Access Control Manager™ 5.10.8 Release Notes

Version 5.10.8– Released Wednesday, November 29, 2017

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.10.8-upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.10.8.ova
- ACM_VM_5.10.8.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.10.8 from revisions prior to ACM 5.6.0. The system must first be upgraded to ACM 5.6.0 and then to 5.10.8.
   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.

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

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 5.10.8. 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 5.10.8 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 5.10.8 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.

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

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 5.10.8. The HID firmware is part of the ACM 5.10.8 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 5.10.8, 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 5.10.8 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.

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

New Features

Functional Features

- Increased number of schedules from 255 per appliance to 255 per panel
- Optimized REST API call for importing identities to include all roles, user IDs in a role and user information from user IDs
- Added functionality to import ACM username from Active Directory
- Added functionality allowing collaborations to configure an identity to use remote authentication
- Added functionality to include domain name to username for Active Directory

Performance Features

- Increased the number of grants per door per minute
- Reduced identity CSV collaboration run time
- Reduced navigation load time

Security Enhancements

- TLS minimum requirement upgraded to 1.1
- Added support for user provided certificates and credentials for external systems
- Added support for certificate validation checks
    - Certificate pinning supported when certs do not have a valid trust chain

Changes

Fixed Issues

- Corrected issue with system upgrade from 5.6.4 to 5.10 taking several hours
- Corrected issue with ambiguous error message on the validation screen during a remote session
- Corrected ACC-ACM integration issue with doors named using Cyrillic letters in ACM not being displayed correctly in ACC when attempting to link them to a camera
- Corrected issue with Identity/Doors Access report or Door/Identities Access report not producing results for an operator logged in remotely
- Corrected issued with system settings not honoring changes to profile language
- Corrected issue with Destroy Batch delegation not deleting identities when "Destroy Batch" is clicked
- Corrected issue with map not being editable and icons being dispersed when user attempts to change the format of the color field
- Corrected reply timeout for Mercury panels from 1 second to 3 seconds

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

Fixed Issues (continued)

- Corrected issue with delegations not being displayed alphabetically and inconsistent controller names in each delegation
- Corrected issue with audit logs not being created for doors configured with antipassback
- Corrected issue with warning message to set locale showing up in upgrade.txt log during an upgrade from ACM 5.10.4 or earlier
- Removed extraneous 'Record updated by system' event when use/lose is enabled
- Corrected issue with ViRDI systems not being created if more than one external systems already exist
- Corrected issue with ACM help files referring ACC as Avigilon 5.10.4 Server
- Corrected memory issue resulting in system becoming unresponsive due to large number of connected panels
- Correct issue with ACM 5.10.6 where existing LDAP collaborations failed to update some identities with remote domain not set
- Corrected issue with ACM 5.10.6 where a full schedules download would fail to download all schedules, due to an indexing issue with the schedule download

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

CVE-2016-2183 and CVE-2016-6329

ACM Known Issues

- Issue: Virtual station numeric keypad switched to standard device keyboard.
  Description: A virtual station on a Firefox browser changes from numeric keypad to standard device keyboard after first digit of PIN is entered on an Android mobile device. The cursor also jumps behind the first digit, resulting in an incorrect PIN
  Affected Version: ACM 5.10.2
  Workaround: Avoid using Firefox browser when using a Virtual Station on an Android device.
  Fix: Scheduled to be corrected in a service release

- Issue: Token reports are not filtering properly on the deactivate date.
  Description: Results from Tokens Pending Expiration Report do not correspond to the proper time frame selected in the filter and doesn't match with the results obtained on the identity search
  Affected Version: ACM 5.10.4
  Workaround: Avoid using local appliance time and translate the time period into UTC.
  Fix: Scheduled to be corrected in a service release

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

ACM Known Issues (continued)

- Issue: Incorrect badge preview.
  Description: When loading the badge tab for an identity, if there is no template information saved for the identity the first badge template image will show and it may not match with the name of the badge template displayed in the Badge Template drop down box
  Affected Version: ACM 5.10.4
  Workaround: Save the template for the identity
  Fix: Scheduled to be corrected in a service release
- Issue: Token database grows to large size causes failure of download
  Description: For large number of transactions producing grants that change last area of an identity token record can trigger a token download to all Mercury panels causing the queue to get stuck
  Affected Version: ACM 5.10.4
  Workaround: Contact technical support to resolve issue
  Fix: Scheduled to be corrected in a service release
- Issue: Scheduled transaction report fails to run
  Description: Scheduled transaction report fails to run when UK English is selected in “my account” settings
  Affected Version: ACM 5.10.8
  Workaround: Change settings to US English
  Fix: Scheduled to be corrected in a service release
- Issue: Operator is prevented from adding new identities
  Description: Issue that prevents an operator with Identities View Only, Identities View/Edit and Enrollment Operator delegation is prevented from adding new identities
  Affected Version: ACM 5.10.8
  Workaround: Only use Enrollment Operator as delegation
  Fix: Scheduled to be corrected in a service release
- Issue: Some holidays are not downloaded to controller
  Description: Issue that prevents all holidays from being downloaded to controllers
  Affected Version: ACM 5.10.6, with more than 47 holidays, on controllers that have been reset/downloaded
  Workaround: Edit any holiday making a change and save
  Fix: Scheduled to be corrected in a service release

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

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
- 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

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.

Sub-Panel Firmware (continued):

- 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

© 2017, Avigilon Corporation. All rights reserved. No license is granted with respect to any
copyright, industrial design, trademark, patent or other IP rights of Avigilon or its licensors.