disabled, cameras will still detect events, but will not display the boxes outside of searches.

Tip: To change this setting for all cameras, change the Video Analytics Activity overlay option in Client Settings. For more information, see *Video Overlays* on page 111.

1. In the device Setup tab, click .

   The Settings dialog box opens.

2. Select the **Display Classified Objects** checkbox to enable bounding boxes. Clear the box to disable the display.
3. Click **OK**.

Injecting Text and Overlaying it on Video

You can inject text into ACC and view the text overlay on live and recorded video. You can select the cameras on which the text overlay will be shown and also toggle to show or hide the text overlay. In multi-server sites, you can send the same text to cameras connected to different servers. Use the point of sale (POS) transaction interface to inject text into ACC.

1. Enable textual inputs for text to be displayed in the image panel:
   a. Click in the top-right and click **Client Settings**.
   b. Navigate to the **Overlays** tab and select the **Text Inputs** check box.
   c. Click **OK**.
2. Set up a POS transaction. See *Adding a POS Transaction Source* on page 149.
3. Navigate to the **View** tab and click and drag the camera linked to the POS source from the System Explorer to an empty image panel.

Once the POS source sends textual data into ACC, the text is displayed in the bottom-right of the image panel.

Tip: Configure only one POS transaction source per camera for the text overlay to display properly. However, you may configure one POS transaction source to feed to multiple cameras.

Important: ACC has the `CFG_CONFIG_ENTRY(TransactIdleTimeout_s, L"CmnServ/TextTransact", false, Float, 600.0f)` configuration setting which sets a timeout period of 10 minutes by default. If ACC receives a start transaction signal but never receives any further text input or an end transaction signal, then it will reach the timeout and automatically end the transaction and the associated recording. Change the default value of `600.0` (seconds) to any required value. The timeout period value should account for the length of time that you expect each segment of a video to be.

WARNING — Changing the timeout period value may lead to unbounded recording. If the connection between the POS transaction source and ACC fails and the end delimiter is never received, then ACC will keep recording for the entire timeout period.

Searching the Injected Text

You can search for a text string from the POS transaction source to find the corresponding video.

1. In the New Task menu ☰, click **Text Source Transactions**.
2. In the **Search: POS Transactions** view, select the camera associated with the POS transaction source.
3. Optionally, set a Date Range: by selecting values for the **From:** and **To:** fields. You can also specify a **Duration:** value.
4. Enter the text string to be searched in the **Text:** field.
5. Optionally, you may select a specific value for your search from the **Method:** drop-down menu.
6. Click **Search**.

You can also create rules based on the injected text string values. To learn more about how to add rules, see *Adding a Rule* on page 126.

Events and Rules

Configure analytic and motion detection events, which can be used to set up rules. Rules allow you to select a set of actions that occur in response to events.

Analytic Events

You can define analytic events on each Avigilon video analytics device.

The events can be used to set up notifications or rules.

Adding an Analytic Event

1. In the New Task menu ☰, click **Site Setup**.
2. Select a camera, then click **Analytic Events** .
3. Click **Add**.
4. Enter a name. This should be unique throughout the ACC site.
5. Select the **Enabled** checkbox. If the checkbox is clear, the video analytics event will not detect or trigger any events.
6. Select an **Activity:**. For a description of each option, see *Analytic Event Descriptions* on page 120.

7. For *Activities In Regions of Interest* on the next page:
    a. Select the **Object Types:** the event applies to. If you only expect people or vehicles in a scene, select only one object type.
    b. Configure the green overlay to specify the region of interest.

    > **Note:** Analytic events are only triggered if the bottom center of the detected object's bounding box is in the region of interest or crosses the beam.

    c. Add an exclusion area if needed. This exclusion area applies only to this video analytics event configuration. Video analytics events are *not* detected in an exclusion area. It does not apply to other analytic events, Classified Object Motion detection, Motion Search, and the Avigilon Appearance Search feature.
    d. Configure the event settings:
        - **Occupancy Area:** — The name of a physical space in which the number of objects are counted. Use the same name to link different Enter and Exit events to the same occupancy area.
        - **Sensitivity:** — The likeliness of an object to trigger the event. The greater the sensitivity, the more likely an event will be triggered for objects detected with low confidence. The default is 8.
        - **Number of Objects:** — The number of objects required to trigger the event.
        - **Threshold Time:** — The minimum duration of the event before the system triggers an event. The default is 0-30 seconds depending on the activity.
        - **Timeout:** — The maximum duration of the event. Events that are still active after this time will trigger a new event. The default value is 60 minutes.
        - **Prohibited Direction:** — The arrow in the circle defines the direction that objects should not be traveling.
8. For *Temperature Detection Activities* on page 122:
    a. Ignore the Sensitivity:, Number of Objects:, and Threshold Time: settings.
    b. In **Timeout**, select the recording duration for the event. The default is 8 seconds. The range is 2-15 seconds.
    c. Configure the event settings:
        - If **Object with lower temperature** is selected, configure **Lower Temperature Threshold (°C)** or **(°F)**: The threshold below which a person may need further screening. Default is the calibrated value from the thermal camera.
        - If **Object with elevated temperature** is selected, configure **Elevated Temperature Threshold (°C)** or **(°F)**: The threshold above which a person may need further screening. Default is the calibrated value from the thermal camera.
        - If **Object with expected temperature** is selected, configure both of the above threshold events. Any temperature detection that falls between the specified thresholds is considered within the acceptable range.

d. When a detected temperature matches the threshold defined, the event triggers the camera to record for the specified duration.

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

Editing and Deleting Video Analytics Events

1. In the New Task menu, click **Site Setup**.
2. Select a camera, then click **Analytic Events** .
3. Select an event from the Analytics Events: area.
   - To edit the event, click and make the required changes.

     Note: If you change the name of the event, any rules or alarms linked to the event may no longer work.

   - To delete the video analytics event, click .

Analytic Event Descriptions

The following tables show the Activity: options that can be used when configuring analytic events. For more information and advanced options, see *Analytic Events* on page 118.

Activities In Regions of Interest

Note: The region of interest is like a rug or tripwire. Events are only triggered if the bottom center of the detected object's bounding box is in the region of interest or crosses the beam.

Activity:	Description
Objects in area	The event is triggered when the selected number of objects are present in the region of interest for longer than the threshold time. The object can appear from within the region of interest or enter from outside. Only one Objects in area event is activated when the specified number of objects are detected in the area. Additional objects in the area will not trigger additional events. Compare this with **Object appears or enters area** and **Objects enter area** below.
Object loitering	The event is triggered for each object that stays within the region of interest longer than the threshold time. Each object triggers a separate event. The event resets when the object leaves the region of interest or the event times out.

Activity:	Description
Objects crossing beam	The event is triggered when the specified number of objects have crossed the beam in the specified direction within the threshold time. If the number of objects is 1, the event is triggered after the threshold time elapses. ◦ To change the direction of the beam, click . ◦ To detect objects traveling in either direction of the beam, click .
Object appears or enters area	The event is triggered once for each object that is present in the region of interest for longer than the threshold time. The object can appear from within the region of interest or enter from outside the region of interest. This video analytic event causes many alarms. For example, if 20 objects are detected within the region of interest, 20 events are triggered – one for each object.
Object not present in area	The event is triggered when no objects are present in the region of interest for longer than the threshold time.
Objects enter area	The event is activated when the first object enters the region of interest and then is triggered if the specified number of objects also enter the region of interest within the threshold time. If the number of objects is 1, the event is triggered after the threshold time elapses. The region of interest must be smaller than the camera field of view to detect the object before it enters the region of interest. Objects that appear from within the region of interest will not trigger an event. Only one event is activated when the specified number of objects are detected in the area. Additional objects in the area will not trigger additional events.
Objects leave area	The event is activated when the first object leaves the region of interest and then is triggered if the specified number of objects also leave the region of interest within the threshold time. If the number of objects is 1, the event is triggered after the threshold time elapses. The region of interest must be smaller than the field of view of the camera.
Object stops in area	The event is triggered if a classified object is detected moving within the region of interest then stops moving for longer than the threshold time. One event is activated for each object that stops. An object can only be tracked for up to 15 minutes.
Direction violated	The event is triggered for each object that moves within 22 degrees of the prohibited direction for longer than the threshold time. One event is activated

Activity:	Description
	for each classified object that moves in the prohibited direction.
Enter occupancy area	The event is triggered for each object that enters an occupancy area. One event is activated for each classified object that enters an area in the specified direction. To define an occupancy area, create Enter and Exit occupancy area events. To ensure accurate counts, be sure to create events for each camera with an entrance to the occupancy area.
Exit occupancy area	The event is triggered for each object that exits an occupancy area. One event is activated for each classified object that exits an area in the specified direction. To define an occupancy area, create Enter and Exit occupancy area events. To ensure accurate counts, be sure to create events for each camera with an exit from the occupancy area.
Objects too close	The event is triggered when two detected people are closer than the specified distance for longer than the threshold time. If there is a group of people, an event will be triggered for each pair that is too close.

Temperature Detection Activities

The following analytic events are supported in the Avigilon H4 Thermal Elevated Temperature Detection camera. When a detected temperature matches the threshold defined, the event triggers the camera to record for the specified duration.

Activity:	Description
Object with lower temperature	This event is triggered when a lower temperature at or below the threshold is detected by a camera. Default is the calibrated value from the thermal camera. For example, if the default is 35.0 °C and 34.9 °C is detected, an event triggers the camera to record.
Object with elevated temperature	This event is triggered when an elevated temperature at or above the threshold is detected by a camera. Default is the calibrated value from the thermal camera. For example, if the default is 37.5 °C and 37.5 °C is detected, an event triggers the camera to record.
Object with expected temperature	This event is triggered when a temperature within the acceptable range is detected by a camera. Using the same examples above, if 37.5 °C is the **Object with elevated temperature** and 35.0 °C is the **Object with lower temperature**, and a temperature is detected within the 35 °C to 37.5° C range, an event triggers the camera to record.

Motion Detection Events

Motion detection is usually used to trigger video recording. For more information, see *Recording Schedule Templates* on page 47.

You can also configure the system to generate motion events that can be used when searching video or to trigger notifications and rules.

There are two types of motion detection available:

- **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.

  Note: The H5A Fisheye camera displays a circular deadzone in the center, overlayed on the image in the analytics panel. Object detection is not available in this circular area.

- Select a camera, then click **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.

Setting Up Classified Object Motion Detection

Set up classified object motion detection to define classified object motion events. Motion events can be used when searching recorded video, or to trigger notifications and rules.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Motion Detection** .

   Note: The H5A Fisheye camera displays a circular deadzone in the center, overlayed on the image in the analytics panel. Object detection is not available in this circular area.

3. In the **Classified Object Motion Detection** tab, configure the green overlay to define the region of interest where motion is detected.

   Note: Motion events are only triggered if the bottom center of the detected object's bounding box is in the region of interest.

- To change the shape or size of the overlay, click and drag the markers on the border. Extra markers are automatically added to help you fine tune the shape of the overlay.
- To move the overlay, click and drag.
- To add an exclusion area, click . The red exclusion area is added inside the overlay.

  Classified object motion is *not* detected in exclusion areas. This exclusion area is only for Classified Object Motion detection. It does not apply to other analytics features like Analytic Events, Motion Search, and the Avigilon Appearance Search feature.

  - 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.
  - To delete the exclusion area, select an exclusion area then click .
- To restore the green overlay, click .

4. Define the objects that are detected by the system.
   - **Object Types:** — select the objects that will trigger the motion event.
   - **Sensitivity:** — move the slider to adjust how likely the system is to generate a motion event.

     If you set the slider to the left, the device will generate fewer motion events for objects detected with higher confidence. Use this setting for scenes with a high level of activity.

     If you set the slider to the right, the device will generate more motion events for objects detected with lower confidence. Use this setting for scenes with little activity.

     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 detections.
   - **Threshold Time:** — enter how long an object must move before a motion event is generated.
   - **Pre-Motion Record Time:** and **Post-Motion Record Time:** — enter how long video is recorded before and after a motion event.
5. Click **Apply** to save your settings.

Setting Up Pixel Motion Detection

Set up pixel motion detection to define motion events. Motion events can be used when searching recorded video, or to trigger notifications and rules.

1. In the New Task menu , click **Site Setup**.
2. Select a camera, then click **Motion Detection** .
3. In the **Pixel Motion Detection** tab, define the region of interest where motion is detected. A motion event is generated for changes in any pixel within this region of interest.

   > **Tip:** 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 and drag to add a new pixel motion detection area. You can draw multiple overlays to define the pixel motion detection area.
   - — click and drag to exclude areas from the pixel motion detection area.
   - — manually draw pixel motion detection areas.
   - — select the entire image panel for pixel motion detection.
   - — clear the image panel of all pixel motion detection areas.
4. Define how sensitive the system should be to pixel motion.
   - **Sensitivity:** — adjust how much each pixel must change before it is considered in motion.

     When the sensitivity is High, small movements like dust floating immediately before the camera lens are detected.
   - **Threshold:** — adjust how many pixels must change before the image is considered to have pixel motion.

     When the threshold is High, only large movements like a truck driving across the scene are detected.

     > **Tip:** The **Motion** indicator above the Threshold: slider indicates how much motion is occurring in the current scene. The camera will only detect pixel motion if the Motion indicator moves to the right of the Threshold: marker.
   - **Pre-Motion Record Time:** and **Post-Motion Record Time:** — specify how long video is recorded before and after the pixel motion event.
5. Click **OK** to save your settings.

Adding a Rule

FOR STANDARD AND ENTERPRISE EDITION

Rules tell the system what to do when an event occurs. For a complete list of events and actions, see *Rule Events and Actions* on page 128.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Rules** .
3. Click **Add**.
4. Select the events you want included as triggers. Click **Next**.
5. Select as many actions as you want to include as responses. Click **Next**.
6. Select the conditions that must be met to activate the rule. Click **Next**.

   > **Tip:** Events, Actions, and Conditions can be further defined if they appear as blue text after being selected.

7. Add a **Rule Name:** and **Rule Description:**. The name should be unique throughout the ACC site.
8. Assign a schedule. For more information, see *Scheduling Rules* below.
9. Click **Finish**.

Scheduling Rules

FOR STANDARD AND ENTERPRISE EDITION

When you configure a rule based on an event that affects the entire site, you can assign the rule a schedule. Schedules control when rules are triggered — at specific times during a day, or only on specific days.

The **Schedule** option is displayed on the last step of adding or editing a rule.

- 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 . Complete the following steps:
  1. Give the new schedule a name. This should be unique throughout the ACC site.
  2. Give the first recurrence a unique 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.

> **Note:** 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.

Editing and Deleting Rules

FOR STANDARD AND ENTERPRISE EDITION

1. In the New Task menu, click **Site Setup**.
2. Click the site name, then click **Rules** .
3. Select a rule and click **Edit**, or **Delete** to remove the rule.
4. When you're finished updating the rule, click **Finish**.

Rule Events and Actions

FOR STANDARD AND ENTERPRISE EDITION

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 126 or *Adding Rules for ACM Appliance Events* on page 106.

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 expired.
Database error	Server database generated an error.
Data initialization error	Server database generated an error during initialization.
Data volume failed	Server data volume failed.
Data volume recovered	Server data volume 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 started.
Data upgrade completed	Server data upgrade finished.
Data upgrade failed	Server data upgrade failed.
Data recovery started	Server data recovery started.
Data recovery completed	Server data recovery finished.
Data recovery failed	Server data recovery failed.
Bookmark save failed	A bookmark was not saved properly.

Event	Description
Network connection found	A server network connection was found.
Network connection lost	A server network connection was lost.
Email send error	An error occurred while sending an email notification.
Server hardware event	A server hardware error occurred.
Archiving started	Server backup started.
Archiving completed	Server backup finished.
Archiving interrupted	Server backup failed.
Server connection lost	Server connection to the site was lost.
Analytics server queue full	Video analytics service cannot 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 stopped or restarted.
Active Directory connection failed	The Active Directory connection failed.

Device Events

Event	Description
Connection created	A camera or device was connected to a server.
Connection removed	A camera or device was disconnected from a server.
Connection created to standby server	A camera or device was connected to a standby server.
Connection removed from standby server	A camera or device was disconnected from a standby server.
Connection failed	A camera or device connection failed.
Device failed	A camera or device connection failed for more than 5 minutes.
Connection restored	A camera or device connection was 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.

Event	Description
Motion detection started	A motion detection event started on a camera.
Motion detection ended	A motion detection event ended on a camera.
Video analytics event started	A video analytics event started.
Video analytics event ended	A video analytics event ended.
Unusual Motion event started	A video analytics camera or device detected unusual pixel motion.
Unusual Motion event ended	An Unusual Motion event ended.
Unusual Activity event started	A video analytics camera or device detected a classified object behaving unusually.
Unusual Activity event ended	An Unusual Activity event ended.
IR Ring Failed	An IR illuminator ring failed on a device.
Tampering detected	A video analytics camera or device detected an unexpected change in the scene.
Recording started	A camera or device started recording.
Recording ended	A camera or device stopped recording.
Recording interrupted	A camera or device recording was interrupted.
Recording resumed	A camera or device recording was 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 started a firmware upgrade.
Firmware upgrade completed	A camera or device finished a firmware upgrade.
Firmware upgrade failed	A camera or device firmware upgrade failed.
Obsolete firmware detected	A camera or device is using obsolete firmware. The system is unable to perform an automatic upgrade.
ONVIF event started	A customized third-party camera ONVIF event started.
ONVIF event ended	A customized third-party camera ONVIF event ended.
Presence detected	The Avigilon Presence Detector sensor detected a presence.
Presence dwell time exceeded	The Avigilon Presence Detector sensor detected a continuous presence for longer than the configured dwell time.

Event	Description
Presence dwell ended	The Avigilon Presence Detector sensor no longer detects a presence that remained for longer than the configured dwell time.
Presence ended	The Avigilon Presence Detector sensor no longer detects a presence. If the presence remained for longer than the configured dwell time, a Presence dwell ended event is also triggered.
Face watch list match started	A camera detected an appearance of a profile from a watch list.
Face watch list match stopped	The camera no longer detects the appearance of a watch list profile.
Person without a mask detected	A camera detected a person without a face mask.
Person without a mask no longer detected	The camera no longer detects a person without a face mask.

User Events

Event	Description
User login	A user logged in.
User logout	A user logged out.
Emergency privilege override performed	A user enabled Emergency Privilege Override.
Server setting changed	A user changed the server settings.
Site setting changed	A user changed the site settings.
Device setting changed	A user changed the camera or device settings.
Device connected	A user connected a camera or device to a server.
Device disconnected	A user disconnected a camera or device from a server.
Digital output triggered	A user manually triggered a digital output.
Bookmark added	A user added a bookmark.
Bookmark updated	A user updated a bookmark.
Bookmark deleted	A user deleted a bookmark.
PTZ moved	A user moved a PTZ camera.
PTZ idle	A user left a PTZ camera idle.

Event	Description
Export performed	A user performed a video export.
Speaker activated	A user started broadcasting audio through camera or device speakers.
Speaker deactivated	A user stopped broadcasting audio.
Virtual matrix monitor opened	A user opened a Virtual Matrix monitor in the View.
Map added	A user added a new map.
Map updated	A user updated a map.
Map deleted	A user deleted a map.
View added	A user added a saved View.
View updated	A user updated a saved View.
View deleted	A user deleted a saved View.
Web Page added	A user added a new web page.
Web Page updated	A user updated a web page.
Web Page deleted	A user deleted a web page.
Site View updated	A user updated the organization of cameras and folders in the System Explorer.
Custom keyboard command triggered	A user triggered a custom keyboard command.

Alarm Events

Event	Description
Alarm acknowledged	An alarm was acknowledged.
Alarm auto acknowledged	An alarm was acknowledged automatically.
Alarm triggered	An alarm was triggered.
Alarm assigned	An alarm was assigned to a user.
Alarm unassigned	An alarm was unassigned from a user.
Alarm purged	An alarm was purged.

POS Transaction Events

Event	Description
POS transaction started	A POS transaction started.
POS transaction ended	A POS transaction ended.
POS transaction exception	A POS transaction exception occurred.

License Plate Recognition Events

Event	Description
License plate detection started	A license plate was detected.
License plate detection ended	A license plate is no longer detected.
License plate watch list match	A license plate on an LPR Watch List was 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 • 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

Event	Description
	• 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: • 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

Event	Description
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 an event.

User Notification Actions

Action	Description
Display on-screen message	An on-screen message is displayed about the event.
Send email	An email notification is sent to the selected recipients.
Send notification to Central Monitoring Station	A notification is sent to the central monitoring station.
Play a sound	A notification sound is played in the ACC Client software when the event occurs.

Monitoring Actions

Action	Description
Start live streaming	The associated live video displays when the event occurs.
Video intercom call	The video intercom call opens in a new image panel with a ring tone.
Focus of Attention	The event video displays in the Focus of Attention tab if it is open.
Create Bookmark	The event video is bookmarked.
Open a saved view	The selected saved View automatically displays.
Start live streaming on a virtual matrix monitor	The live video from the selected camera automatically displays on the selected Virtual Matrix monitor.
Open a map on a virtual matrix monitor	The selected map automatically displays on the selected Virtual Matrix monitor.
Open a web page on a virtual matrix monitor	The selected web page automatically displays on the

Action	Description
	selected Virtual Matrix monitor.

Device Actions

Action	Description
Reboot device	The camera or device reboots when the event occurs.
Pause device	The camera or device goes on standby when the event occurs. Streaming and recording are paused.
Resume device	The standby camera or device resumes streaming and recording activity when the event occurs.
Activate digital output	A digital output is triggered when the event occurs.
Deactivate digital output	A digital output is deactivated when the event occurs.

PTZ Actions

Action	Description
Go to Preset	The selected PTZ camera moves to the selected preset position when the event occurs.
Go to Home Preset	The selected PTZ camera moves to the home position when the event occurs.
Run a Pattern	The selected PTZ camera runs a selected pattern when the event occurs.
Set Auxiliary	The selected PTZ camera starts the selected auxiliary command when the event occurs.
Clear Auxiliary	The selected PTZ camera ends the selected auxiliary command when the event occurs.

Alarm Actions

Alarm	Description
Trigger an alarm	An alarm triggers when the event occurs.
Acknowledge an alarm	An alarm is acknowledged when the 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 when the event occurs.
Digital input is not active	The rule is triggered if the connected digital input is inactive when the event occurs.

Notifications and Alarms

Configure notifications to alert users of important events.

Alarms

Alarms are custom rules for cameras and devices that immediately bring suspicious activity to the attention of a user. Alarms can be monitored in the Alarms tab or from the ACC Mobile 3 app, available for free on the App Store and Google Play™ store.

Adding an Alarm

1. In the New Task menu , click **Site Setup**.
2. Click **Alarms** .
3. Click **Add**.
4. Choose the trigger source for your alarm.
    - **Motion Detection** — Motion is detected across the camera's field of view.
    - **Video Analytics Event** — A custom event has been triggered on a video analytics-enabled camera.

      Note: All video analytic events linked to the camera will trigger this alarm. To trigger alarms for specific analytic events, see *Adding an Analytics Alarm* on the next page.

    - **Digital Input Activation** — A signal was detected from an active device on the site.
    - **License Plate Watch list Match** — A camera has detected a registered license plate.
    - **POS Transaction Exception** — A point of sale (POS) source has detected an exception to the transaction rules.
    - **Device Error** — A device has lost connection, failed to complete a task, or is at risk of tampering.
    - **System Error** — The server has unexpectedly disconnected, storage has encountered a problem, or your licenses have expired.
    - **External Software Event** — An event from a custom integration has been triggered.

- **Face Watch List Match** — A camera has detected a profile from a Face Watch List. Each profile triggers a separate alarm. You can update which watch lists are linked to this alarm from the Face Watch Lists tab. See *Face Watch Lists* on page 142.

5. Select which devices will be involved in the alarm. Click **Next**.
6. Enter a **Pre-Alarm Record Time:** for how long to record before an alarm is triggered, and the **Recording Duration:**. Select the devices to link to the alarm. Click **Next**.
7. Add the users and groups that will receive notifications about the alarm. Click **Next**.

   Tip: Users with no wait time will be informed of an alarm immediately.

8. Select which actions should be taken when acknowledging the alarm. Click **Next**.
9. Name the alarm, assign a priority, and add a schedule.
10. Click **Finish**.

For more information, see *Reviewing Alarms* on page 168 and *Searching Alarms* on page 182.

Editing and Deleting Alarms

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Click on one of your existing alarms. Click **Add**.
4. Select an alarm and click **Edit** to update or **Delete** to remove the alarm.
5. Click **Finish** to save changes.

Adding an Analytics Alarm

If there are multiple analytics events per camera, use the following method to trigger alarms for specific analytic events.

1. Add an alarm using **External Software Event** as the alarm trigger. Give the alarm a specific name and note it for the following steps. For more information, see *Alarms* on the previous page.
2. Add a rule based on the **Video analytics event started** trigger.
3. Select the video analytics events you want to trigger the rule for.
4. Select the **Trigger an alarm** rule action and select the alarm created above.

   For more information, see *Adding a Rule* on page 126.

   Tip: If analytics events on different cameras have the same analytics event name, selecting that analytics event will trigger the rule for all cameras.

Email Notifications

You can automatically email individuals and groups when events occur.

1. In the New Task menu , click **Site Setup**.
2. Click **External Notifications** .

Configuring the Email Server

When generating email notifications, the ACC Client must have access to an email server.

1. In the **Email Server** tab, configure the following.
   - **Sender Name:** — The name that will be displayed in each email.
   - **Sender Email Address:** — The email address that will be displayed in each email.
   - **Subject Line:** — The subject displayed in each email.
   - **SMTP Server:** — The server address used by the site.
   - **Port:** — The SMTP port number.
   - **Timeout (seconds):** — The maximum time a server will spend trying to send an email.
2. If the email server uses encryption, select the **Use secure connection (TLS/SSL)** checkbox. For servers that use STARTTLS encryption, select the **Use STARTTLS** checkbox.
3. If the email account has a username and password, select **Server requires authentication** checkbox and enter the credentials.
4. Click **OK**.

> **Tip:** After the Email Server is configured, you can add Rules that send email notifications to selected recipients. See *Adding a Rule* on page 126.

Adding Recipients

1. In the **Email Notifications** tab, click **Add**.
2. Configure the following.
   - **Email Group Name:** — Enter a name for the email group.
   - **Add Email** — Manually add a single email.
   - **Add User/Group** — Include a user or group's email.
3. Select the **Email Trigger** and customize which cameras, devices, or transactions will be included. For more information, see *Email Notification Triggers* on the next page.
4. To attach camera images to the email notifications, select the **Attach images from device(s) linked to the event** checkbox.
5. Select an **Email Schedule** and enter a limit on email frequency.
6. Click **OK**.

Editing Email Notifications

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **External Notifications** .
3. Select an email group and makes your changes, or click **Remove** to delete the group.
4. Click **OK**.

Email Notification Triggers

The following table describes the email notification trigger options that are available when setting up an email notification. For more information, see *Email Notifications* on the previous page.

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 • Data upgrade completed • Data upgrade failed

Email Notification Trigger	Description
	• 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.

Central Station Monitoring

FOR STANDARD AND ENTERPRISE EDITION

Notifications are supported as XML over SMTP or SIA over IP. Check with your monitoring service for their preferred method.

1. In the New Task menu, click **Site Setup**.
2. Click the site name, then click **External Notifications**.
3. In the **Central Station Monitoring** tab, enable central station monitoring and select the method for your notification.
4. Add the email or account information for the monitoring company.
5. Set the **Minimum Heartbeat Interval:** to the frequency your monitoring company recommends. This message confirms that your site is communicating with their network.

   > **Tip:** Click **Send Test Message** to make sure that you've correctly entered all contact information.

6. Click **Apply** then **OK**.

After Central Station Monitoring is configured, you can create a rule to automatically send email notifications with video or image attachments. For more information, see *Adding a Rule* on page 126.

Face Recognition

FOR ENTERPRISE EDITION

With Face Recognition, administrators can create watch lists of people of interest for operators to search and monitor.

Face Watch Lists

Watch lists allow operators to monitor and search for specific people across your site. You can create rules and alarms based on different watch lists, as well as monitor live appearances using *Focus of Attention* on page 166 or search for recorded appearance events. For more information, see *Searching Events* on page 182. You can also search based on an uploaded photo. For more information, see *Searching from a Face Watch List Profile* on page 146.

Editing a Watch List

By default, all sites have one face watch list. Update your watch list as needed.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. Select a watch list and edit the settings:
   - **Name:** — The watch list name.
   - **Description:** — Information about the watch list.
   - **Default Minimum Match Confidence:*** — The default minimum confidence required for a profile match to trigger an event. The recommended confidence is **Medium**.
   - **Default Profile Expiry:*** — Select how long profiles are stored in the watch list. After this time, profiles are removed from the watch list and will no longer generate events. You can still view past events after this period if the recorded video is available.

     This setting only affects the expiry date for new profiles. Existing profiles will continue to use their previously set expiry date.

   - **Alarms** — Toggle whether profiles in this watch list trigger a Face Watch List Match alarm. To add a new alarm, see *Alarms* on page 137.

   * Individual profiles can have their own custom settings. For more information, see *Editing a Profile* on page 145.

   All changes are automatically saved.

Adding a Watch List

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. In the top-left, click **Add Watch List**.
4. Enter a **Name** and **Description**, then click **OK**.

Deleting a Watch List

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. Select a watch list, then click in the top-right corner.
4. Click **Yes** to confirm.

Configuring Data Retention

To set how long the ACC system stores appearance signatures, see *Identity Data Retention* on page 41.

Exporting a Watch List to Another Site

Watch lists are site-specific. You can copy a watch list from one site to another using the backup and restore settings.

> **Note:** Both sites should use the same version of the ACC Server software. Existing watch lists will be overwritten.

1. In the New Task menu , click **Site Setup**.
2. Click the site with the watch list you want to copy, then click **Backup Settings** .
3. Enter a password, then click **OK**. Select where to save the AVS file.
4. Click the name of the site you want to copy the watch list to.
5. Click **Restore Settings** and select the AVS file.
6. Enter the password, then click **OK**.
7. Select **Use custom settings**, then **Choose Settings**. Clear all settings except **Face Watch Lists**, then click **OK**.
8. Click **OK**, then **OK** again.

Adding Watch List Profiles

Watch list entries are called profiles. You can have up to 5000 profiles across all watch lists in a site. Avoid creating multiple profiles of the same person.

> **Tip:** A good profile is like a passport photo — a high-resolution, front-facing image of a person's face that includes the shoulders and some distance above top of head.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. Select a watch list, then click **Add Profiles**.
4. Select the profile images to upload. Use the `Ctrl` and `Shift` keys to select multiple files.
5. Click **Open**.

   The upload progress is displayed. If any errors occur during the upload process, they will appear in an exportable list.
6. Click **Close**.

Adding a Profile from Recorded Video

You can add profiles from recorded video from any camera across a site licensed for Face Recognition, even cameras that do not have Face Recognition enabled.

1. In a View tab or in an Avigilon Appearance Search result, find the person of interest. A front-facing image works best.
2. In the top-right corner of the image panel, click .
3. Click and drag to select a reference image. A square box that includes the person's shoulders and some distance above top of head is ideal.
4. In the following dialog box, describe the person of interest.
   - **Short Description:** — Identifies the person of interest in event search results and Focus of Attention events. Use a unique description for each profile.
   - **Long Description:** — Displays when viewing an event search result or Focus of Attention event. Provide additional information about the person of interest, like what operators should do if a match is detected.
5. Select a watch list to add the profile to.
6. Click **OK**.

   A notification confirms that the image is queued to be added.

Profile Status and Quality

Select a profile to see its status and quality on the right-hand side.

If a server cannot process an image, it is listed under Errors:

- — Pending. If processing takes longer than a couple of minutes, the ACC Server or ACC Analytics Service may be unavailable.
- — Rejected. The server cannot reach the ACC Analytics Service, is a dfferent version, or the image failed to upload. This may also occur if the system could not detect a face, multiple faces were detected, or the image resolution is poor.
- — The status is unknown.

After they are processed, profiles of Good, Average, or Poor quality will be used to detect matches throughout the site. The profile quality impacts the match performance, so replace poor quality profiles if possible.

Editing a Profile

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. In the left-side explorer, select a profile. Use the search bar to filter by name.

   You can also double-click a profile image to edit it.
4. By default, profiles use the minimum match confidence set by the watch list. Select a **Minimum Match Confidence:** in the drop-down list to override the default.
   - **Low** — The system generates events when a detected person matches the profile with a low level of confidence. This may result in more false alarms.
   - **Medium** — This is the recommended value.
   - **High** — The system only generates events when a detected person matches the profile with a high level of confidence. This may result in missed events.

   Your changes are automatically saved.

Changing Profile Expiry

You can set custom expiration dates for individual profiles.

1. Click **Change...**.
2. Select a new expiry date or click **Remove Expiration** to keep the profile from expiring.

   Your changes are automatically saved.

Moving a Profile

If you have multiple watch lists, you can move a profile from one watch list to another. The profile will use the new watch list's default expiry date.

1. Click **Move...**.
2. Select a watch list, then click **OK**.
3. Click **Yes** to confirm.

Deleting a Profile

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. In the left-side explorer, click to remove a profile.

Searching from a Face Watch List Profile

Search for a person or vehicle of interest from a Face Watch List profile.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Face Watch Lists** .
3. In the left-side explorer, click a list and then a profile from the list.
4. Click the **Appearance Search** button in the profile details.
5. Search video footage in the Appearance Search Options window:
    a. Click **Date Range** to set the date and time of your search.
    b. Click **Cameras** to select the cameras you want to include in the search. By default, all cameras enabled with the Avigilon Appearance Search feature are selected.
    c. Optional. Fill out the **Reason for Search**.
    d. Click **Search**.

    For more information, see *Avigilon Appearance Search Results* on page 180.

License Plate Recognition

FOR ENTERPRISE EDITION

License Plate Recognition (LPR) reads and stores vehicle license plates from any video streamed through the ACC software.

Setting Up License Plate Recognition

License Plate Recognition (LPR) is only available if you have the feature licensed for your site and if the ACC 7 LPRv2 plugin is installed on each server in the site. AI NVRs do not require the LPRv2 plugin.

1. In the New Task menu , click **Site Setup**.
2. Select a server, then click .
3. Select a lane from the License Plate Lane list and complete the following fields:
    - **Name:** — The name for the lane. This should be unique throughout the ACC site.
    - **Camera:** — The camera that will perform LPR. One camera can be used for multiple lanes.
    - **License Plate Configuration:** — The regional plate format the camera will recognize. For more information, see *Supported License Plates* on page 148.
    - **Pre-Event Record Time:** — How long video is recorded before the license plate is recognized.
    - **Post-Event Record Time:** — How long video is recorded after the license plate is recognized.
    - **Minimum Confidence:** — The minimum confidence required for a detected license plate to be registered as an LPR event.
    - **Enable this lane** — Enable LPR on this lane.

- **Max Image Analysis Rate:** — Enter an image rate between 1-60 images per second (ips). This specifies the maximum frame rate analyzed by the LPR service.
    - When higher than the camera's image rate, the LPR service will analyze more frames, increasing the processing time.
    - When lower than the camera's image rate, the system will analyze fewer frames, 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.

   A red overlay means the detection area is too large and cannot be used.

5. Click **OK**.

LPR is now configured for your site and you can add Watch Lists to your site. For more information, see *LPR Watch Lists* below.

> **Note:** Monitor the server CPU and memory usage after enabling LPR. Ensure the server has enough resources.

Configuring LPR Data Retention

To set how long the ACC system stores license plate data, see *Identity Data Retention* on page 41.

Displaying the LPR Overlay

You can display license plates as they're detected in video by enabling the License Plate overlay.

1. In the top-right corner of the ACC Client window, select > **Client Settings** > **Display**.
2. In the Image Overlays: area, select the **License Plate** checkbox.
3. Click **OK**.

LPR Watch Lists

Watch lists allow you to automate the search for specific vehicles across your site.

Adding a Watch List

You can add a list by importing CSV files or by manually entering license plates.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **License Plate Watch List** .
3. Click **Add**.
    - To import a watch list, click **Import** and select a CSV file to upload.
    - To add a single license plate, click **Add** and enter the license plate.

> **Note:** Your file must include a column including Minimum Confidence to determine the likelihood of a match before an LPR event is registered.

Exporting a Watch List

You can export an existing Watch List as a text file or a 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. Select a Watch List and click **Edit**.
3. Click **Export**.

   A CSV file is downloaded.

Editing or Deleting a Watch List

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Select a watch list and click **Edit** to add and remove plate numbers or click **Delete** to remove the list.
4. Click **OK**.

Supported License Plates

The following license plates are supported. To configure the license plate format for your server, see *Setting Up License Plate Recognition* on page 146.

- Argentina
- Australia
- Brazil
- Canada
- China
- Japan
- Malaysia
- Mexico
- Middle East[2]
- New Zealand

- Europe
- Egypt
- Gulf Cooperation Council[1]
- India
- Indonesia
- Iran
- Iraq
- Israel
- Russia[3]
- Singapore
- South Africa
- South Korea
- Thailand
- United Kingdom
- United States

[1] Includes Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates.
[2] Includes Lebanon, Jordan, and Yemen.
[3] Includes Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, and Uzbekistan.

POS Transactions

FOR STANDARD AND ENTERPRISE EDITION

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.

Adding a POS Transaction Source

You can add multiple devices as point of sale (POS) sources for transactions if they are connected to your network.

1. In the New Task menu, click **Site Setup**.
2. Select your server, then click **POS Transactions** .
3. Click **Add**.
4. Enter the **Hostname/IP Address:** and the **Port:** of your device. If the ACC system is connected as a Server to the device, enter the ACC port number.
5. Select the **Connection Type:**. In most cases, the ACC system is connected as a **Client** to the device, but there may be cases where the ACC system is configured as a **Server**. Click **Next**.
6. Select the **Data Format** for the source. This format will be used to recognize and capture the device's output. Click **Next**.
7. Select the **Exceptions:** from the source if you require any. Exceptions are the parts of a transaction that are ignored by the system. Click **Next**.
8. Select the cameras or devices to link directly to the POS source as well as their **Pre-Transaction Record Time:** for how long to record before a transaction, and its **Post-Transaction Record Time:**. Click **Next**.
9. Provide a name and description for the transaction source. Click **Finish**.

Now that you have a transaction source, you can format the data. For more information, see *Adding Data Formats* on the next page.

Adding Data Formats

The data received from most devices will need to be formatted to be easily recognized by the system or a user. While adding a new point of sale (POS) source or editing an existing one, you can customize the output of the device.

1. In the Set Transaction Source Data Format area, click **Add** or select a previous format and click **Edit**.
2. Edit the properties of your new format.
    - **Name:** — The name displayed under your list of formats.
    - **Description:** — A short explanation of the data and device.
    - **Transaction Start Text:** — The received text that signals the start of each transaction.
    - **Transaction End Text:** — Text that signals the end of a transaction.
    - **Encoding:** — The encoding used by the source device.
3. Use **Capture Data** to receive raw data. You can also save this information, or load a previous example of data.
4. Click **Add Filter...** to format the information. Default formats create line breaks and remove excess spacing.
    - **Text to Match** — Enter the text expected to appear from the device, and choose whether to make your search case-sensitive or required to match the entire word.
    - **Action to Take:** — Decide if the transaction responds by removing the item, or replacing the detected text.

    > **Note:** Add as many filters as you want for the data.
5. Click **OK** to add the filter.
6. Click **OK** to save your configured data format.

Adding Transaction Exceptions

By adding exceptions to your transactions, the software will help identify unauthorized discounts, manual price overrides, and false refunds.

1. From the Set Transaction Exceptions section of the Setup Wizard, click **Add** or select a previous exception and click **Edit**.
2. Add a name for the exception.
3. Select which type of exception the system will search for.
    - **Match Text** — Enter the text expected to appear from the device.
    - **Match Value** — Enter the value and its expected relationship, whether equal to, less or more than, or between. You can also add any text that will appear before or after.
4. Click **OK**.

Editing Transaction Sources

1. In the New Task menu , click **Site Setup**.
2. Select your server, then click **POS Transactions** .
3. Select a transaction source, then click **Edit** to change source details, or **Delete** to remove the source.
4. Use the POS Transactions Setup wizard to update the POS source, and click **Next** to move between fields.
5. When you're finished, click **Next** until you reach the end of the wizard and then click the **Finish** button.

Joystick Settings

There are two types of joysticks supported by the ACC Client: standard Microsoft DirectX USB joysticks and the Avigilon USB Professional Joystick Keyboard.

Use the Joystick settings to 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 ACC Client software keyboard commands. For more information about the keypad commands that control the ACC Client software, see *Keyboard Commands* on page 194.

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 ACC Client, select > **Client Settings** > **Joystick**.

   If the keyboard is not automatically detected, an error message is displayed. Click **Scan for Joysticks...**.
3. Select the **Enable left-hand mode** checkbox.
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.
2. In the top-right corner of the ACC Client, select > **Client Settings** > **Joystick**.
3. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.
4. 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.
5. Click **OK**.

Virtual Matrix

FOR ENTERPRISE EDITION

The 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.

The ACC Virtual Matrix can be downloaded from avigilon.com.

Adding a Virtual Matrix

1. Open the ACC Virtual Matrix and log in using your ACC Client credentials.
2. Enter a **Monitor Name** to identify the monitor in the ACC Client software and a **Monitor Logical ID** that can be used with keyboard commands.

   Tip: Click **Add Monitor** to add another monitor.

3. In the ACC Client software, double-click the Virtual Matrix monitor in the System Explorer.
4. Edit the layout, add cameras, and cycle views.

Changes in the ACC Client software automatically appear in the Virtual Matrix.

Adding Sites

The Virtual Matrix can be used to view video from multiple cameras from multiple sites.

1. Move your mouse to activate the monitor settings and click **Add Site**.
2. Find your site in the drop-down list or click **Find Site** to enter the IP address.
3. Enter your credentials and click **Log In**.

Changing Primary Sites

1. Move your mouse to activate the monitor settings and click **Change Site/User**.
2. Find your site in the drop-down list or click **Find Site...** and enter the IP address.
3. Enter your credentials and click **Log In**.

Deleting a Virtual Matrix

If a Virtual Matrix monitor is disconnected, you can remove it from your System Explorer.

- Right click the Virtual Matrix monitor and select **Delete**.

Maps

FOR STANDARD AND ENTERPRISE EDITION

You can create and manage maps that can be monitored in the View tab. Operators can interact with video or alarms from cameras on the map.

> **Note:** To learn more about the new Maps (Preview) feature, see the **ACC Maps (Preview) User Guide** on **help.avigilon.com**.

Adding a Map

You can add a JPEG, BMP, PNG, or GIF as a layout of your site.

> **Tip:** Maps should be smaller than 3000 x 3000 pixels.

1. In the System Explorer, right-click on your site and select **New Map**.
2. Add a name and click **Change Image...** to upload your map.
3. Select the location of the map in your site hierarchy.
4. Click **OK**.

After a map has been added, you can add camera locations and their view.

Adding Cameras to a Map

After you've uploaded a map, add cameras and highlight their field of view.

1. In the System Explorer, right-click on your map and select **Edit**.
2. Click and drag a camera from the System Explorer to add it on the map.
3. Customize the appearance, direction, and size of the camera.
    - **Size** — How large the icon is in relation to the map.
    - **Show As:** — Display the camera as an icon or shape.
    - **Icon, Shape & Cone Color** — The color of the camera con or shape.
    - **Preferences** — Display the field of view, name, or camera region.
    - **Delete from Map** — Remove the camera from the map.
4. In the toolbar, click **Save**.

Editing and Deleting Maps

You can update a map or delete an old map anytime.

- In the System Explorer, right-click then select one of the following:
    - To edit the map, select **Edit...**.
    - To delete the map, select **Delete**. When the confirmation dialog box appears, click **Yes**.

For more information, see *Using a Map* on page 172.

Web Pages

FOR STANDARD AND ENTERPRISE EDITION

Adding a Web Page

If you're connected to the internet, you can add web pages to a site in your System Explorer. Operators can use these web pages for quick access to your ACM appliance or other pages related to your surveillance system.

1. In the System Explorer, right-click a site or site folder and select **New Web Page...**.
2. Enter a web page **Name:** and **URL:**.
3. Select a **Zoom level:** to view the web page inside an image panel.
4. 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.
5. Click **OK**.

Editing and Deleting Web Pages

If a web page address is out of date, you can update the web page or delete the web page from the site.

- In the System Explorer, right-click then select one of the following:
  - To edit the web page, select **Edit...**.
  - To delete the web page, select **Delete**. When the confirmation dialog box is displayed, click **Yes**.

For more information, see *Opening a Web Page* on page 173

Using ACC

For operators who spend time monitoring live and recorded video or investigating events, this section covers how to control and search video, use devices, and export clips.

Controlling Live and Recorded Video

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**.

> **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.

Adding and Removing Cameras

At any point in time, you can add and remove cameras to your View using your System Explorer.

- Click and drag a camera from the System Explorer to an empty image panel in the **View** tab.

  > **Tip:** You can view the same camera in multiple image panels to maintain different zoom levels.

- To remove the camera, in the top-right corner of the image panel click .

Maximizing Image Panels

In the top-right corner of the image panel, click to maximize the video. Click to return to the previous size.

Requesting Dual Authorization

If your system has enabled Dual Authorization, a second user must also log in to your ACC site before you can see recorded video.

Request permission from a user with authorization power.

1. In the System Explorer, right-click the site then select **Dual Authorization Log In**.
2. The second user must enter their username and password.
3. Click **Log In**.

You now have access to recorded video.

Manually Recording Video

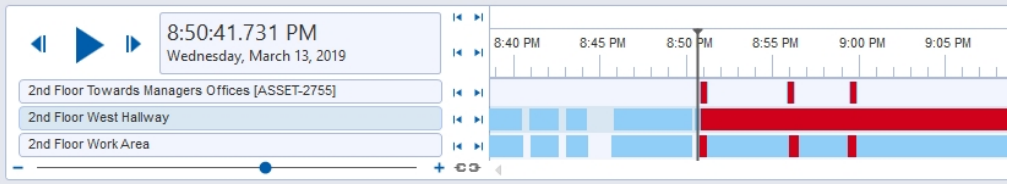
Manual Recording requires the Record Indicator overlay to be enabled. For more information, see *Video Overlays* on page 111.

From the moment that you notice unusual behavior or an event, you can begin recording.

1. In the image panel you want to record, click in the top left corner to start recording. The blue icon indicates recording has started.
2. Click to end recording.

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.



The colored bars on the Timeline show the camera's recording history:

- — motion event video.
- — recorded video.
- — bookmarked video.
- — protected bookmarked video.
- — selected motion or event search result video.
- — video archived by the Continuous Archive feature or unloaded timeline data. Click the area to load archived video from that time range:
  - — archived motion event video.
  - — archived video.

> **Tip:** You can also review archived video by opening the archived AVK file in the Avigilon Player software.

You can view and play through archived video, but you cannot skip between recorded events or search archived video.

- Empty areas show that there is no recorded video.

  If you are missing recorded video due to a network connection or server issue, the system can recover the video from an ONVIF Profile G camera that has an SD card recording video.

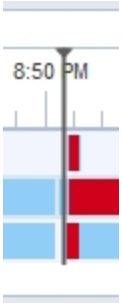
> **Note:** When the ACC Client starts up and displays the timeline, each device initially displays gray bars while the timeline loads the recording. A gray bar implies that the footage is still loading. Data is retrieved on a per device basis and displayed in the timeline when it becomes available eventually.

If a camera is configured with failover connections:

- The camera can appear in multiple locations in the System Explorer. 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 Explorer.

Using the Timeline

> **Tip:** To see how many days of recorded video are available, zoom out of the Timeline. To configure these settings, see *Recording and Bandwidth* on page 42

To...	Do this...
Select a playback time	 • Click the date and select a specific date and time. • Click a point on the Timeline. The marker appears on your selection. Drag the Timeline marker to preview video at different times.
Start playback	Click ▶ . • Click ▶▶ to fast forward. Click again to increase the playback speed. Maximum speed is 8x.

To...	Do this...
	• Click ◀◀ to rewind. Click again to increase the playback speed.
Stop playback	Click ❚❚ . • Click ❚▶ to go forward one frame. • Click ◀❚ to go backward one frame.
Jump forward or backward	Click ⏮ or ⏭ to jump forward or backward by a day, minute, or by camera event.
Zoom in or out of the Timeline	• Move the slider on the bottom left. • Place your mouse over the Timeline and scroll. You can zoom in to a quarter of a second, and zoom out to see years if recorded video exists.
Pan the Timeline	• Move the horizontal scroll bar under the Timeline. • Right-click and drag the Timeline.
Center the Timeline	Right-click the Timeline, and select **Center on Marker.**

You can continue to use the timeline when the ACC Server is in recovery mode. The ACC Server that is in recovery mode will have the **Recovering** suffix shown after its name in the tree under the Setup tab. The server will continue to record new video and you can click on the timeline to view and scrub video.

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 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 Playback

- To disable synchronized recorded video playback in all new View tabs, clear the **Synchronize recorded video playback** checkbox 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.

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**

Viewing Unusual Events

When viewing recorded video from a video analytics device, the Timeline displays motion, Unusual Activity, and Unusual Motion events.

You can filter the Timeline to display Unusual events only.

1. In the top-left corner of the Timeline, select the **Unusual Activity** or **Unusual Motion** checkbox.
2. Select the **Skip Play** checkbox to skip to the next event when playing video.
3. Select which **Anomaly Type** to display:
    - **All** — All unusual events.
    - **Speed** — Events with unusual speed.
    - **Direction** — Events with unusual direction.
    - **Location** — Events in areas where activity does not typically occur.
4. Move the **Rarity** slider to set how rare an event must be. Keep the slider towards the right to reduce noise.
5. Enter a **Minimum Duration** between 0-59 seconds to set how long an event must last. The default value is 2 seconds.
6. Use the Timeline controls to view the event video.

    Unusual Activity is highlighted in yellow bounding boxes. Unusual Motion is highlighted in teal bounding boxes. Image panels without unusual events are dimmed.

You can bookmark and export unusual events like other video analytics events. For more information, see *Bookmarking Recorded Video* on page 189 and *Exporting* on page 186.

Zooming and Panning

To get a better look at events in video, you can zoom or pan to focus on a section of the camera's field of view.

> **Tip:** Fisheye and panomorph video automatically dewarps when you zoom and pan.

Zooming

- Scroll the mouse wheel inside an image panel.

Panning

- Right-click and drag inside an image panel.

You can also use the Zoom and Pan icons on the right side of the toolbar.

For more shortcuts, see *Keyboard Commands* on page 194.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ features, including cameras with fisheye and panomorph lenses. 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 194.

> **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.

   The controls may appear differently depending on the options that the camera supports.
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.

4. Use the other PTZ controls to perform any of the following:

To...	Do this...
Zoom	• Click to zoom in. • Click to zoom out.

To...	Do this...
	• 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**.
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, pattern, or tour	For more information, see *PTZ Presets, Patterns, and Tours* on the next page.
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.
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.
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 following: • Click to move down the options. • Click to move up the options. • Click to confirm your selection. • Click to cancel your selection.

To...	Do this...
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.
	This feature is only available if all servers in the site are running the same version of the ACC Server software.

PTZ Presets, Patterns, and Tours

Pan, Tilt, Zoom (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.

> **Note:** For video analytics devices, classified object detection and analytic events only work when the camera is in its Home position.

Accessing the PTZ Controls Pane

1. In the top-right corner of the View toolbar, click .
2. In the bottom-right corner of the image panel, click .

Adding 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** checkbox if you want this to be the camera's Home preset.
5. Click **OK**.

Adding 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.

Adding a PTZ Tour

If supported, tours allow the PTZ camera to automatically move between a series of preset positions. You can set tours to pause at each preset for a specific amount of time for video monitoring.

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** checkbox 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.

Activating a Preset, Pattern, or Tour

- Select a preset, then click .
- Select a pattern or tour number, then click .

Using the H4 IR PTZ Wiper

1. In the View tab, click in the toolbar to enable PTZ controls.
2. In the bottom-right corner of the image panel, click .
3. Click **Aux**.

   The camera wiper will run.

Tip: You can also use the camera web interface or set up a rule to start an Auxiliary PTZ action when a digital output is triggered in the ACC Mobile 3 application. For more information, see the camera web interface guide on help.avigilon.com or *Adding a Rule* on page 126.

Using the H5 Hardened PTZ Illuminator

If the camera is installed with a narrow illuminator, you can control the illuminator from the Image and Display dialog box.

1. In the New Task menu , click **Site Setup**.
2. Select the camera, then click **Image and Display** .
3. Select one of the following options from the **Narrow Illuminator Mode:** drop-down list:
   - **Disabled** — The installed illuminator will be disabled and turned off.
   - **Enabled** — The installed illuminator will be enabled and turned on.
   - **At Zoom Level** — The installed illuminator will be enabled and turned on at a specific camera zoom level. Move the **Narrow Illuminator Zoom:** slider to set the corresponding zoom value.

   The installed illuminator will turn on accordingly.

Tip: You can also use the camera web interface to configure the narrow illuminator installed on the H5 Hardened PTZ camera. For more information, see the camera web interface guide on help.avigilon.com.

Live Monitoring

Use configured features to monitor your site effectively.

Note: Some features are only available if the site has the required license, and if you have the required user permissions.

Focus of Attention

FOR ENTERPRISE EDITION

The Focus of Attention tab gives you a high-level overview of all sites and cameras you have access to.

- In the New Task menu , click **Focus of Attention**.

  If selected in the settings, active alarms are displayed and cameras are highlighted in red until the alarm is acknowledged.

  As new alarms and events occur, the video appears in the Recent Events list and the corresponding camera changes color in the Overview.

The Overview

The Overview provides an abstract view of your System Explorer. Each hexagon represents a camera grouped by sites and folders. The cameras follow the order of the System Explorer from left to right and change color in response to events.

The camera color indicates the following:

- **Red** — Alarms
- **Yellow** — Face Watch List Matches, People Without Masks, License Plate Matches or Unusual Activity Detection
- **Teal** — Video Analytic Detection or Unusual Motion Detection
- **Blue** — Motion Detection
- **Green** — Highlights the camera displayed in the Recent Events list
- **Gray** — No event
- **Colorless** — Camera offline

Note: Custom events show in Teal on the video in the Recent Events list and as a Teal hexagon with a Blue border in the Overview tab.

Zooming and Panning the Overview

If you have many cameras or sites, you can zoom in and out of the Overview to pay attention to areas of interest.

- Scroll your mouse to zoom.
- Hold Ctrl and click and drag your mouse to pan.

You can also use the controls in the lower-right corner.

- — Displays the Overview zoom and position controls.
- — Centers the System Explorer.

Tip: Drag the Overview to a separate monitor to view Featured Event video and the Overview at the same time.

Changing Focus of Attention Settings

The Focus of Attention Settings dialog box is displayed when you first open the Focus of Attention tab. These settings only affect what the Recent Events list displays.

1. Select the events and cameras you want to view.
2. Click **OK**.

   Your settings are saved.

To edit these settings later, in the top-right corner of the Recent Events list, click .

Monitoring Events

To view video:

- Double-click a camera in the Overview.
- Hover over an event in the Recent Events list and click **Replay** or **Go Live**.

To return to the Overview:

- Double-click the Overview in the bottom-right corner.

The following options are available when you hover over an image panel.

Icon	Description
	Shares the event video with a selected user.
	Opens the event video in a new tab.
	Bookmarks the event.
	Clears the image panel.

Managing Alarms

Active alarms appear at the top of your Recent Events list and the corresponding camera will be red in the Overview.

You can view the alarm video, acknowledge the alarm, or view video from linked cameras.

If another user acknowledges, assigns, or purges the alarm, the alarm will no longer appear active.

Reviewing Alarms

FOR ENTERPRISE EDITION

After an event triggers an alarm, users are shown the camera or source of the alarm trigger. They will be asked to acknowledge and review the alarm, before choosing whether or not to clear it.

Acknowledging Alarms

1. Once notified, click **Acknowledge**.
2. If notes are enabled, enter any relevant details.

> **Note:** Devices and appliances can be connected to alarms and may require custom responses like a digital output.

Arming Image Panels

When you arm an image panel, it reserves that panel for displaying alarms and events. Arming an image panel also allows you to continue monitoring other video when an event is triggered. Arming a panel will not prevent other tasks in an image panel, including closing the video.

1. Select an image panel, and click .
2. Clicking a second time will disarm the panel.

In the event there are multiple alarms at once, linked videos will play in order, but will otherwise play in order of priority.

Reviewing Alarms

1. In the New Task menu under View, click **Alarms** .
2. At the top, choose which alarms to display.
    - **Active Alarms** — Any alarm that is still triggered.
    - **Alarms Assigned to Me** — Alarms that you are responsible for reviewing.
    - **Alarms Assigned to Others** — All alarms that users on a site are responsible for reviewing.
    - **Acknowledged Alarms** — Alarms that have been previously viewed and acknowledged.
3. In the displayed panels, the Alarm Triggers box lists each time the alarm was triggered while the alarm was active. For Face Watch List Match alarms, select a timestamp to view video from a specific trigger.
4. In the displayed panels, depending on the current state of the alarm, select one of the options.
    - **Acknowledge** — Marks the alarm as being viewed and acknowledged.
    - **Assign Alarm** — Assigns the alarm to yourself.
    - **Unassign Alarm** — Removes the alarm assignment from yourself.
    - **Purge Alarm** — Clears the alarm and removes the status.
    - **Open In View** — Plays alarm video in a new View.
    - **Bookmark Alarm** — Saves the alarm within the system.

Identity Verification

FOR STANDARD AND ENTERPRISE EDITION

Note: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. Contact your ACM administrator to update your permissions.

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.

- In the top-right corner of an image panel, click and select the door you want to monitor.

  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.

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

Compare the video to the badge photo to verify the person's identity and prevent unauthorized access.

Note: The identity verification image panel does not update while viewing recorded video or another tab.

Monitoring License Plates

FOR ENTERPRISE EDITION

While you monitor video in an image panel, you can also monitor license plates as they are detected by the system.

Enabling License Plate Overlays

When the license plate overlay is enabled, detected 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 ACC Client window, select > **Client Settings** > **Display**.
2. In the Image Overlays: area, select the **License Plate** checkbox.
3. Click **OK**.

When you view live video for a camera that is configured for license plate recognition, the detected license plates are displayed.

Reviewing LPR Watch List 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.

Monitoring POS Transactions

FOR STANDARD AND ENTERPRISE EDITION

If a camera is linked to a point of sale (POS) transaction source, you can monitor transactions while watching video from the linked camera. Each transaction is separated by date and time, with the most recent transaction highlighted in blue.

1. In the top-right corner of the image panel, click .
2. Select a POS transaction source, then click **OK**. Transactions will display in the next image panel.

> **Tip:** Review previous transactions by hovering on the transaction image panel and scrolling up.

Displaying Cameras Linked to POS Sources

1. Click in the POS transaction image panel.
2. Select a camera, then click **OK**.

Browsing the ACM Appliance in the ACC Client

FOR STANDARD AND ENTERPRISE EDITION

If a web page for an ACM appliance was configured, ACC operators can access it in the ACC Client software.

Click and drag URL from the System Explorer to an image panel.

The web page will display in that image panel.

- ACC operators logged in with their ACM credentials will automatically be logged in to the ACM appliance.
- ACC operators without ACM credentials may see a certificate warning when they first open the web page. Click **Trust** to continue to the log in page.

Note:
If the ACM session times out, operators will need to log in again.

- ACC operators logged in with their ACM credentials will automatically be logged in again when they close the dialog box.
- Administrators can change an operator's timeout settings in the ACM appliance.

Using a Map

FOR STANDARD AND ENTERPRISE EDITION

You can open a map in any image panel, then view video or alarms by interacting with the map.

1. To open a map in an image panel, double-click in the System Explorer.
2. When the map appears in an image panel, do any of the following:

To...	Do this...
Review an alarm	When a camera flashes red, an alarm linked to the camera has been

To...	Do this...
	triggered. • Click the camera to monitor the live alarm video.
Display video from a camera on the map	• 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.

Opening a Web Page

FOR STANDARD AND ENTERPRISE EDITION

If your System Explorer contains web pages for quick access to your ACM appliance or related to your surveillance system configured, you can access them in the View tab.

Click and drag URL from the System Explorer to an image panel.

The web page will display in that image panel.

Paused Video

FOR STANDARD AND ENTERPRISE EDITION

An image panel will stop recording and streaming video and display **Paused** if:

- A device is in Standby mode. For more information, see *Configuring Standby Mode* on page 112.

An image panel will display **Standby** if:

- A device connection is lost and it is in failover state. For more information, see *Failover Connections* on page 48.
- An encoder without any camera sources is viewed.

Using Linked Devices

If you have devices linked to cameras, you can control them from the ACC Client software.

Note: Some features are only available if the site has the required license, and if you have the required user permissions.

Granting Door Access

FOR STANDARD AND ENTERPRISE EDITION

Note: To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. Contact your ACM administrator to update your permissions.

If your site is connected to an ACM appliance, you may be able to grant door access from any camera that is linked to a door.

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.

Using Video Intercom

FOR STANDARD AND ENTERPRISE EDITION

Video Intercom allows you to verify the identity of visitors before allowing access to secure areas by answering calls from a device.

1. When a call is displayed, click to answer or to ignore the call.
2. If connected to an ACM appliance, click to allow access.
3. Click to end the call.

   Tip: Multiple ACC operators can answer or join a call, and you can record the conversation to be reviewed later.

Using Audio

FOR STANDARD AND ENTERPRISE EDITION

The camera's microphone and speakers must be enabled before you can listen to or broadcast audio.

Configuring Two-Way Audio

You can choose between Full-duplex audio, which allows simultaneous communication, or Half-duplex audio, which only allows communication from one side at a time.

1. In the top-right corner of the ACC Client, select > **Client Settings**.
2. In the Client Duplex Audio Setting: area, select **Full-duplex** or **Half-duplex**.
3. Click **OK**.

Listening to Audio

When an audio input device is linked to a camera, the button is displayed in the image panel of the camera's video. By default, the audio is muted.

- In the lower-right corner of the image panel, click to mute or activate the audio.
- Move the slider to change the volume.

Broadcasting Audio in a View

When speakers are linked to a camera, the button is displayed in the image panel of the camera's video. This button allows you to broadcast audio from the camera through your computer's microphone, like a Public Address (PA) system.

1. To broadcast audio, hold and speak into your microphone. The moving red bar confirms your microphone's levels. If the level is low, speak louder or adjust the microphone volume in the Windows Control Panel.
2. Release the button to stop the broadcast.

Triggering Digital Outputs

FOR STANDARD AND ENTERPRISE EDITION

While you monitor live video in an image panel, you can manually trigger any digital output that is connected to the camera.

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.

Managing Views

Operators can monitor live and recorded video in a View tab. The View tab contains a layout of image panels that lets you organize how video is displayed.

You can share Views with other users during investigations.

Cycling Cameras

Note: You can only cycle through cameras with a Logical ID.

When there are many cameras across your site, cycle through those cameras to preview video before opening them in a new image panel.

- Hold / and press + to preview the next camera.
- Hold / and press - to preview the previous camera.

For more shortcuts, see *Keyboard Commands* on page 194.

Cycling Cameras across Sites

FOR ENTERPRISE EDITION

To cycle through cameras from all sites that you are logged in to, update your Client Settings.

1. In the top-right corner of the Client, select > **Client Settings**.
2. Select the **Display next camera by logical ID across all sites** checkbox.
3. Click **OK**.

Adding and Removing Views

In the ACC Client software, you'll use Views to monitor video. Each View is its own tab and can display multiple different cameras.

1. Click to add another View.
2. To close a view, click .

For more information, see *Adding and Removing Cameras* on page 156.

Maximizing Views

In the toolbar, click to maximize the View. Click to return to the previous size.

Cycling Views

If you have multiple View tabs open, you can cycle through them by displaying each one a few seconds at a time.

1. Access cycle settings by clicking > **Client Settings** > **General**.
2. Set the **Cycle dwell time:** to decide how long a camera will display.
3. Click **OK**.
4. In your View tab, click to enable cycling. Clicking again will disable cycling.

View Layouts

Customize the number and shape of image panels in your View by editing the View Layout.

1. In the toolbar, click .
2. Select a configured layout or click **Edit Layouts** to create a custom configuration.
3. If you are creating a custom configuration, select a layout and enter the number of columns and rows.

   > **Tip:** Click on the dotted or red borders to increase or decrease the size of an image panel. Up to 64 cameras can fit in a View.

4. Click **OK** to save.

Saving Views

FOR STANDARD AND ENTERPRISE EDITION

After you've customized a View, you can save and share it with users across your site. Saved Views appear in the System Explorer.

Saving a View

1. In the toolbar, click > **Save As New View**.
2. Select the site you'll add the view to, assign a name, and then add a unique number as the Logical ID to mark the view in your site.

   > **Tip:** Click to choose where to display the View in the System Explorer.

3. Click **OK** to save your view.

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. In the toolbar, select > **Update Saved View**.

Renaming a View

1. In the System Explorer, right-click and select **Edit** or **Delete**.
2. Update the Name or Logical ID.
3. Click **OK** to update the View.

Deleting a Saved View

1. In the System Explorer, right-click and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Shared Views

FOR ENTERPRISE EDITION

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 View toolbar, click .
2. 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, close the View tab.

Searching

You can quickly search through a camera's recorded history for video of an event.

Search can be accessed in the following ways:

- In the New Task menu , select a Search option.
- In Recorded mode, click in the image overlay and draw a box around the object of interest to perform Appearance Search on the object, or click in the toolbar and then select a Search option.
- While viewing recorded video, click in the image panel and then select a Search option. This search will only be performed on the selected camera video.

Note: Some features are only available if the site has the required license, and if you have the required user permissions.

Avigilon Appearance Search™ Feature

FOR ENTERPRISE EDITION

If you have video analytics cameras with the Avigilon Appearance Search feature enabled, you can search your site for persons or vehicles of interest.

Searching by Description

If you have a physical description of a person or vehicle of interest, start an Avigilon Appearance Search query. Searching for vehicles by description requires the ACC Server software version 7.2 or later.

You can select as many or few search criteria as you want. The system ranks results that match all descriptions higher.

> **Note:** When searching for video in both day and night scenes, avoid using color as a search criteria. For example, the color red may appear gray at night.

1. In the New Task menu, click **Appearances** .
2. Select the person or vehicle icon.
3. Select the icons that best represent the person or vehicle description.
4. Click **Date Range** to set the date and time of your search.
5. Click **Cameras** to select the cameras you want to include in the search. By default, all cameras enabled with the Avigilon Appearance Search feature are selected.
6. Click **Search**.

   Only the first 15 minutes of search results are displayed, regardless of the Date Range selected. Move the Search Results Graph window to view more results.

   For more information, see *Avigilon Appearance Search Results* on the next page.

Searching Recorded Video

You can start a search for both people and vehicles of interest based on one instance in recorded video.

1. Complete a Motion, Thumbnails, Alarm or Identity search, or use the Timeline to find the person or vehicle of interest.
2. Click the bounding box around the person or vehicle and select one option:
   - **Find Appearances After This** — Search for instances of the person or vehicle after this event.
   - **Find Appearances Before This** — Search for instances of the person or vehicle before this event.
   - **Additional Search Options** — Select cameras and a time range before performing the search.

Only the first or last 15 minutes of search results are displayed, regardless of the Date Range selected. Move the Search Results Graph window to view more results.

For more information, see *Avigilon Appearance Search Results* below.

Searching by Uploaded Photo

Search for a person of interest by uploading a photo of the face or body. Or upload a photo of a vehicle of interest. If you have a photo with more than one object, separate them into individual photos. A photo with more than one object cannot be searched.

1. In the New Task menu , click **Appearances** .
2. Click Photo in the Appearance Search Options window.
3. Click **Choose File** or drag and drop the file from your desktop or folder. The accepted formats are .jpg, .jpeg, .bmp, .gif, tif and .tiff.

   The photo is automatically cropped, and if searched, is retained for a specific amount of time. For more information, see *Identity Data Retention* on page 41.
4. Search for the person or vehicle in video footage:
   a. Click **Date Range** to set the date and time of your search.
   b. Click **Cameras** to select the cameras you want to include in the search. By default, all cameras enabled with the Avigilon Appearance Search feature are selected.
   c. Optional. Fill out the **Reason for Search**.
   d. Click **Search**.

   For more information, see *Avigilon Appearance Search Results* below.

Avigilon Appearance Search Results

The search results may not always match the person or vehicle of interest. Refine your results before they are saved.

> **Note:** Only the first 15 minutes of search results are displayed, regardless of the Date Range selected. Move the Search Results Graph window to view more results.

Refining Results

1. Use the **Search Results Graph** or **Timeline** to view additional results. Click to edit the date range.
2. In the top-left area, click **Change Cameras** to add or remove cameras from the search.
3. For description searches, update the search criteria in the **Appearance Description** area.
4. If a search result matches the person or vehicle of interest, hover over a thumbnail and click ☆. This improves the system's accuracy.

> **Tip:** If there are multiple objects in the scene, a white bounding box outlines the match detected by the system. Hover over a thumbnail and click to zoom in on the image from the search result.

Saving Results

When you have verified search results, you can either bookmark or export them.

- Click to bookmark all starred results.
- Click to export all starred results.

  For Native video exports, select the **Password Protection:** and **Include Identity Data:** checkboxes to enable LPR, Appearance, or Face Recognition data in the Avigilon Player.

  For AVI video exports, select the **Blur background** checkbox to obscure everything except the detected person or vehicle.

> **Tip:** Hover over a thumbnail and select the checkbox of all results you want to star, bookmark, export, or remove.

Identity Search

FOR STANDARD AND ENTERPRISE EDITION

> **Note:** To use this feature, your ACM identity must be imported into the ACC software and have the appropriate ACM permissions. Contact your ACM administrator to update your permissions.

You can search for an individual by their name or badge ID. This search displays door events using the person's badge, as well as video from linked cameras.

1. In the New Task menu, click **Identity**.
2. Enter the person's name or badge ID and press **Enter**.
3. Select the person of interest.
4. Click **Date Range** to set the date and time of your search.
5. Click **Doors** to select the doors to include.
6. Click **Search**.

   Up to 50 of the person of interest's most recent door events are displayed. Thumbnails of video from linked cameras are displayed under each door event. For more information, see *Identity Search Results* on the next page.

Identity Search Results

A search result may show video from 5 seconds before or after a door event. This video may not always match the person of interest, and some search results may not have video if the camera was not scheduled to record at that time.

Review and refine your results as needed.

Refining Results

1. In the **Identity Details** area, select what types of door events to show.
2. In the top-left area, click **Change Doors** to add or remove doors from the search. Click to edit the date range.
3. Click a thumbnail to view associated video in the image panel. Click to zoom in on the image from the video.
4. If you have cameras with the Avigilon Appearance Search feature enabled and linked to doors, select **Appearances Only**.

   > **Tip:** Hover over the thumbnail and click to start an Avigilon Appearance Search query.

Saving Results

- Hover over a thumbnail and select the checkbox of all results you want to bookmark or export.
  - Click **Bookmark** to save the event for quick access.
  - Click **Export** to download a copy of the event.

    For AVI video exports, select the **Blur background** checkbox to obscure everything except the detected person.

Searching Alarms

FOR ENTERPRISE EDITION

All alarms that are triggered across your site can be searched.

1. In the New Task menu under Search, click **Alarms** .
2. Select all of the alarms to include in your search.
3. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
4. Click **Search**.

   Your search results are displayed. For more information, see *Reviewing Search Results* on page 186.

Searching Events

Search for configured events in recorded video.

1. In the New Task menu, click **Events**.
2. Select the cameras to include in your search.
3. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
4. Select the type of events to include in your search:
    - **Motion** — Motion was detected in the target area.
    - **Digital Input** — A signal was sent from a device.
    - **Classified Object** — A person or vehicle was detected in the configured region of interest.
    - **Tampering** — An unexpected change in the scene was detected.
    - **ONVIF** — A third-party ONVIF device event was detected.
    - **Presence** or **Presence Dwell** — The Avigilon Presence Detector sensor detected an individual.
    - **Unusual Motion** — Unusual pixel motion was detected.
    - **Unusual Activity** — A classified object behaving unusually was detected.
    - **Face Watch List Match** — A watch list match was detected.
    - **Person Without Mask** — A person without a face mask was detected.
5. Click **Search**.

    Your search results are displayed. For more information, see *Reviewing Search Results* on page 186.

Searching Motion

Search for motion events from cameras configured for Classified Object Motion or Pixel Motion detection events.

Classified Object Motion

1. In the New Task menu, click **Motion**.
2. Select the cameras to include in your search.
3. Select **Classified Object Motion** and update the following:
    - **Object Types:** — select the objects to search for.
    - **Confidence:** — set how certain the system must be that it identified the correct object type.
    - **Minimum Threshold Time:** — set how long the object must be in the scene before it is considered a search result.
    - **Show Results As:** — select whether to display each classified object as an individual search result or as a single search result if multiple objects are detected within the time entered.
4. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
5. In the camera preview, adjust the green region of interest to specify the search area. You can add or remove areas to exclude from the search as needed.
6. Click **Search**.

    Your search results are displayed. For more information, see *Reviewing Search Results* on page 186.

Pixel Motion

1. In the New Task menu , click **Motion** .
2. Select the cameras to include in your search.
3. Select **Pixel Motion** and update the following:
   - **Motion Activity Image Overlay:** — highlights detected motion with a red overlay if enabled.
   - **Threshold:** — specify how many pixels must move to be defined as motion. A higher threshold provides fewer false results.
   - **Join results less than** — set the minimum time between search results. Enter up to 100 seconds.
4. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
5. In the camera preview, adjust the green region of interest to specify the search area.
6. Click **Search**.

   Your search results are displayed. For more information, see *Reviewing Search Results* on page 186.

Searching License Plates

FOR ENTERPRISE EDITION

With License Plate Recognition (LPR) configured, you can search your site for a specific license plate.

1. In the New Task menu , click **LPR** .
2. Select the cameras to include in your search.
3. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
4. Enter the license plate number you are searching for and select the minimum Match percent.

   The Match percent is how similar the detected plates must be to the search query to be displayed as a result. A higher percent will result in fewer false positives while a lower percent will result in more events.

   If no license plate number is entered, the system will search for all detected license plates over the selected search period.

5. Click **Search**.

   Your search results are displayed. For more information, see *Reviewing Search Results* on page 186.

   The **Confidence** column displays how confident the algorithm is that the detected plate number is the actual plate number.

Searching Text Source Transactions

FOR STANDARD AND ENTERPRISE EDITION

Search for specific transactions recorded by a point of sale (POS) transaction source.

1. In the New Task menu , click **Text Source Transactions** .
2. Select the POS transaction sources you want to include in your search.
3. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
4. In the **Search Text:** field, add any product name or transaction value you want included in your search.

   > **Tip:** Leaving the text field blank will search for all transactions.

5. Click **Search**.

   Your search results are displayed. For more information, see *Reviewing Search Results* on the next page.

Searching Thumbnails

When examining video for changes, use the Thumbnail search to display a series of comparison images over time.

1. In the New Task menu , click **Thumbnails** .
2. Select the cameras to include in your search.
3. Enter a **Date Range** or use the Timeline range markers to set the date and time of your search.
4. Click **Search**.
5. Double-click a thumbnail to narrow your search or click **Open In View** to display the result in a new View tab.

   > **Tip:** Click Step Out to return to the previous series of thumbnails.

Searching by Drawing Box Around Object of Interest

Search for a person or vehicle of interest by drawing a box around the face or body. Only a single object can be searched at a time.

1. In Recorded mode, click in the image panel.
2. Draw a box around the person or vehicle of interest. A photo is automatically uploaded.
3. In the Appearance Search Options window:
   a. Click **Date Range** to set the date and time of your search.
   b. Click **Cameras** to select the cameras you want to include in the search. By default, all cameras enabled with the Avigilon Appearance Search feature are selected.
   c. Optional. Fill out the **Reason for Search**.
   d. Click **Search**.

For more information, see *Avigilon Appearance Search Results* on page 180.

Reviewing Search Results

After completing a search, you can review and save your results.

Reviewing Results

- Use the Timeline to watch and review the event video.
- Click **Add to new View** to display the results in a View tab.
- Click **Perform a motion search on this event** to further refine your search.

Saving Results

- Click **Export this event** to download a copy of the event as a video, image, or audio. For more information, see *Exporting* below.
- Click **Export results to a file** to download a CSV or text file of search results.
- Click **Bookmark this event** to save the event for quick access. For more information, see *Bookmarking Recorded Video* on page 189.

Exporting

You can export content in multiple video and image formats. You can export bookmarks, search results, and video from the Timeline. You can also export snapshots of an image panel as you monitor video.

Note: The Windows operating system does not allow special characters to be used in file names. When exporting bookmarks, special characters in a bookmark name are replaced by underscores (_) for the file name to be valid in Windows.

Adding Content to Export

As you investigate video, you can queue content that you want to export.

- **Search Results and Bookmarks** — Click **Export this event**.
- **Timeline** — Right-click the Timeline and select **Add Export**.
- **Snapshot** — In an image panel, click .

  A notification confirms that the file was added to the list.

  Continue working or click the link in the notification to open the Export tab. Each export file is

displayed in the order it was added.

> **Note:** Only snapshots of recorded video are added to the Export tab. Snapshots of live video are exported individually in Live Snapshot tabs.

You can also add content directly in the Export tab:

1. In the New Task menu ☰, click **Export**.
2. Click **Add** and select the type of file you want to export:
   - **Video** — Export as a Native AVE or AVI file. The Native format requires the Avigilon Player software, which lets users view recorded video with Timeline controls and search capabilities.

     For Native video exports, select the **Password Protection:** and **Include Identity Data:** checkboxes to enable LPR, Appearance, or Face Recognition data in the Avigilon Player.
   - **Image** — Export as a JPEG, TIFF, or PNG file.
   - **Audio** — Export as a WAV file.
   - **Document** — Export as a PDF file with notes or send a file directly to your printer.
   - **Video History** — Export content from live video you viewed. For more information, see *Exporting Video History* below.
3. Update the export options. For more information, see *Export Options* on the next page.

Combining Export Files

Export files can contain several clips and images from your investigation.

- To combine files, drag and drop. Expand and collapse the file to show and hide its clips.
- To add a clip to a file, click +.
- To remove a clip from file, click ×.
- To rename a file, double-click its name and enter a new name. Click outside the field to save.

Exporting Video History

You can export clips of video that was viewed live.

1. In the New Task menu ☰, click **Export**.
2. Click **Add** > **Video History**.
3. Select the cameras and enter a date range to search.
4. Click **Search**.

   A list of devices viewed is displayed.

- **View Time** — When the video was viewed.
- **Video Start Time** and **Video End Time** — The clip length.
- **Device** — The camera viewed.
- **Workstation** — The workstation that viewed the video.

5. Select the clip you want to export. Use the `Ctrl` and `Shift` keys to select multiple clips.
6. Click **Add to Export**.

   A Native AVE file is added to your Export list. Expand the file to view and edit the selected clips.

Exporting Files

1. In the Export tab, select the files you want to export.
2. Click **Export**.

   A warning is displayed if your files may contain identity data but the Password Protection: and Include Identity Data: checkboxes were not selected.

3. Select a folder and then click **Select Folder** to start the export.

   While the export is in progress, you can Pause , Resume , or Cancel the export.

   When the export is complete, click to open the file location.

   - To edit and re-export the file, click .
   - To clear the file from the list, click .
   - To clear all finished files, click **Clear finished**.

> **Tip:** To export a video to a disc, place a writable disc in the drive and click **Burn to Disc**.

Export Options

The following table displays the options available for different export formats.

Format	Export Options
Native AVE video	• **Image Rate:** Select a high image rate to maintain quality or a low one to reduce the file size. • **Maximum file size:** The export file will not exceed this size. • **Include Identity Data:** The export file will contain LPR, Appearance, or Face Recognition data. The export must be password-protected to enable this. • **Password Protection:** Select to add a password. • **Export Avigilon Player:** Select to include a copy of the Avigilon Player

Format	Export Options
	with the export file.
AVI video	• **Resolution:** Select the export video resolution. • **Overlays:** Select the video overlays to include. • **Change Image Region...** Select the field of view to export.
Images and print	• **Quality:** Select the image quality. • **Resolution:** Select the export image resolution. • **Images to Export:** Select the number of images to export from the selected time range. • **Overlays:** Select the image overlays to include. • **Change Image Region...** Select the field of view to export. • **Display Adjustments...** Adjust the Black, White, and Gamma levels. • **Add Export Notes...** Enter text to include with the PDF or print image. • **Printer Settings...** Select your printer and adjust print settings.

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**.
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.

   You can only bookmark multiple cameras from the same site.
4. Enter a **Time Range to Bookmark:** or move the black time range markers on the Timeline.
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** checkbox.

   Note: Protected bookmarks are never deleted. These videos take up space and can become the oldest video on the server.

7. To make the bookmark private, select the **Bookmark is private** checkbox. 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**.

Managing Bookmarks

1. In the New Task menu , click **Bookmarks** .
2. In the **Search** field, enter the bookmark name to find it in the list.
3. Select a bookmark and use the Timeline to review the video.
4. Select one or more bookmarks, and click one of the following:
   - — Prevents the video from being deleted. These videos take up space and can become the oldest video on the server.
   - — Removes protection.
   - — Exports the video.
   - — Removes the bookmark tag from the recorded video.
   - **Perform a motion search on this event** — Begins a Motion Search.
   - **Edit this bookmark** — Updates the bookmark name, description, time range, or cameras.
   - **Export results to a file** — Exports a CSV or text file of all the bookmark details.

   Note: The Windows operating system does not allow special characters to be used in file names. When exporting bookmarks, special characters in a bookmark name are replaced by underscores (_) for the file name to be valid in Windows.

Archiving Recorded Video

FOR STANDARD AND ENTERPRISE EDITION

Storage Management must be enabled in the Avigilon Control Center Admin Tool or ES device web interface before you can archive video.

You can archive video from any number of cameras in your system for an extended time range.

Files are always archived in Avigilon Backup (AVK) format and playable using the Avigilon Player.

1. In the New Task menu , click **Archive** .
2. In the System Explorer, select all cameras from a single server that you want to archive.
3. In **Archive Options**, set the time range of the archive.
4. Select the **Delete oldest archives when disk full** checkbox will overwrite old archive files when the archive folder is full.

   > **Note:** 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 Emergency Privilege Override

If you are part of a group with emergency override privileges, you can enable access to high-resolution live and recorded video, including video recorded before you logged in, and control PTZ cameras, microphones, and speakers. To configure your group permissions, see *Emergency Privilege Override* on page 90.

1. In the System Explorer, right-click a site and select **Enable Emergency Override**.
2. Click **Yes** in the following dialog box.

Emergency privilege override will be disabled once you log out or if you right-click the site and select **Disable Emergency Override**.

> **Note:** If you are part of a group with emergency override privileges but do not see the Enable Emergency Override option, you may already have access to all emergency privileges.

Additional Support

Reporting Issues

If an error occurs in the ACC software, you can contact Avigilon Technical Support using **this form** or call +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**.

Anonymous Data Collection

To improve our products and features, Avigilon collects anonymous usage data from your ACC site if it is connected to the internet. No personal information is collected. For more information, see our **Privacy Statement**.

To opt out:

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **General** .
3. Clear the **Send anonymous usage data:** checkbox.
4. Click **OK**.
5. In the top-right corner, click > **Client Settings**.
6. In the General tab, clear the **Send anonymous usage data** checkbox.

Basic ACC System Health Check

When there are ACC issues, perform these steps before contacting Technical Support. The basic ACC system check involves the following:

1. Check for server hardware problems.
2. Ensure ACC Server and ACC Client (and other ACC components) are the same version.
3. Ensure the server is protected by a UPS. Click **here** for more details.
4. Check antivirus configuration. Ensure ACC applications are in the exclusion list of the antivirus. Click **here** for more details.
5. Check server NIC configuration. Ensure server NICs have the correct IP addresses. Click **here** for more details.

   Important: To review all the IP addresses in one place, see ACC *Site Health* on page 20. Before you change the IP address of a server that is a member of a multi-server site or a parent-child site family configuration:

   - If the new IP address configuration brings all servers to the same IP subnet (i.e., same broadcast domain/network):
     - Remove server from site and/or (if applicable) disconnect server from parent site.
     - Shut down ACC Server.
     - Set/change IP addresses and/or Windows computer name. Changing the Windows computer name requires a reboot.
     - Start ACC Server and add back to the multi-server site or re-connect to parent site.
   - If the new IP address configuration brings all servers to a different IP subnet (i.e., different broadcast domain/network):
     - Prepare remote access for each server that needs a new/change of IP address.
     - Call Technical Support. This involves temporarily removing the server from the multi-server site and putting the server offline for a few minutes (depending on how fast the server shuts down and restarts). More steps need to be done by Technical Support before the server is put back to the multi-server site.
6. Ensure each server NIC is not overloaded. Generate a Site Health Report. Compare the bandwidth usage of server NICs with the server recording and playback limits. Refer to the server datasheet on the **Avigilon Video Infrastructure** product page.
7. Ensure Drive C is not used as an ACC Data Volume.
8. Ensure Drive C has at least 20 GB of free space.
9. Ensure each device that is connected to ACC as ONVIF has the correct time zone, date and time details and is synchronized to a time/NTP server. To review the IP addresses and connection type (ONVIF) of all the connected cameras, see ACC *Site Health* on page 20.
10. For more information, see the **Pre-Site Checklist** in the *Initial ACC System Setup and Workflow Guide*.

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.

> **Tip:** Several commands require a camera's Logical ID.

> **Note:** Some features are only available if the site has the required license, and if you have the required user permissions.

Image Panel and 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	+ *<image panel #>* +
Display a specific camera in the View A device's Logical ID is required.	/ + *<logical ID>* + Enter	+ *<logical ID>* +
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	+ 0 +
Remove camera from the selected image panel	Backspace	

Command	Key Combination	Keypad Combination (Image Panel buttons)
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 For recorded video	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. In a Video Intercom panel, press to mute microphone. Press again to unmute.	 Hold to speak. Release to stop 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	

Command	Key Combination	Keypad Combination (Image Panel buttons)
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	
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>*	+ *<logical ID>* +
Open a Virtual Matrix monitor The Virtual Matrix monitor's	Ctrl + G + *<logical ID>*	+ *<logical ID>* +

Command	Key Combination	Keypad Combination (View buttons)
Logical ID: is required.		

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
Change to next layout	Alt +]	
Change to previous layout	Alt + [	

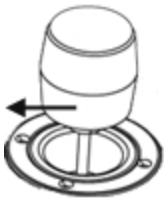
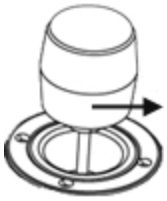
Playback Commands

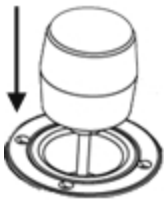
Command	Key Combination	Keypad Combination (Timeline buttons)
Play/Pause video playback	Spacebar	

Command	Key Combination	Keypad Combination (Timeline buttons)
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 + ←	
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	Ctrl + C	

Command	Key Combination	Keypad Combination (Timeline buttons)
marker		

PTZ Commands (Digital and Mechanical)

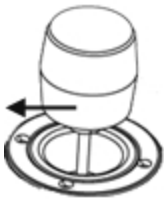
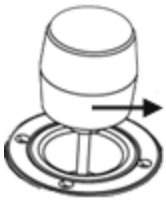
Command	Key Combination	Keypad Combination (PTZ buttons)
Toggle PTZ controls	Ctrl + D	
Zoom in	+	
Zoom out	–	
Pan left	←	
Pan right	→	
Tilt up	↑	

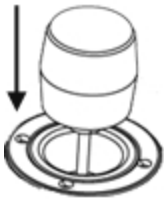
Command	Key Combination	Keypad Combination (PTZ buttons)
Tilt down	↓	
Open iris	Home	
Close iris	End	
Focus near	Insert	
Focus far	Delete	
PTZ menu left	←	
PTZ menu right	→	
PTZ menu up	↑	
PTZ menu down	↓	
Activate preset	Q + *<Preset #>*	PRESET + *<Preset #>* + ENTER
Run pattern		PATTERN + *<Pattern #>* + ENTER
Start auxiliary	W + *<Aux #>*	START + *<Aux #>* + ENTER
Stop auxiliary	E + *<Aux #>*	STOP + *<Aux #>* + ENTER

Joystick Controls

The ACC Client software supports two types of joysticks, the Avigilon USB Professional Joystick Keyboard and standard USB joysticks. After your joystick has been configured, you can use it to pan, tilt, zoom, and more.

Note: Some third-party joysticks may require additional custom configuration.

Command	Keyboard	Joystick
Toggle PTZ Control	Ctrl + D	
Zoom In	+	
Zoom Out	–	
Pan Left	←	
Pan Right	→	
Tilt Up	↑	

Command	Keyboard	Joystick
Tilt Down	↓	
Open Iris	Home	
Close Iris	End	
Focus Near	Insert	
Focus Far	Delete	
Move Menu Left	←	
Move Menu Right	→	
Move Menu Up	↑	
Move Menu Down	↓	
Activate Preset	Q + <Preset #>	PRESET + <Preset #> + ENTER
Run Pattern		PATTERN + <Pattern #> + ENTER
Start Auxiliary	W + <Aux #>	START + <Aux #> + ENTER
Stop Auxiliary	E + <Aux #>	STOP + <Aux #> + ENTER