Access Control Manager™ 5.10.4 Release Notes

Version 5.10.4– Released Monday, August 14, 2017

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.10.4-upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.10.4.ova
- ACM_VM_5.10.4.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.10.4 from revisions prior to ACM 5.6.0. The system must first be upgraded to ACM 5.6.0 and then to 5.10.4.
   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 5.8.4.12_SR1 of AvigilonAcmIntegrations are not compatible with ACM 5.10.4. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.
- 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 5.10.4 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 5.10.4 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 5.10.4. The HID firmware is part of the ACM 5.10.4 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 5.10.4, 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 5.10.4 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 the following ViRDI biometric readers:
  - Finger print terminal with smart card authentication (AC2000SC)
  - Finger print terminal with smart card authentication and LCD screen (AC5000SC-Plus)
  - Fingerprint and smart card enrollment reader (FOH02-SC)
- Added support for the following Simons Voss SmartIntego locks (EMEA only):
  - Digital Smart Handle
    - SI.SHASF8A721CC1A
    - SI.SHAS07C001CC1A
    - SI.SHASF8C001CC1A
    - SI.SHBS08C051CC1A
  - Digital cylinder
    - SI.Z4.30-30.MI.CO
    - SI.Z4.30-10.MI.HZ
    - SI.Z4.SO.A40.MI
  - Digital Padlock
    - SI.Z4.PL.08.60.MI.ML.WP
    - SI.Z4.PL.08.60.MI.SL.WP

  Note: The following SmartIntego features are not yet supported due to Mercury firmware limitations:
  - Door monitoring
  - Escape return function
  - Office mode
  - Whitelist function
  - Battery status
- Added functionality for ACM Verify users honoring partition

Changes

Fixed Issues

- Corrected issue with door search function being case sensitive and not triggering search when clicking "enter" key
- Corrected translation issue with delegation comparison reports in CSV format not being translated to languages that are not English
- Corrected issue with map not auto sizing to the browser display area and not being scrollable to view icons automatically placed at the bottom
- Corrected error resulting from adding a large number of interlocks resulting in pagination not working

Fixed Issues (continued)

- Corrected issue with inactivity timer auto logout affecting inactive tabs in spite of active adjacent tabs for the same system
- Corrected error resulting from entering a non-integer in the “Issue Level” field of the Tokens tab for an identity rather than issuing an alert for incorrect entry
- Corrected issue with incorrect door policy and transaction report in PDF format for a registered HID panel
- Corrected issue with incorrect card format not resulting in validation error message
- Corrected issue with priority data for a configured door not being displayed on the Monitor>Verification page
- Corrected issue with instructions entered in the Physical access> Events edit page appearing in the wrong column of the grid view of an event report
- Corrected issue with map icon for a configured NDE door not listing "Facility code only" for available door modes when the icon is clicked
- Corrected issue with subpanel batch add screen not honoring the subpanel limit when either 8 PIM400's or 8 Engage Gateways are selected to be connect to an MC-ICS Mercury panel
- Corrected error resulting from creating an ACC server on a replicated appliance while logged into another replicated appliance
- Corrected issue with misalignment of icons on the door status screen for 4 or more available device statuses associated to a door
- Corrected issue with a group of roles with just one identity being presented with a scheduler and batch add option
- Corrected issue with missing time stamp from the date field in the identity console of a local grant event
- Corrected issue with "Unlock", "Locked No Access", "Facility Code Only", "PIN Only", "Card and PIN", "Card or PIN" modes not displaying in the door mode selection list when creating a global action
- Corrected issues with "Clear custom layout" function in account settings not applying to the Monitor>Search page
- Corrected issue with the access tab of a door not honoring the deletion of an identity and displaying timed access data for the identity for both door and access group
- Corrected issue with UDF fields with type “string” displaying limited characters of the entire input string
- Corrected issues with few instances not being replicated from a primary appliance to a stand by appliance during an upgrade to ACM 5.10.0 or ACM 5.10.2
- Corrected issue with the door policy report for a virtual station showing incorrect filed names for certain attributes
- Corrected issue with missing "before" and "after" operators for the date field of an identity search criteria

Fixed Issues (continued)

- Corrected issue with Bosch panel incorrectly showing as online in spite of a wrong password being entered for a B9512G panel
- Corrected issue with events associated to "Appliances" not being translated for systems that are not English
- Corrected issue with ACM Verify delegations not being translated for systems that are not English
- Corrected error resulting from clicking help files for systems in Chinese, French, Portuguese or Russian
- Corrected issue with Mercury LED modes of the secondary appliance in a replicated system not being configured due to missing LED Buzzer delegations for a non admin role during a system upgrade to 5.10.0 or 5.10.2
- Corrected issue with the appliance not saving the remote authentication settings for an external system in the first attempt
- Corrected issue with incorrect pagination when accessing the last page for roles that have assigned identities with timed access schedules
- Corrected error resulting from switching to a Wiegand card formal from ABA mag format
- Corrected issue with the same MR51e Mercury subpanel allowed to be connected to two Mercury panels i.e. EP1501 and EP2500
- Corrected issue with the event search screen not able to sort rows inversely
- Corrected issue with Bosch panel (D9412GV4) showing connected, syncing only outputs and users but not areas and points within ACM
- Corrected issue with misaligned menu arrows on a chrome browser for an android device

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

CVE-2016-0747, CVE-2016-0746, CVE-2016-0742

ACM Known Issues

- Issue: Limit on databases listed under "Identity SQL server pull" collaborations
  Description: When performing a search on identities across several databases the "Database" pulldown field will only display results from a subset of the available databases for a large number of databases connected to an external server
  Affected Version: ACM 5.8.4
  Workaround: Avoid connecting more than 50 databases when performing a search across several databases
  Fix: Scheduled to be corrected in a service release

ACM Known Issues (continued)

- Issue: Incorrect panel count
  Description: The hardware active/inactive menu on the hardware status screen displays incorrect number of active panels
  Affected Version: ACM 5.10.0
  Workaround: None
  Fix: Scheduled to be corrected in a service release

- Issue: Missing partition objects
  Description: An operator configured to belong to two partitions could see objects belonging to only one of the two partitions that the operator belongs to and be allowed to select blank partitions on an object.
  Affected Version: ACM 5.10.2
  Workaround: None
  Fix: Scheduled to be corrected in a service release

- Issue: Hard area anti pass back issue with HID panels
  Description: Master doors on HID panels allow access to an identity/token into second area/office, even if the identity/token hasn't yet exited the first area/office
  Affected Version: ACM 5.10.0, ACM 5.10.2
  Workaround: Swipe the card twice within 30 seconds to activate access denied event
  Fix: Scheduled to be corrected in a service release

SmartIntego Known Issues

- Issue: SmartIntego WaveNet 8|8 bit format not working
  Description: When adding a Smart Intego Gateway Node in ACM with the assigned address based on the 8 bit | 8 bit WaveNet format, ACM does not connect to the GatewayNode.
  Affected Version: ACM 5.10.4
  Workaround: Use 11|5 or 12|4 WaveNet format
  Fix: Mercury firmware limitation, scheduled to be corrected in a service release

- Issue: Door standard access time over 60 sec resulting in incorrect strike time
  Description: Setting standard access time (door>operations) over 60 seconds results in an incorrect actual strike time
  Affected Version: ACM 5.10.4
  Workaround: Avoid setting standard access time above 60 seconds
  Fix: Mercury firmware limitation, scheduled to be corrected in a service release

SmartIntego Known Issues (continued)

- Issue: DHCP settings for SmartIntego Gateway Node not working
  Description: MAC and Hostname (i.e. DHCP settings) do not work when configuring SmartIntego Gateways as Simons Voss subpanels.
  Affected Version: ACM 5.10.4
  Workaround: Use static IP settings when setting up the SmartIntego Gateway node
  Fix: Mercury limitation, scheduled to be corrected in a service release

- Issue: SmartIntego door status show as offline
  Description: Door status for any SmartIntego door appear offline on the door screen
  Affected Version: ACM 5.10.4
  Workaround: Refer to event transaction screen to validate receiving events from Simon Voss doors to make sure door is online and communicating with panels
  Fix: Mercury limitation, scheduled to be corrected in a service release

- Issue: Battery alarm not being generated
  Description: Any alarm for low battery events from a SmartIntego lock are not be generated by Mercury panels
  Affected Version: ACM 5.10.4
  Workaround: None
  Fix: Mercury limitation, scheduled to be corrected in a service release

Firmware Included

Panel Firmware:

- rcp-update-1.8.0.0
- EP1501-VER-1-22-9.crc
- EP1501-VER-1-24-1.crc
- EP1502-VER-1-22-9.crc
- EP1502-VER-1-24-1.crc
- EP2500-VER-1-22-9.crc
- EP2500-VER-1-24-1.crc
- M5IC-VER-1-22-9.crc
- M5IC-VER-1-24-1.crc
- MSICS-VER-1-22-9.crc
- MSICS-VER-1-24-1.crc
- Scp2-AES-VER-3-120.crc
- Scp2-VER-3-120.crc
- ScpC-AES-VER-3-120.crc
- ScpC-VER-3-120.crc

Sub-Panel Firmware:

- ScpE-AES-VER-3-120.crc
- ScpE-VER-3-120.crc
- 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
- MI-RS4-APPL-VER-1-57-3.aax
- MR16IN-APPL-VER-1-32-1.aax
- MR16IN-APPL-VER-1-32-2.aax
- MR16OUT-APPL-VER-1-32-1.aax
- MR16OUT-APPL-VER-1-32-2.aax
- MR50-APPL-VER-1-52-14.aax
- MR50-APPL-VER-1-53-3.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-SERIES1-VER-1-11.aax
- MRDT-APPL-VER-1-63-0.aax
- MRDT-APPL-VER-1-63-4.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