avigilon™

Avigilon Control Center™ and Access Control Manager™ Unification Guide

For ACC software version 7.14.16 and ACM physical or virtual version 6.36 or newer

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-ACC7ACM-U-G

Revision: 6 - EN

20230302

Table of Contents

Introduction

The Avigilon Control Center (ACC) software can be combined with the Access Control Manager (ACM) appliance to provide enhanced security and surveillance for your organization.

This document describes how to configure your ACM appliance and your ACC software to interact seamlessly. Once your ACM appliance, roles, and identities are connected to the ACC software, you can create rules for access control events and grant door access and perform identity verification from ACC. You can bookmark, export, and archive video connected to ACM panels, subpanels, and inputs.

System Requirements

For the best performance and full functionality, use the latest versions of the ACC Client and Server software and the ACM system.

To access the ACM appliance, you will need:

- An Internet connection.
- A web browser.

Avigilon Certified Solution

- Single ACM physical or virtual instance
- 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.
- Servers — NVR Premium, Standard, or Value
  - Optimized for video surveillance applications in a 24/7/365 environment.
  - ACC software is preinstalled, configured and enhanced for optimal system compatibility.
  - Certified for the Avigilon surveillance environment — ACC software, LPR, Web Endpoint, Analytics, HDSM™ and 1-30 MP cameras.
  - High throughput of up to 1800 Mbps.
  - Documented network architecture for a wide-variety of applications.
  - Avigilon warranty and support included.
  - Access to Avigilon System Design Tool (SDT) to calculate storage requirements.

- Workstations — HD Video Appliance or NVR Workstation
  - Preloaded and configured with ACC video management software.
  - High-performance recording capacity.
  - Supports high resolution monitors.
  - Throughput of up to 400 Mbps.
  - Avigilon warranty and support included.
  - Access to Avigilon SDT to calculate storage requirements.

ACC Client Software Requirements

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

ACC Server Software and Workstation Requirements

ACC Server Software

System Requirement	Recommended	Minimum
OS*	Windows Server 2016	Windows Server 2012 R2 / 2016 / 2019, Windows 8.1 (64-bit) or Windows 10 (64-bit)
Processor	Intel® Xeon® E5 v3 (6 cores, 1.9 GHz)	x86 64-bit (dual-core, 1.9 GHz)
Memory	16 GB DDR4	4 GB DDR3
Storage	SATA-III 7200 RPM Enterprise Class	SATA-II 7200 RPM Enterprise Class

ACC Server Workstation

System Requirement	Recommended	Minimum
OS*	Windows 10 (64-bit)	Windows 8.1 (64-bit) or Windows 10 (64-bit)

System Requirement	Recommended	Minimum
Processor	8th Generation Intel Celeron® CPU or higher	Intel Quad-core (2.0 GHz)
Memory	8 GB DDR4	4 GB DDR3
Video	NVIDIA® Quadro P620	PCI Express®, DirectX 10.0 compliant with 256 MB RAM
Storage	SATA-III 7200 RPM	SATA-II 7200 RPM

* Run Windows Update before launching the ACC software.

ACC and ACM Unification Recommendations

System Requirement	Minimum	Notes
ACC software	7.14.16	Installation on a dedicated machine. For example, ACC and SALTO ProAccess SPACE server should not be installed on the same machine.
ACM physical or virtual	6.36.0	

Note: Newly added ACM identities are not available in ACC for up to 1 hour after being added (when replication occurs).

ACC Site and ACM Sizing Recommendations

ACM Edition[1]	Maximum ACM Size PANELS, SUBPANELS, INPUTS, DOORS, AND OPERATORS IMPORTED TO ACC	Maximum ACC Sites
Enterprise (4 thread CPU)	4,150	150
Enterprise Plus (8 thread CPU)	6,750	200
Virtual (16 thread CPU)	13,500	250

Note: The maximum number of ACC sites supported may be impacted by high-CPU consuming ACM operations, such as:

- Report generation
- Global anti-passback
- Large number of IP gateways
- Operators that continuously switch between the ACM application pages
- Integrations that use the ACM REST API

[1] The recommendations do not apply to the Professional edition.

ACM™ and ACC™ Configuration

Note: Currently, ACM and ACC failover systems are not supported when an ACM appliance is connected to an ACC site.

To connect the ACM appliance to the ACC site, an administrator must do the following:

1. Configure the ACM appliance.
2. Connect the ACM appliance to an ACC site.
3. Configure ACM features in the ACC software.

Each process is described below.

Configuring the ACM Appliance

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. Ensure the **ACC Administrator** has the following rights:
    - Appliance Listing
    - Delegations Listing
    - Doors Grant
    - Doors Listing
    - Force Password Change
    - Identities Listing
    - Identities Login - Remote
    - Identities Photo Render
    - Inputs Listing
    - Panels Listing
    - Partitions List
    - Roles Listing
    - Subpanels Listing

- System Summary Listing
- REST Appliance Status Display
- REST Get Doors
- REST Get Identities
- REST Get Identity
- REST Get Inputs
- REST Get Panels
- REST Get Right Groups
- REST Get Roles
- REST Get Subpanels

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 **ACC Administrator** 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. Uncheck the **Force Password Change** checkbox. Do not enable MFA for the ACC user account.
   - 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 the ACM Appliance to an ACC Site

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 AC *Hostname* in the Setup tab.

Configuring ACM Features in ACC

Importing ACM Roles

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.
- 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.

For more information on managing groups, see the ACC Client Help files.

Linking Doors to Cameras

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.

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.

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

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 list of ACM rules, actions, and conditions, see *Rule Event and Action Descriptions* on page 19.

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:**.
7. Click ✓ to save the new rule.

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 URL up and down the right pane to set where it is displayed.
    - If your site includes 🏢 folders, select a location for the web page URL in the left pane. The right pane updates to show what is stored in that directory.
5. Click **OK**.

Monitoring Doors

After the ACM appliance and ACC software are configured, ACC operators with access rights to the doors in ACM can monitor door activity.

Granting Door Access

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.

Identity Verification

If your camera is linked to a door in the ACM appliance, you can monitor authorized and unauthorized door activity in an adjacent image panel.

- 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.

Identity Search

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* below.

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.

Browsing the ACM Appliance in the ACC Client

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.

Rule Event and Action Descriptions

The following tables describe the trigger events, actions, and conditions that are available when you set up a rule.

Note: Some actions are only available for ACC Enterprise edition software.

Rule Events

Rule events are the events that trigger a rule.

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 • Invalid card format • Invalid PIN only request

Event	Description
	- 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
Input activated	An installed ACM panel or subpanel input was activated.
Input deactivated	An installed ACM panel or subpanel input was

Event	Description
	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 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.

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**.