Access Control Manager™ 5.10.2 Release Notes

Version 5.10.2– Released Wednesday, June 07, 2017

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.10.2-upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.10.2.ova
- ACM_VM_5.10.2.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.10.2 from revisions prior to ACM 5.6.0. The system must first be upgraded to ACM 5.6.0 and then to 5.10.2.
   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, 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 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

1. NOTE: Previous versions to 5.8.4.12_SR1 of AvigilonAcmIntegrations are not compatible with ACM 5.10.2. 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 5.10.2 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 5.10.2 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 5.10.2. The HID firmware is part of the ACM 5.10.2 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 5.10.2, 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 5.10.2 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.

New Features

Functional Features

- Introducing ACM Verify browser that provides the ability to use a mobile device as a virtual station
    - Added "Virtual Station Count" for number of licensed virtual doors under counts on the Appliance(Edit): About screen
      Note: Up to 50 concurrent ACM Verify sessions supported. Maximum number of licenses that can be added cannot exceed the total number of doors (Mercury and/or HID). New systems and upgraded systems receive one ACM Verify virtual station at no cost.
    - Added a new page called "Paired Devices" under Setup and Settings to enable pairing of ACM with a mobile device
    - Added "Avigilon" as vendor for adding a new virtual station on the Door: Add New screen
        - Added Managed and Unmanaged mode for the virtual station
        - Added "Into Area" dropdown list to define the area a virtual station belongs to
- Added support for Allegion Schlage LE locks
- Added support for Allegion Schlage AD300 locks
- Added support for domain controllers using TLS version 1.2

UI Features

- Created a new mobile aware interface for ACM Verify browser
    - Added a mobile page to pair a mobile device with ACM
    - Added a new menu to show all existing virtual stations and paired devices
    - Added a pin number field for users to enter their pin number
    - Added picture for dual authentication in managed mode
    - Added functionality to manually approve or reject an identity in managed mode
- Created mobile aware pages for Login and Door Listing screens

Changes

Fixed Issues

- Corrected issue with the event panel time column incorrectly displaying the appliance time
- Corrected issue with a global action incorrectly showing the contents of a previously created global action group rather than its own contents
- Corrected issue with deleting a command added to a newly created macro thereby deleting commands from other macros
- Corrected issue with transaction reports with large number of records from being created

Fixed Issues (continued)

- Corrected error resulting from checking-in users with HID Easy Lobby
- Corrected delay issue with logging into an appliance serving multiple sites
- Corrected issue with tokens unable to be reactivated within the “use or loose” threshold
- Corrected issue with embossed number not being displayed on the monitor verification screen
- Corrected translation issue with the popup that appears when browsing to the appliance backup file location for an interface with language that is not English
- Corrected issue with available roles not being updated when editing a group
- Corrected display issue with server status (under external systems>Avigilon) not translated for an interface with language that is not English
- Correct issue with monitor search displaying incorrect data when the page layout is changed by moving columns
- Corrected issue with a Bosch intrusion panel that is connected to two appliances, displaying incorrect status for one of the appliances, when the panel is physically disconnected and reconnected back to both the appliances
- Corrected issue with date field of report edit screen, for any report that contains the date edit box, not being wide enough to display the date and time
- Corrected issue with the identity profile page displaying page links that do not honor the items per page limit rather the available number of identity profiles
- Corrected display issue with the event "date changed by user" not being translated for a Chinese interface
- Correct display issue with event search screen not scaling according to the browser
- Corrected display issue with width of door forced or held buttons (under Monitor>HW Status) not adjusting according to the characters for German and Russian languages
- Corrected display issue with width of Master and Perimeter buttons (under Monitor>Intrusion Status>Areas) not adjusting according to the characters for German and Russian languages
- Corrected connection issue with IE11 browser following a Windows update
- Corrected display issue with ACC server and cameras status not being translated for an interface with language that is not English
- Corrected issue with password required to be entered again when editing the backup location for an appliance
- Corrected issue with incorrect assignment of access groups and groups when special characters are used as names for roles, groups and access groups
- Corrected issue with “use or loose” threshold unable to be disabled by deleting the value in its field under system settings
- Corrected issue with the badge template dropdown not listing the templates alphabetically
- Corrected issue with door being deleted in spite of its interlock being associate to a trigger and a macro

Fixed Issues (continued)

- Corrected issue with Bosch intrusion users with authority level 0 in RPS not appearing in ACM
- Corrected issue with the doors not sorting in an ascending order when a door's state is changed
- Corrected issue with misalignment of the door listing page resulting from adjusting “Unlocked (Classroom/Store room)” door mode
- Corrected issue with outdated advanced filter help
- Corrected issue with export collaboration not translated for an interface with language that is not English
- Corrected issue with panel being deleted in spite of a door assigned to it
- Corrected issue with data picker not being displayed when cursor is placed on a date field
- Corrected issue with map icons not moving unless the page is refreshed
- Corrected issue with “comm” status of an offline door not being updated on a map
- Corrected issue with door interaction filter confirm button not being displayed properly on a mobile device, when the system interface language is set to Chinese
- Corrected issue with monitor events not being sorted by icons
- Corrected display issue with the event "low battery and RC loss/ lock offline" not being translated for an interface with language that is not English
- Corrected delay issues with “comm” status on the Hardware status screen and door screen taking long to be updated when door action is triggered
- Corrected issue with a PIM400/Engage Gateway selected as a subpanel, allowing overlapping door count values for additional gateways/modules on the same RS-485 bus
- Corrected error resulting from navigating to a backup location for an appliance with backup type "Windows Share Mount"
- Corrected issue with appropriate events for door type (Aperio, PIM, NDE) not being listed on the doors events screen
- Corrected issue with advanced filters for door mode "unlocked" not filtering doors unless both alarms and door mode have "unlocked" selected
- Corrected issue with tokens not honoring the “use it or lose it” it timestamp until the next check is performed or the token has been modified
- Corrected issue with incorrect data for alarm status in an event type report when event alarm status is toggled between enabled and disabled

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

- Common vulnerabilities addressed by upgrading SSL libraries
- Upgrades to Network Time and LDAP directory services to resolve common vulnerabilities

Known Issues

- Issue: Message for HID firmware upgrade
  Description: During an HID firmware upgrade the message indicating a successful panel upgrade may get buried in between several error messages that are not critical and can be ignored
  Affected Version: ACM 5.6.4
  Workaround: Look carefully through the log for upgrade message
  Fix: Scheduled to be corrected in a service release

- Issue: AD300 and Gateways on same port resulting in AD300 going online/offline
  Description: When an AD300 subpanel and an ENGAGE Gateway are connected on the same panel, it may result in an unstable AD300 lock connection
  Affected Version: ACM 5.10.2
  Workaround: Avoid having an AD300 on the same port as an ENGAGE Gateway
  Fix: Mercury firmware (1.23.6 and 1.24.1) limitation, scheduled to be corrected in a service release

- Issue: Bosch panel status still remains online after user inputs the wrong password
  Description: When a user enters a wrong password for an intrusion panel that is online, the panel may not go offline and allow full command and control for that panel to be executed
  Affected Version: ACM 5.10.2
  Workaround: Uninstall and re-install the panel to break the connection and create a new instance with a new login
  Fix: Bosch firmware (v3.03) 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

Panel Firmware (continued):

- 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
- 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