Access Control Manager™ 5.10.10 Release Notes

Version 5.10.10– Released Wednesday, February 01, 2018

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.10.10-upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.10.10.ova
- ACM_VM_5.10.10.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.10.10 from revisions prior to ACM 5.6.0. The system must first be upgraded to ACM 5.6.0 and then to 5.10.10.
   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.

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, click on “Appliance” under Setup and Settings.
   b. Go to the “Software Update tab” and select Help near the top right of the browser window.
   c. Search for the link labelled “updating appliance software” for ACM upgrade instructions.

Note: The Enable Remote TCP/IP Management option has been disabled by default on all ACM upgrades starting with the ACM 5.6.4 release. Contact Avigilon Support for instructions on how to enable it.

ACM with ACC Integration Upgrade Instructions

- NOTE: Previous versions to 5.8.4.13 of AvigilonAcmIntegrations are not compatible with ACM 5.10.10. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.
- Instructions for installing the AvigilonAcmIntegration-5.8.4.13
   a. Download AvigilonAcmIntegration- 5.8.4.13 from 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-5.8.4.13
   f. Ensure Vidproxy service is running
   g. Login to the upgraded 5.10.10 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 5.10.10 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.

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 5.10.10. The HID firmware is part of the ACM 5.10.10 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 5.10.10, 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 5.10.10 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.

Notes: - 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.

- For G-series Bosch panels a number of issues have been noted. Avigilon recommends upgrading the Bosch firmware to the latest version i.e. 3.04.015.

New Features

Functional Features

- Added support for SimonsVoss SmartIntego door position switch
- Added RAID 5 support for ACM Enterprise Plus appliance for 256, 512, 1024 and 2048 readers
- Added support for OSDP secure channel
- Added support for Mercury MR serial Input/output (SIO) devices: MR50-S3, MR52-S3, MR16IN-S3 and MR16OUT-S3
- Added support for USB badging camera
- Added support for ViRDI HID iCLASS and Prox AC2000 and AC5000Plus terminals
- Added support for HID RPM firmware 3.6.3 for V1000, V2000, and Embedded Controller
- Added support for SMB Client version 2.00 (samba 4.7.3)

Performance Features

- Reduced time required to download tokens
- Reduced time required to upgrade from ACM 5.6.4
- Reduced time required to load panel listing screen
- Reduced time required to load door listing screen
- Reduced time required to open an existing or add a new elevator access level for a system with large number of schedules
- Reduced time required to execute a REST call for a very large system

Changes

Fixed Issues

- Corrected issue with 2 Person Control failing intermittently due to occupancy counts getting out of sync
- Corrected issue with "Identity Photo Gallery Report" and "Identity Summary Report" Grid view not loading when special characters are used in User Defined Field
- Corrected issue with a partitioned operator being able to remove an object from all partitions that they can view
- Corrected issue with external video integrations no longer working due to the password getting inadvertently removed
- Corrected issue with missing "Partial Credential Attempt" Event
- Corrected issue with backup/restore not working due to incorrectly mounted USB on an Enterprise appliance
- Corrected issue with default ACM values not being fully translated
- Corrected sorting issue with translated drop down menu items
- Corrected issue with scheduled reports not running for a system with ENG-UK locale

Fixed Issues (continued)

- Corrected error resulting from pausing and resuming the Monitor > Events table before it is fully loaded
- Corrected issue initializing constants resulting in warnings logged during upgrades
- Corrected issue with preview mode not working during image capture on a Firefox browser when capturing an image using an IP camera for badging
- Corrected issue with the LE lock not accepting a card credential to turn on Apartment Mode which resulted in the door being locked, while status says "Unlocked (Apartment)"
- Corrected issue with “Use/Lose Threshold” field not enforcing valid data
- Corrected issue with a schedule Audit log failing to generate a PDF for a large amount of data
- Corrected issue with antipassback violations due to an occupancy count mismatches with two man control and hard ABP configured
- Corrected issue with battery alarm event for a SimonsVoss door not being generated
- Corrected issue with incorrectly displaying a SimonsVoss door as online
- Corrected issue with the scheduled custom audit log report erroneously displaying LDAP attribute names instead values
- Corrected issue with the system not being able to connect to a SmartIntego Gateway node when WaveNet format is set to 8bit|8bit
- Corrected issue with the system not limiting the number of subpanels that can be added on Port 2 of EP1501 downstream
- Corrected issue with panel not being saved when attempting to add two panels with identical addresses on two different ACM browsers
- Corrected issue with Simple Macros displaying outputs for SimonsVoss Wireless lock
- Corrected issue door not respecting the “Access Time When Open” parameter when Strike Mode is set to “Full Strike” time
- Corrected issue with emails not being sent when either "Use TLS" or "Use Start TLS" is enabled for SMTP mail settings
- Corrected issue with available hardware vendor not being updated when adding a new panel each time the panel is switched to a replicated appliance
- Corrected issue with Mercury tab disappearing when editing a policy with a door, input and output
- Corrected issue with SSH authorization code not being saved when an appliance is upgraded from ACM 5.10.2 to ACM 5.10.8
- Corrected issue with incorrect user defined field name being displayed in an identity summary and photo gallery report when a filter with a UDF is added to these reports
- Corrected issue with invalid error preventing the addition of SCP Panels
- Added validation to prevent changing the Panel for a door with dependencies
- Corrected issue with time stamp not showing up on the Monitor>Events>Verification page when a token is swiped on an online door the identity has access to

This release addresses the following Common Vulnerabilities and Exposures associated with:

CVE-2017-9613

ACM Known Issues

- Issue: Dates not sorted properly in the monitor when using Russian locale on user account
  Description: Sorting events by dates in the Monitor>Events tab may not adhere to the locale format the user account is set for
  Affected Version: ACM 5.10.4
  Workaround:
  Fix: Scheduled to be corrected in a service release

- Issue: ACM Profile batch update creates job for wrong group
  Description: When scheduling two profile batch updates consecutively for two different group, both updates are applied to the first group.
  Affected Version: ACM 5.10.6
  Workaround: Reload the page before scheduling the next batch update for the update to be executed properly
  Fix: Scheduled to be corrected in a service release

- Issue: ACM may create corrupted roles
  Description: Some roles may get corrupted and prevent access to the appliance for some users.
  Affected Version: ACM 5.10.4
  Workaround: Ensure that the stop date field of the role is not blank
  Fix: Scheduled to be corrected in a service release

- Issue: Monitor search for sources with capital Cyrillic letters may not fetch any results
  Description: Search criteria starting with a Cyrillic upper case on any transaction based report may not fetch results on events
  Affected Version: ACM 5.10.8
  Workaround: Use lower case when using Cyrillic font for door, panels, inputs or output names
  Fix: Scheduled to be corrected in a service release

- Issue: Operator not able to delete identities
  Description: If the operator's account has an apostrophe in its password it won't be able to delete identities

ACM Known Issues (continued)

Affected Version: ACM 5.10.8
Workaround: Avoid using special characters in passwords for administrator accounts
Fix: Scheduled to be corrected in a service release

- Issue: ACM report source filter bugs
  Description: Some source may not come up in the drop down box supposed to contain the result of the search performed with the current text input. Also when trying to search object with a name containing a coma, the UI may select the first item in the list instead of showing the results and start the search for the next item.
  Affected Version: ACM 5.10.8
  Workaround: Copy and paste in the exact names of the sources in search criteria.
  Fix: Scheduled to be corrected in a service release

Firmware Included

Panel Firmware:

- rcp-update-1.8.0.0
- rcp-update-1.8.2.0
- EP1501-VER-1-22-9.crc
- EP1501-VER-1-24-1.crc
- EP1501-VER-1-25-6.crc
- EP1502-VER-1-22-9.crc
- EP1502-VER-1-24-1.crc
- EP1502-VER-1-25-6.crc
- EP2500-VER-1-22-9.crc
- EP2500-VER-1-24-1.crc
- EP2500-VER-1-25-6.crc
- M5IC-VER-1-22-9.crc
- M5IC-VER-1-24-1.crc
- M5IC-VER-1-25-6.crc
- MSICS-VER-1-22-9.crc
- MSICS-VER-1-24-1.crc
- MSICS-VER-1-25-6.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
- M5-16DOR-APPL-VER-1-32-2.aax
- M5-20IN-APPL-VER-1-32-2.aax
- M5-20IN-APPL-VER-1-32-3.aax
- M5-2K_APPL-VER-1-57-6.aax
- M5-2K-APPL-VER-1-56-15.aax
- M5-2RP-APPL-VER-1-57-12.aax
- M5-2RP-APPL-VER-1-57-3.aax
- M5-2SRP-APPL-VER-1-57-12.aax
- M5-2SRP-APPL-VER-1-57-3.aax
- M5-8RP-APPL-VER-1-57-5.aax
- M5-8RP-APPL-VER-1-57-9.aax
- MR16IN-APPL-VER-1-32-1.aax
- MR16IN-APPL-VER-1-32-2.aax
- MR16IN-APPL-VER-3-20-4.aax
- MR16OUT-APPL-VER-1-32-1.aax
- MR16OUT-APPL-VER-1-32-2.aax
- MR16OUT-APPL-VER-3-20-4.aax
- MR50-APPL-VER-1-52-14.aax
- MR50-APPL-VER-1-53-3.aax
- MR50-APPL-VER-3-20-4.aax
- MR51E-APPL-VER-1-5-12.aax
- MR51E-APPL-VER-1-6-12.aax
- MR52-APPL-VER-1-57-13.aax
- MR52-APPL-VER-1-57-5.aax
- MR52-APPL-VER-3-20-4.aax
- MR52-SERIES1-VER-1-11.aax
- MS-ACS-APPL-VER-1-0-5.aax
- MS-ACS-APPL-VER-1-0-6.aax
- MS-I8S-APPL-VER-1-0-1.aax
- MS-R8S_APPL-VER-1-0-1.aax
- MS-R8S-APPL-VER-1-0-2.aax