# Access Control Manager™ 5.10.0 Release Notes

Version 5.10.0 – Released Wednesday, April 05, 2017

## Files Released

### Avigilon Access Control Manager Physical Appliance Files

- 5.10.0-upgrade

### Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.10.0.ova
- ACM_VM_5.10.0.zip

## Upgrade Path

1. There is no direct upgrade path to ACM 5.10.0 from revisions prior to ACM 5.6.0. The system must first be upgraded to ACM 5.6.0 and then to 5.10.0.
   The upgrade package for ACM 5.6.0 is available at ftp://ftp.avigilon.com/ACM/5.6.0/
   The release notes for ACM 5.6.0 is available at ftp://ftp.avigilon.com/ACM/5.6.0/ACM 5.6.0 Release Notes v2.pdf

2. There is no direct upgrade path to ACM 5.6.0 from revisions prior to ACM 5.2.0. The system must first be upgraded to ACM 5.2.0 and then to 5.6.0.
   The upgrade package for ACM 5.2.0 is available at ftp://ftp.avigilon.com/ACM/5.2.0/
   The release notes for ACM 5.2.0 is available at ftp://ftp.avigilon.com/ACM/5.2.0/ACM 5.2.0 Release Notes.pdf

## ACM Upgrade Instructions

It is not required to use the built in admin account for software upgrade application. ACM delegations needed to upload, run, and delete software upgrades are: Appliances Listing, Appliances Edit, Appliance Software Listing, Appliance Software Apply, Appliance Software New (for adding upgrades) and Appliance Software Delete (for deleting upgrades). Any login with these delegations in its role(s) can administer and apply software upgrades for a physical or virtual appliance.

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

## ACM Upgrade Instructions (continued)

1. The upgrade instructions can be found in Access Control Manager (ACM) help menu
   a. After logging in to Access Control Manager, select Help near the top left of the browser window and search for “updating appliance software”

*Note: The Enable Remote TCP/IP Management option has been disabled on all ACM upgrades starting with the ACM 5.6.4 release.*

## ACM with ACC Integration Upgrade Instructions

1. NOTE: Previous versions to 5.8.4.12_SR1 of AvigilonAcmIntegrations are not compatible with ACM 5.10.0. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.
2. Instructions for installing the AvigilonAcmIntegration-5.8.4.12_SR1
   a. Download AvigilonAcmIntegration-5.8.4.12_SR1from http://avigilon.com/support-and-downloads/for-software/acc-integration-and-plug-in-downloads/
   b. Make a backup copy of Avigilon\ACM to ACC Integration\ACM to ACC Alarm Gateway\AlarmConfig.xml
   c. Uninstall previous version of the AvigilonAcmIntegration
   d. Reboot the appliance (ACC) that the integration was installed on
   e. Install the AvigilonAcmIntegration-5.8.4.12_SR1
   f. Ensure Vidproxy service is running
   g. Login to the upgraded 5.10.0 ACM appliance. Navigate to Settings/External Systems, select the Avigilon tab; select the appropriate ACC Integration IP link from the list (may be more than one). Click on the Save button to reinitialize the handshake between ACM and ACC. Wait until the “Avigilon Server was successfully updated” prompt is presented and camera status for each camera shows display of “Online”. Verify camera streaming

## ACM with replication Upgrade Instructions

1. For the ACM 5.10.0 upgrade on a replicated system, apply the software upgrade to the appliance with replication address 1 first, while all other appliances in its replicated system are online and replicating data amongst themselves successfully.
2. Allow the upgrade on the replication address 1 appliance to complete and the appliance to reboot and come back online.

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

## ACM with replication Upgrade Instructions (continued)

3. The remaining appliances in the replicated system are allowed be upgraded in any order, and should be upgraded as soon as possible once the replication address 1 appliance is upgraded.
4. On the replication address 1 appliance, once the upgrade is complete the user interface will return to a login screen, and when the user logs back into the appliance the EULA screen will be displayed for acceptance. On the other appliances, the user interface will also be redirected to the login screen after the upgrade completes.

*Note*: All other appliances will not function correctly until the EULA is accepted.

## HID Firmware Upgrade

For systems with HID VertX EVO field hardware, Avigilon recommends upgrade to ACM 5.10.0. The HID firmware is part of the ACM 5.10.0 upgrade package and will allow you to update the HID VertX EVO field hardware with HID firmware version 3.5.2.1837.

- After upgrading the ACM to version 5.10.0, upgrade HID VertX EVO V1000 with RCP 1.8.0.0. The HID firmware version 3.5.2.1837 will be automatically updated as a part of the RCP 1.8.0.0.
- Repeat the upgrade for HID VertX EVO V2000 with RCP 1.8.0.0 and HID firmware version 3.5.1-1483 will be updated automatically.

*Note: ACM 5.6.4 is the first version of ACM to support the migration from Access Control Manager Embedded Controller 1.8.0.0. If your HID firmware is not running 1.8.0.0, please upgrade it.*

## ACM with Bosch Intrusion Upgrade

- ACM 5.10.0 now requires a new Application Passcode in addition to the Automation Passcode (formerly labelled “Password”) be configured to establish the connection with new AND existing intrusion panels.
- The Application Passcode can be found (and set) in RPS under "AUTOMATION / REMOTE APP" / "Remote App Passcode" and in ACM under "Settings/External Systems/Bosch Intrusion/<panel>/Application Passcode".
- This passcode must be set in both ACM and RPS. If it does not match the panel will fail to connect.

*Note: Users upgrading from 5.8.0 and 5.8.2 must setup the new additional security passcode to get the intrusion panels online again in ACM.*

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

## New Features

Functional Features

- Added customization of Mercury LED modes through ACM
- Added functionality to assign doors or access groups to an identity for a scheduled duration
- Added functionality to schedule token activation and expiry for any time of day
  *Note*: *Existing expiry dates will be shifted by one minute (from 12:01AM appliance time to 12:00AM appliance time). New tokens will default to the current appliance time activates "Now", deactivates in "Now + 1 year".*

UI Improvements

- Enhanced the entire look and feel for Doors list screen
  - Added sorting by Device status, Door name, Panel name, Door state and Door mode
  - Added new icons for Device status
  - Improved navigation of Device status, Appliance name and Group name with drop down menus
  - Added advanced filters to sort by Alarms, Door Status and Door modes and the capability to save filters

Performance Improvements

- Reduced load time by 75% when modifying large groups of identities on a physical appliance
- Reduced time required to add a door to an access group with large number of doors
- Reduced time to create an identity for a profile with a large group of identities assigned to it
- Reduced time to filter a transaction report by embossed number for large number of rows
- Reduced time required by an identity collaboration to pull all identities from a remote LDAP database with more than 10K identities down to few minutes

## Changes

## Fixed Issues

- Corrected issue with a collaboration failing due to special characters being used in the window share password field
- Corrected issue with shifting of map icons when ACM is running on chrome

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

## Fixed Issues (continued)

- Corrected issue with badge image not being generated when using special characters in the user defined fields of the badge template
- Corrected search issue with identity groups not returning any results
- Corrected issue with keypad as a configurable parameter model when adding a subpanel
- Corrected issue with the date picker “now” button in calendar schedules appearing to be not clickable
- Corrected Area report issue with the filter name being displayed incorrectly
- Corrected issue with roles not honoring the appliance time zone due to differences in the PC local time zone (Asia) and appliance time zone (UTC) resulting in denied access
- Corrected installation issue due to EULA not allowed to be accepted when installing a new ACM version on a virtual machine
- Corrected translation issue with the badge designer canvas for German, Spanish and Russian languages
- Corrected error resulting from navigating to the Bosch intrusion help for a system with interface language other than English
- Corrected error resulting on the event colors tab when using a numeric and a non-numeric priority code together
- Corrected issue with the "RF loss/Open loop" event being inaccurately logged as "Reader offline" event during an RF failure
- Corrected badge designer GUI issue with elements overlapping and graphics being duplicated for a system with interface language other than English
- Corrected language issue with lockout message when user exceeds maximum login attempts for a system with interface language other than English
- Corrected issue with the SMTP password not honoring a blank field in the appliance SMTP settings
- Corrected "Door Config" report issue displaying all door processing attributes rather than attributes only for door types
- Corrected display issue with incorrect tamper status and door mode for an offline NDE or AD400 door
- Corrected issue with advanced search filters on identities belonging to a group not honoring the search criteria
- Corrected synchronization issue of intrusion panels when a few Bosch panels are added
- Corrected issue with incompatible inputs, outputs and readers being listed in the dropdown when adding a door to a Mercury 1501 panel
- Corrected issue with invalid "Offline Door Mode" field being displayed on the door's parameter tab for AD400 and NDE doors
- Corrected issue with time not being updated when the hour field on the appliance page is manually set to a single digit

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

## Fixed Issues (continued)

- Corrected ACC-ACM alarm gateway issue caused by the Windows 7 firewall resulting in all cameras being offline
- Corrected error resulting from upgrading a system with UK English as the system language
- Corrected issue with subpanel field disappearing when switching from a wireless to a wired subpanel on the door parameter tab
- Corrected photo export issue with collaborations deleting everything in the base folder
- Corrected issue with source field not being retained when saving a panel trigger without a name for a system with interface language other than English
- Corrected translation issues with roles in the available box for a system with interface language other than English
- Corrected translation issues with delegations when filtered by doors for a system with interface language other than English
- Corrected issue with root filesystem of appliance not being set as read only
- Corrected issue with token deactivate date not honoring the token activate date
- Corrected issue with some events not translated for an interface with language that is not English
- Corrected issue that allowed the 'use remote authentication' option to be selected even when there is no remote domain configured to authenticate to

## Known Issues

- Issue: Action group mix-up in global actions
  Description: If a global actions belonging to an action group is clicked, the CN from a previously deleted global action may appear in the edit screen
  Affected Version: ACM 5.8.4
  Workaround: Avoid deleting a global action from an action group
  Fix: Scheduled to be corrected in a service release

- Issue: Disappearance of macro commands
  Description: Deleting a macro command from a newly added macro may lead to commands from other macros to be deleted as well
  Affected Version: ACM 5.8.2
  Workaround: None
  Fix: Scheduled to be corrected in a service release

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

## Firmware Included

### Panel Firmware:

- rcp-update-1.8.0.0
- EP1501-VER-1-21-2.crc
- EP1501-VER-1-22-9.crc
- EP1502-VER-1-21-2.crc
- EP1502-VER-1-22-9.crc
- EP2500-VER-1-21-2.crc
- EP2500-VER-1-22-9.crc
- M5IC-VER-1-20-7.crc
- M5IC-VER-1-22-9.crc
- MSICS-VER-1-22-9.crc
- Scp2-AES-VER-3-120.crc
- Scp2-VER-3-120.crc
- ScpC-AES-VER-3-120.crc
- ScpC-VER-3-120.crc
- ScpE-AES-VER-3-120.crc
- ScpE-VER-3-120.crc

### Sub-Panel Firmware:

- M5-16DO-APPL-VER-1-32-2.aax
- M5-20IN-APPL-VER-1-32-2.aax
- M5-2K-APPL-VER-1-56-13.aax
- M5-2K-APPL-VER-1-56-15.aax
- M5-2RP-APPL-VER-1-57-2.aax
- M5-2RP-APPL-VER-1-57-3.aax
- M5-2SRP-APPL-VER-1-57-2.aax
- M5-2SRP-APPL-VER-1-57-3.aax
- M5-8RP-APPL-VER-1-57-3.aax
- M5-8RP-APPL-VER-1-57-5.aax
- MR16in-APPL-VER-1-31-1.aax
- MR16in-APPL-VER-1-32-1.aax
- MR16out-APPL-VER-1-31-1.aax
- MR16out-APPL-VER-1-32-1.aax
- MR50-APPL-VER-1-51-0.aax
- MR50-APPL-VER-1-52-14.aax
- MR51e-APPL-VER-1-4-8.aax
- MR51e-APPL-VER-1-5-12.aax
- MR52-APPL-VER-1-51-0.aax
- MR52-APPL-VER-1-57-5.aax
- MR52-SERIES1-VER-1-11.aax
- MS-ACS-APPL-VER-1-0-5.aax
- MS-I8S-APPL-VER-1-0-1.aax
- MS-R8S_APPL-VER-1-0-1.aax

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.