

Access Control Manager™ 5.8.4 Release Notes

Version 5.8.4 – Released Wednesday, February 22, 2017

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.8.4-upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.8.4-disk1.vmdk
- ACM_VM_5.8.4.mf
- ACM_VM_5.8.4.ovf
- ACM_VM_5.8.4.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.8.4 from revisions prior to ACM 5.6.0. The system must first be upgraded to ACM 5.6.0 and then to 5.8.4.
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, 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 of AvigilonAcmIntegrations are not compatible with ACM 5.8.4. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.
2. Instructions for installing the AvigilonAcmIntegration-5.8.4.12.
 - a. Download AvigilonAcmIntegration-5.8.4.12_SR1 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-5.8.4.12_SR1.
 - f. Ensure Vidproxy service is running.
 - g. Login to the upgraded 5.8.4 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 5.8.4 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 5.8.4. The HID firmware is part of the ACM 5.8.4 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 5.8.4, 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 5.8.4 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 can now be changed from ACM. If it is changed from RPS, ACM will override it to the default passcode.

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

- Added support for MS Bridge: MS-ICS, MS-ACS, MS-I8S and MS-R8S
- Added support for B6512 Bosch Intrusion Panel
- Added certification for VMware™ vSphere ESX 6.x and VMware™ vSphere ESXi 6.x
- Added threshold to number of incorrect login attempts
- Added support for 40 Bosch intrusion panels per ACM appliance
- Added support for NDE wireless gateway and locks

Performance Features

- Improved stability bringing large numbers of panels online simultaneously
- Reduced load time when loading the door listing screen, panel listing screen and group listing screen
- Reduced search time for advanced search criteria to 2 seconds

Changes

Fixed Issues

- Corrected issue when using a special character in a door name causing the selected door to appear in both the available and member door list
- Corrected error resulting from using a special character in the value field of the user list
- Improved fail over response time when an appliance becomes inactive
- Corrected issue with expired batch jobs automatically being renewed to run in the following years
- Corrected translation issues with certain words for interface in Russian language
- Corrected issue with blank token date fields displaying an invalid date value on the monitor events screen
- Corrected issue with non-English collaborations displaying incorrect data
- Corrected issue with the Area Identity report not displaying the Last Accessed time in the grid view
- Corrected issue with custom audit reports not honoring schedules and resulting in an error
- Corrected issue with large scheduled Transaction Report (PDF) returning no results by enforcing a limit of 50,000 records
- Corrected issue with large scheduled Audit Log Report (PDF) returning no results by enforcing a limit of 13,000 records
- Corrected issue with large scheduled Identity Summary Report (PDF) returning no results by enforcing a limit of 100,000 records

Fixed Issues (continued)

- Corrected issue with Door Delegations assigned to roles not preventing those roles from executing the unauthorized door actions
- Corrected wrapping issue of door icons on oversized maps
- Corrected erroneous decrement of assimilation remaining (under appliance/about tab) by one for an HID V1000 and V2000 panel after a firmware upgrade
- Corrected issue with inconsistent status and data display when a Bosch panel and ACC Server coexist in a replicated environment
- Corrected error message when a profile status field was left blank
- Corrected Bosch panel configuration issue resulting from ACM not being able to interpret international characters used in RPS input fields
- Corrected formatting issue of identity first, last and middle name after importing through a collaboration
- Corrected issue with any time zone which is one day ahead of UTC resulting in an inaccurate deactivate date for an identity with multiple tokens
- Corrected scrolling issue with the notes window for the monitor events and maps screen
- Corrected validation error on the physical action event page due to blank or invalid value for the alarms color field
- Corrected issue with transaction report and audit log report not displaying the accurate number of events in the grid view
- Corrected issue with having to re-enter your password when editing the file source/destination of an existing collaboration
- Corrected issue with export collaborations failing when two collaborations are in progress simultaneously
- Corrected printing issue with the first page of a help file being blank
- Corrected error resulting from multi role assignment in a SQL collaboration
- Corrected error on the doors page of physical access when adding a door without providing vendor and door information
- Corrected issue with a policy simultaneously showing up in both the available field and members field of a group
- Corrected issue with missing links for groups in help
- Corrected issue with token issue, activate and deactivate dates being reset to current date when attempting to download the token
- Corrected issue with delays in panel and door configuration updates when collaborations are running

This release addresses the following Common Vulnerabilities and Exposures:

- Fix for CVE-2016-6210, CVE-2016-6515, VulnDB 142343, VulnDB 142344

Known Issues

- Issue: Badge Image may fail print job if template's user defined field data contains dots
Description: If the badge template contains a user defined field with dots in its name the badge image isn't generated.
Affected Version: ACM 5.8.0
Workaround: Avoid using dots in user defined fields of badge designer
Fix: Scheduled to be corrected in a service release
- Issue: The orientation of an identity's photo may be incorrectly displayed when captured with a mobile device (both iOS and Android).
Description: Pictures taken on mobile devices are always recorded in the camera's native orientation (home button on the right) with additional EXIF data indicating how the camera was oriented at the time. ACM (and Windows) does not recognize EXIF data so pictures taken on mobile devices will always be displayed in the native orientation which may be sideways or upside down relative to the subject.
Affected Version: ACM 5.8.2
Workaround: Hold the mobile device in landscape mode with the home button to the right to take identity photos.
Fix: Scheduled to be corrected in a service release
- Issue: Monitor Events page may show inaccurate panel time
Description: The panel time and date of an event may inaccurately show the appliance's time
Affected Version: ACM 5.8.2
Workaround: Refer to transactions tab under Identity for correct panel time
Fix: Scheduled to be corrected in a service release
- Issue: Invalid accented characters in host name give an error
Description: International characters in the host name of an appliance may result in an error
Affected Version: ACM 5.8.0
Workaround: Avoid using accented characters in the host name of an appliance
Fix: Scheduled to be corrected in a service release
- Issue: Slow Transaction report when filtering by Embossed number field
Description: There may be delays when running a transaction reports using an embossed number filter for a very large database
Affected Version: ACM 5.6.4
Workaround: Avoid using embossed number as a filter for transaction reports
Fix: Scheduled to be corrected in a service release

Known Issues (continued)

- Issue: Incorrect identity search for Boolean fields
Description: The number of records found when performing an identity search using Boolean fields may not add up to the total number of identities
Affected Version: ACM 5.8.4
Workaround: No workaround
Fix: Scheduled to be corrected in a service release

Firmware Included

Panel Firmware:

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

Sub-Panel Firmware:

- MS-I8S-APPL-VER-1-0-1.aax
- MR51e-APPL-VER-1-5-12.aax
- M5-8RP-APPL-VER-1-57-5.aax
- MS-ACS-APPL-VER-1-0-5.aax
- M5-20IN-APPL-VER-1-32-2.aax
- M5-2RP-APPL-VER-1-57-3.aax
- MR52-SERIES1-VER-1-11.aax
- M5-2K-APPL-VER-1-56-13.aax
- MR16in-APPL-VER-1-31-1.aax
- MRDT_APPL-VER-1-63-0.aax
- M5-8RP-APPL-VER-1-57-3.aax
- MR51e-APPL-VER-1-4-8.aax
- M5-2K-APPL-VER-1-56-15.aax
- MR16out-APPL-VER-1-31-1.aax
- MS-R8S_APPL-VER-1-0-1.aax
- M5-2SRP-APPL-VER-1-57-2.aax
- MR50-APPL-VER-1-51-0.aax

Sub-Panel Firmware (continued):

- MR52-APPL-VER-1-51-0.aax
- MR52-APPL-VER-1-57-5.aax
- MR16in-APPL-VER-1-32-1.aax
- MR50-APPL-VER-1-52-14.aax
- M5-16DO-APPL-VER-1-32-2.aax
- M5-2SRP-APPL-VER-1-57-3.aax
- M5-2RP-APPL-VER-1-57-2.aax
- MR16out-APPL-VER-1-32-1.aax