Access Control Manager™ 5.12.0 SR2 Release Notes

Version 5.12.0 SR2 – Released Friday, September 28, 2018

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.12.0_SR2-upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.12.0_SR2.ova
- ACM_VM_5.12.0_SR2.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.12.0 SR2 from revisions prior to ACM 5.10.2. The system must first be upgraded to ACM 5.10.2 and then to 5.12.0 SR2.
   The upgrade package for ACM 5.10.2 is available at ftp://ftp.avigilon.com/ACM/5.10.2/
   The release notes for ACM 5.10.2 are available at ftp://ftp.avigilon.com/ACM/5.10.2/ACM 5 10 2 Customer Release Notes.pdf

2. 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 are available at ftp://ftp.avigilon.com/ACM/5.6.0/ACM5.6.0 Release Notes v2.pdf

3. 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 are available at ftp://ftp.avigilon.com/ACM/5.2.0/ACM 5.2.0 Release Notes.pdf

ACM Upgrade Instructions

Any login with the following rights assigned its delegation can administer and apply software upgrades for a physical or virtual appliance:

- Appliances Listing
- Appliances Edit
- Appliance Software Listing
- Appliance Software Apply
- Appliance Software New (for adding upgrades)
- Appliance Software Delete (for deleting upgrades)

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 since ACM 5.6.4. 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 5.12.0 SR2. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.
- Instructions for installing 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 5.12.0 SR2 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 5.12.0 SR2 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.
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 5.12.0 SR2. The HID firmware is part of the ACM 5.12.0 SR2 upgrade package and will allow you to update the HID VertX EVO field hardware with HID firmware version 3.6.3.101.

- After upgrading the ACM to version 5.12.0 SR2, upgrade HID VertX EVO V1000 with RCP 1.8.2.0. The HID firmware version 3.6.3.101 will be automatically updated as a part of the RCP 1.8.2.0.
- Repeat the upgrade for HID VertX EVO V2000 with RCP 1.8.2.0 and HID firmware version 3.6.3.101 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

- As of ACM 5.8.4, a new Application Passcode must be configured in addition to the Automation Passcode (formerly labelled “Password”) 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".

ACM with Bosch Intrusion Upgrade (cont'd)

- 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

- Enhanced Badge Designer features:
  - Updated default background color to white.
  - Added borders around badge, DB, Text and Graphic fields to aid field alignment.
  - Added option to add frame around the photo and frame color selection.
  - Added word wrapping on Text and DB fields.
  - Added default settings for Badge Photo Height and Width.
  - Updated button styles for Save, Cancel Changes and Delete.
- Enhanced image editing functionalities for Identity Photos:
  - Removed the Capture Tab.
  - Added Upload a Photo and Capture a Photo on the identity photo tab.
  - Added photo editing functionality for Upload Photo from File and Capture Photo.
    - Added Photo Editing Tools available with tooltips to describe functionality.
    - Added support for Crop Box Height and Width
    - Added functionality for zoom, move, rotate, flip, and reset.
    - Added 16:9, 4:3, 1:1, 2:3, and free aspect ratios.
- Added functionality to filter Roles by search criteria.
- Added functionality to create new Templates for easy of configuration:
  - Added Templates option under the Physical Access tab.
  - Added Door templates with door parameters and door operations.
- Added functionality to create new doors from a Door Template.
- Added functionality to bulk update door parameters and door operations with a Door Template.
- Added functionality to bulk delete doors from the Doors page.
- Added functionality to save the Operators' door selections when saving custom Verification configurations.
- Added functionality to select the Verification page as the home page for Operators.
- Added support for Arabic.
- Added support for Partition license enforcement.
- Added an Add Doors button at the top of the Doors tab under Physical Access.

New Features (cont'd)

- Added option for Priority Door State:
  - Added checkbox to designate Door Policy or Global Action as a Priority Door State
  - Added "Policies Set Priority" right to provide access to the "Priority Checkbox" on a Door Policy.
  - Added "Global Action Set Priority" right to provide access to the "Priority Checkbox" on a Door Mode Global Action.
  - Added "Doors Commands During Priority" right to enable manual door commands to be sent by an operator from ACM during a Priority Action.
  - Enhanced door listing screen and maps to identify doors that are part of an active Priority Door State.
- Added a Clear Pin button to the Identity Token tab.
- Added functionality to highlight doors where a manual command or a specific lock function (for wireless doors) prevents the custom schedule from changing the door mode.

Performance Features

- Reduced time required to generate reports
- Reduced time required to create large groups

Changes

Fixed Issues

- Corrected an issue where the Replication without Failover stopped working after upgrading to ACM 5.12.0 or 5.12.0 SR1.
- Corrected an issue with the Rest API call to search Identities not returning correct results.
- Corrected an issue where the Badge Designer was not compatible with IE11.
- Corrected an issue where wireless lock function was displayed incorrectly in ACM when the Mercury panel was offline.
- Corrected an issue with Timed Area Antipassback permitting access to a reader within the specified Antipassback delay period.
- Corrected and issue with Into Area Occupancy count decreasing when an identity enters the area.
- Corrected an issue with increased badge font size in badge templates after upgrading to ACM 5.12.0. See Known Issues regarding badge templates created in ACM 5.12.0.
- Corrected an issue with Input and Output status icons on Maps not displaying their current status in ACM 5.12.0.
- Corrected an issue where Hardware Status Monitor page labelled Active Alarms as "Active".
- Corrected an issue where events were not sorted chronologically when event dates were displayed in dd/mm/yyyy format.

Fixed Issues (cont'd)

- Corrected an issue where two profile batch updates for two different groups scheduled consecutively apply both updates to the first group.
- Corrected an issue where the Collaboration log displayed incorrectly with Cyrillic letters.
- Corrected an issue where an Operator Account with a password containing special characters was unable to delete objects.
- Corrected an issue where search failed to return sources, door names, or identities containing special characters.
- Corrected an issue where reports were not generated when scheduled by a remote user.
- Corrected an issue where erroneous "Secure Channel not enabled" events were generated for NDE Wireless Locks.
- Corrected an issue where text only fields were rendered underneath a background image on Maps.
- Corrected an issue with CSV imports where user defined text box fields were not imported.
- Corrected an issue with improper pagination of the door transactions tab and the EOL Resistance page.
- Corrected an issue where the identity audit report could not be generated from Identity Audit Tab.
- Corrected an issue where the User was erroneously logged out after a failed attempt to change the password.
- Corrected an issue with the Door tab allowing invalid inputs for Door Operations fields.
- Corrected an issue with the Appliance Page allowing invalid values for Port address fields.
- Corrected an issue with Global Actions gateway field allowing invalid values.
- Corrected an issue with the identity button on Event Monitoring or Event search failing to return information.
- Corrected an issue where Bosch panels did not operate during a failover
- Corrected an issue where the user was erroneously logged out when saving changes made in My Account if the old password field was filled in.
- Corrected an issue where "Incomplete card and PIN Sequence" event displayed erroneously for HID doors in a global linkage.
- Corrected an issue where batch identity profile update failed when updating more than 10 records for profiles that had a partition selected.
- Corrected an issue where Appliance Backup failed if the backup name contained special characters.
- Corrected an issue where multiple OSDP reader addresses conflicted by default.
- Corrected an issue where Operator could not schedule jobs if the Operator login contained parentheses.
- Corrected an issue where the reader LED Drive options were incorrectly displayed for each Reader Type.
-

Fixed Issues (cont'd)

- Corrected an issue where the CSV Identity Summary Report was missing the headers if an identity had multiple tokens.
- Corrected an issue where a mobile device could not be paired to ACM if the appliance time zone was outside North America.
- Corrected an issue where a wireless door continued to display the lock function after the lock function was disengaged.
- Corrected an issue where non-graphic files could be uploaded to the Badge Designer.
- Corrected an issue where groups were not editable if the name of an identity in the group contained special characters.

ACM Known Issues

- 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 future release

- Issue: Invalid card schedule error in ACM Verify
  Description: When using ACM Verify to access virtual doors with an access group set to use a custom schedule, an invalid card schedule error occurs even though the custom schedule is valid.
  Affected Version: 5.10.6
  Workaround: Set the access group to use the default 24 hours active schedule.
  Fix: Scheduled to be corrected in a future 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 Cyrillic font for door, panels, inputs or output names
  Fix: Scheduled to be corrected in a future release

- Issue: Windows Share Backup fails if password contains $
  Description: When using Windows Share Backup, the backup process fails when the user password contains $
  Affected Version: ACM 5.10.8
  Workaround: Do not use $ in user password
  Fix: Scheduled to be corrected in a future release

ACM Known Issues (cont'd)

- Issue: AD-400 privacy button does not function
  Description: The privacy button on AD-400 wireless locks does not lock the door when the lock is connected to a Mercury panel.
  Affected Version: 5.10.10 SR1
  Workaround: Downgrade Mercury panel firmware to version 1.21.2, which can be found at: ftp://ftp.avigilon.com/ACM/PanelFirmware/Mercury
  Fix: Scheduled to be corrected in a future Mercury firmware release

- Issue: Transaction report search does not return results when searching with full name
  Description: Search criteria with full name (any combination of first name and last name) will not return valid results in the Transaction report
  Affected Version: ACM 5.10.10 SR1
  Workaround: Combine two search criteria: first name and last name when searching for the full name in Transaction Report. I.e. when searching for John Smith, use:
    - First Name contains: John
    - Last Name contains: Smith
  Fix: Scheduled to be corrected in a future release

- Issue: Status Icons not displayed for objects on Map if some objects are missing
  Description: If some objects on a map are deleted, other maps may not display status icons for valid objects
  Affected Version: 5.10.10 SR1
  Workaround: Save the map with missing objects to remove missing objects
  Fix: Scheduled to be corrected in a future release

- Issue: Destroy Batch button unavailable after identity deletion and search
  Description: The batch destroy button is not available after deleting identities and then running an advanced search on the same identity search tab
  Affected Version: 5.12.0
  Workaround: Clear search and re-run advanced search with the same criteria
  Fix: Scheduled to be corrected in a future release

- Issue: Badge templates upgraded from ACM 5.12.0 may need updates
  Description: The font size for text fields on badge templates created in ACM 5.12.0 may be different after upgrade to 5.12.0 SR1
  Affected Version: 5.12.0
  Workaround: Manually adjust the text size or use auto resize for text fields
  Fix: This issue only affects badge templates created in ACM 5.12.0 and will not be corrected in a future 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

Sub-Panel Firmware (cont'd):

- 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