Access Control Manager™ 6.24.0.7 Release Notes

Version 6.24.0.7 – Released Monday, September 27, 2021

Files Released

Avigilon Access Control Manager Physical Appliance Files

- ACM-6.24.0.7-20210923-121113.upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_6.24.0.7.zip
- appliance_acm-5.2.0.7-acm_6.24.0.7-20210923.143840-genericx86-64_vm_hyper-v.zip

Upgrade Path

NOTE: ACM 6.24.0.7 is not compatible with previous versions to 6.14.20.2 of ACC/ACM Integration. Avigilon recommends upgrading existing ACC/ACM integrations to current versions of ACM and ACC.
NOTE: ACM 6.24.0.7 is not compatible with previous versions to 1.2.0.0 of Milestone VidProxy Services.

1. Always perform a configuration and transaction backup of the current version prior to any upgrade and save to a secure location.
2. There is no direct upgrade path to ACM 6.24.0.7 from ACM 6.0.0. The system must first be upgraded to ACM 6.2.0 then to 6.24.0.7.
3. There is no direct upgrade path to ACM 6.2.0 from ACM 5.12.2. The ACM 5.12.2 system must first be upgraded to ACM 6.0.0 then to 6.2.0.
4. 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.
5. 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.
6. 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.
7. Please refer to the upgrade release notes for further information.
8. Download upgrade file from https://www.avigilon.com/software-downloads/

ACM Upgrade Instructions

Perform a full backup (configuration and transactions) of the current version prior to applying this upgrade

- Manual door modes set thru the UI or via global actions will be reverted to scheduled door modes following the upgrade
- Replication must be disabled on all appliances prior to upgrade (Previous ACM upgrades required replication to be active to complete properly, this is not the case for ACM 6.24.0.7)
- Upgrades are supported on ACM Professional (Dell OptiPlex XE2, XE3) ACM Enterprise (Dell PowerEdge R210, R220, R230 and R240) and Enterprise PLUS (Dell PowerEdge R330 and R340)
- The appliance will be offline from clients and controllers for the duration of the process
- Avoid running reports on the appliance for a few hours after the upgrade. The upgrade process will continue in the background performing a postgres reindex once the appliance is back online with clients and controllers
- ACM Virtual, please take a snapshot and check the system to ensure storage is not over allocated before proceeding with the upgrade and have a minimum of 500GB disk free space
- ACM Virtual instances should have VMNic1 and VMNic2 connected in the host prior to performing ACM 6.24.0.7 upgrade
- Identity account may require inactivity timer set to indefinite for extended upgrade times to observe status without requiring to log in and observe logs under appliance
- The upgrade instructions can be found in Access Control Manager (ACM) help menu
    - After logging in to Access Control Manager, click on “Appliance” under Setup and Settings
    - Go to the “Software Update tab” and select Help near the top right of the browser window
    - Search for the link labelled “updating appliance software” for ACM upgrade instructions
    - Follow the instructions to apply the ACM 6.24.0.7 upgrade
    - Wait for the system to reboot
    - After upgrade is complete, login to open ACM 6.24.0.7
    - If the default password has never been changed, there will be a one-time prompt to change your default password.

ACM Virtual Appliance

VMware

- Importing ACM Virtual Appliance ACM_VM_6.24.0.7.ova requires a minimum of vSphere version 6.5

Hyper-V

- Importing ACM Virtual Appliance appliance_acm-5.2-acm_6.24.0.7-20210904.060006-3-genericx86-64_vm_hyper-v.zip requires a minimum of Windows Hyper-V Generation2

ACM with replication Upgrade Instructions for Peer-to-Peer (2 or more appliances without Hot Standby)

1. For the ACM 6.24.0.7 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
2. For the ACM 6.24.0.7 upgrade on a peer-to-peer replicated system, disable the replication on all appliances.
3. Apply the software upgrade to all appliance in any order
4. Allow the upgrade on all appliances to complete and the appliances to reboot and come back online.
5. Accept the EULA for all appliances.
6. Re-enable replication on all appliances.

ACM with replication Upgrade Instructions for Hot Standby Auto Failover

1. Perform a configuration and transactions backup of ACM 6.24.0.7 and save to secure location.
2. For the ACM 6.24.0.7 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.24.0.7 upgrade on a hot standby replicated system, manually failover to let the secondary appliance take over the session.
4. Disable replication on both appliances.
5. Apply the upgrade to the primary appliance and accept the EULA once it completes.
6. On the secondary appliance replication page, click “Fail back” and make sure the primary appliance takes over the session.
7. Upgrade the secondary appliance and accept the EULA once it completes.
8. Re-enable replication on both appliances.

ACM with replication Upgrade Instructions for 4 mixed peer to peer and Hot Standby

1. Perform a configuration and transactions backup of ACM 6.24.0.7 and save to secure location.
2. Appliance 1 and 2 are peer to peer; appliances 3 and 4 are failover appliances monitoring 1 and 2 respectively.
3. On appliance 3 and 4, navigate to appliance replication page, click on take over button on appliance 3, 4. Make sure that appliance 3, 4 take over the control from appliance 1, 2 successfully. Observe that panels are online on appliance 3
4. Navigate to the appliance replication tab on each appliance. Uncheck enable replication and save the configuration on each appliance
5. Upload upgrade file to appliance 1 and 2. Apply the upgrade files on 1 and 2
6. Wait till upgrade finishes successfully on appliance 1 and 2. Accept the EULA.
7. Navigate to appliance 3 and 4's appliance replication tab, click on the fail back button on appliance 3,4. Make sure appliance 1, 2 take the control back successfully (First try might not succeed, try multiple times). Observe that panels are online on appliance 1
8. Upload upgrade file to appliance 3 and 4. Apply the upgrade files on 3, 4
9. Wait till upgrade finishes successfully on appliance 3 and 4. Accept the EULA.
10. Navigate to appliance replication page on each appliance, check enable replication and save the configuration on each appliance

    NOTE: If you have a scenario where one Hot Standby is monitoring multiple appliances, you should upgrade each monitored appliance one at a time by using the Hot Standby in turns and update the Hot Standby last.

Changes

New Features

- ACM maximum supported controllers increased to 1,000.
- Added Batch Update support for SALTO doors.
- The "Access Port" and "Callback Port" are now displayed in the Panel report for ASSA ABLOY panels (DSR).
- Added a checkbox to set the visibility (hide/show) of a global action in ACM Expedite.
- ACM Expedite:
    - UX and UI improvements
    - Localized content
    - Connection error handling

Fixed Issues

- Corrected issue where messages were sent to all Schlage GWE when a credential was edited in ACM resulting in performance degradation.
- Corrected issue where credentials get deleted from Schlage wireless locks (NDE, LE, Control) in Wi-Fi mode after the lock is synched with ACM.
- Corrected issue where Mercury LED modes on color and off color displayed (not found) and could not be configured.
- The disk space usage threshold has been updated to remove the "false-positive" low disk warning on the dashboard.
- Corrected issue where the Audit tab of an Access Group showed no record.
- Corrected issue where the Access port and Callback port couldn't be set at creation time of an ASSA ABLOY (DSR) panel with a REST command.
- Corrected issue where the panel name was missing in the Door Configuration Report for ASSA ABLOY IP-Enabled doors.
- Corrected issue where no event was generated for an ASSA ABLOY IP-Enabled lock when the battery was critically low.
- Corrected issue where token numbers were displayed in decimal format in the door transactions report (trace) on Maps.
- Corrected issue where a global action could be triggered by unintentionally swiping an item in ACM Expedite.
- Corrected issue enforcing users to change their password on remote authentication.
- Corrected issue where an ASSA ABLOY IP-enabled door was displayed as overridden (blue box around the item) in the door list page after the override ended.
- Corrected issue where doors were reported "online" when the panel they are connected to was offline.
- Corrected issue where the "Door Forced Filter" and "Two Card Control" fields show incorrect selection state.

ACM Known Issues

- Issue: ACM-ACC Unification - ACM-ACC communication failures

  Description: ACM may intermittently become unresponsive and give an error message due to the size and specific setup of a large ACC-ACM integration. The connected ACC server could show connection errors to ACM frequently if the simultaneous operators limits are exceeded.

  Affected Version: ACM 5.12.2.31 forward

  Workaround: Avoid connecting more than 20 simultaneous operators for an Enterprise appliance and more than 50 for an Enterprise Plus appliance.

Fix: Scheduled to be corrected in a future release.

- Issue: ASSA ABLOY IP-Enabled Wi-Fi and POE doors do not display forced open or Held Open status in the door listing page or on the doors placed on maps. ACM does not record or display forced open or held open return events from ASSA ABLOY IP-Enabled Wi-Fi and POE doors.

  Description: When ASSA ABLOY IP-Enabled Wi-Fi and POE doors generate a forced open or help open event, ACM logs/displays the event in the event monitor and alarms may be configured however the status of the doors remains unchanged in a secure state on the door list page and on maps.

  Affected Version: ACM 6.18.0.53 forward

  Workaround: None

  Fix: Scheduled to be corrected in a future release.

- Issue: ACM Expedite only shows the number of global actions that appear on the first page of the global actions list in ACM.

  Description: There is a setting in ACM that lets operators set the number of items that should be displayed on each page. By default, only 20 items are displayed per page. If there are more items to display, pagination will be displayed to navigate through them. ACM Expedite only loads the items that are displayed on the first page.

  Affected Version: ACM 6.22.0.7 forward

  Workaround: Set the *Items/Page* setting to a value larger than the number of global actions defined in your system. This setting can be found in the *user preference menu*, under *My Account*.

  Fix: Scheduled to be corrected in a future release.

Firmware Included

Controller Firmware:

- **HID VertX V1000/V2000**
  - rcp-update-1.8.2.4
- **Mercury Security**
  - EP1501-VER-1-29-1-0633.crc
  - EP1501-VER-1-29-2-0634.crc
  - EP1502-VER-1-29-1-0633.crc
  - EP1502-VER-1-29-2-0634.crc
  - EP2500-VER-1-29-1-0633.crc
  - LP1501-VER-1-29-1-0633.crc

- LP1501-VER-1-29-4-0647.crc
- LP1502-VER-1-29-1-0633.crc
- LP1502-VER-1-29-4-0647.crc
- LP2500-VER-1-29-1-0633.crc
- LP2500-VER-1-29-4-0647.crc
- LP4502-VER-1-29-1-0633.crc
- LP4502-VER-1-29-4-0647.crc
- M5IC-VER-1-27-1.crc
- M5IC-VER-1-27-5.crc
- MSICS-VER-1-27-1.crc
- MSICS-VER-1-27-5.crc
- pivCLASS-Embedded-Auth-Removal_Pkg_01_00_00_#14.crc
- pivCLASS-Embedded-Auth_Pkg_05_10_27_#145.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:

- **Mercury Security**
  - 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-1-56-15.aax
  - M5-2K-APPL-VER-1-57-12.aax
  - M5-2K_APPL-VER-1-57-6.aax
  - M5-2RP-APPL-VER-1-57-12.aax
  - M5-2RP-APPL-VER-1-57-3.aax
  - M5-2RP-APPL-VER-1-58-6.aax
  - M5-2SRP-APPL-VER-1-57-12.aax
  - M5-2SRP-APPL-VER-1-57-3.aax
  - M5-2SRP-APPL-VER-1-58-6.aax
  - M5-8RP-APPL-VER-1-57-15.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
  - MI-RS4-APPL-VER-1-57-6.aax
  - MR16IN-APPL-VER-3-20-4.aax
  - MR16IN-APPL-VER-3-21-10.aax
  - MR16IN-SER2-APPL-VER-1-32-2.aax
  - MR16IN-SER3-APPL-VER-3-21-0.aax
  - MR16OUT-APPL-VER-3-20-4.aax

- MR16OUT-APPL-VER-3-21-10.aax
- MR16OUT-SER2-APPL-VER-1-32-2.aax
- MR16OUT-SER3-APPL-VER-3-21-0.aax
- MR50-APPL-VER-3-20-4.aax
- MR50-APPL-VER-3-21-10.aax
- MR50-SER2-APPL-VER-1-53-15.aax
- MR50-SER2-APPL-VER-1-54-4.aax
- MR50-SER3-APPL-VER-3-21-0.aax
- MR51E-SER2-APPL-VER-1-8-14.aax
- MR51E-SER2-APPL-VER-1-8-4.aax
- MR52-APPL-VER-3-20-4.aax
- MR52-APPL-VER-3-21-10.aax
- MR52-SER1-APPL-VER-1-11.aax
- MR52-SER2-APPL-VER-1-58-11.aax
- MR52-SER2-APPL-VER-1-59.0.aax
- MR52-SER3-APPL-VER-3-21-0.aax
- MR62E-SER3-APPL-VER-3-21-0.aax
- MR62E-SER3-APPL-VER-3-21-10.aax
- MRDT-APPL-VER-1-63-0.aax
- MRDT-APPL-VER-1-63-4.aax
- MRDT-APPL-VER-1-63-8.aax
- MS-ACS-APPL-VER-1-0-5.aax
- MS-ACS-APPL-VER-1-0-6.aax
- MS-ACS-APPL-VER-1-00-10.aax
- MS-I8S-APPL-VER-1-0-1.aax
- MS-R8S-APPL-VER-1-0-2.aax
- MS-R8S_APPL-VER-1-0-1.aax