

## Access Control Manager<sup>™</sup> 6.0.0.24 Release Notes

Version 6.0.0.24 – Released Tuesday, January 8, 2020

### Files Released

#### Avigilon Access Control Manager Physical Appliance Files

- acm-upgrade-V6.0.0.24-20191231-083114.upgrade


#### Avigilon Access Control Manager Virtual Appliance Files



- ACM\_VM\_V6.0.0.ova
- ACM\_VM\_6.0.0.24.zip

### Upgrade Path

Contact Technical Support if an error occurs during the upgrade process

#### Upgrade the ACM Software

1. Always perform a configuration and transactions backup of the current version prior to any upgrade. Refer to prior version release notes for upgrade paths.
2. There is no direct upgrade path to ACM 6.0.0.24 from revisions prior to ACM 5.12.2.
3. The system must first be upgraded to ACM 5.12.2 and then to 6.0.0.24. Please refer to the 5.12.2 upgrade release notes prior to any upgrade.
4. ACM system that have a DEMO license (visible on the help about tab under  > **Appliance**) require a permanent license prior to being upgraded to ACM 6.0.0.24.
5. Perform a configuration and transactions backup of ACM 5.12.2
6. Download the ACM 6 upgrade file from <http://avigilon.com/support-and-downloads/for-software/acm/downloads/>
7. Manual door modes set through the ACM UI or via global actions will be reverted to scheduled door modes following the upgrade, it is recommended to restore all doors prior to upgrades.
8. 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 6.0.0.24)
9. Upgrades are supported on ACM Professional (Dell OptiPlex XE2, XE3) ACM Enterprise (Dell PowerEdge R210, R220, R230 and MBX) and Enterprise PLUS (Dell PowerEdge R330)
10. The appliance will be offline from clients and controllers for the duration of the process.
11. 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.


12. 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.
13. ACM Virtual instances should have VMNic1 and VMNic2 connected in the VMWare host prior to performing ACM 6.0.0.24 upgrade.
14. Identity account used to perform the upgrade may require inactivity timer set to indefinite for extended upgrade times to observe status without requiring to log in again.
15. The upgrade instructions can be found in Access Control Manager (ACM) help menu.
16. Log into the ACM appliance, select  > **Appliance**.
17. In the Software Update tab, click **Add Software Update**.
18. Click **Choose File**.
19. Open the software upgrade file and then click **Save**.
20. Click , then click **OK** in the system warning to begin the upgrade process.
21. Wait for the system to reboot.
22. When the update process is complete and the reboot is complete, you'll be asked to log in and accept the End User License Agreement.

### Upgrade Your License Format

ACM 6.0.0.24 does not require the license format to be upgraded to continue to function normally. ACM 6.0.0.24 does use a different license format than ACM 5.12.2. Follow the instructions below to upgrade your license format to ensure access to new licensed features.


*Note: If you do not upgrade your license format, you can continue to use your existing ACM features. However, you will not be able to license new capabilities or features in the future until the license format is updated.*

*Note: If your system is licensed for more than the maximum number of supported readers, you will not be eligible for an upgrade license.*

1. In the ACM appliance, select  > **Appliance**.
2. In the About tab, click **Download Upgrade File**. The file will be saved to your browser's default Download location.
3. Email the .bin file to [acm.license@avigilon.com](mailto:acm.license@avigilon.com). You will receive a response in 1-2 business days with an Activation ID for each feature you have. You can continue to use the ACM appliance during this time.

### Activate Your New License

After [acm.license@avigilon.com](mailto:acm.license@avigilon.com) emails you a list of Activation IDs, add them to your system.

1. In the ACM appliance, select  > **Appliance**.
2. In the About tab, click **Add License**.
3. If you have Internet access, use the **Automatic** tab. Otherwise, see the instructions for **Offline Licensing** below.

4. Enter one of the Activation IDs you received. Entering one Activation ID will automatically license the system for all features your device is entitled to.
5. Click **Activate Licenses**.

### Offline Licensing

You will need a [licensing.avigilon.com](https://licensing.avigilon.com) account. Contact your organization's Technical Contact for access.

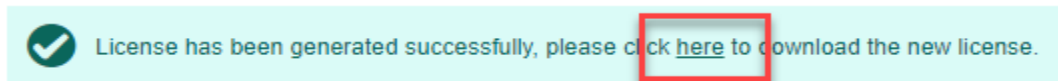
*Note: Offline licensing involves transferring files between a computer running the ACM system and a computer with Internet access.*

#### In the ACM system:

1. Select the **Manual** tab.
2. Click **Save File...** and select where you want to save the .key licensing file. You can rename the file as required.
3. Copy the .key file to a computer with Internet access.

#### In a browser:

1. Go to [licensing.avigilon.com/activate](https://licensing.avigilon.com/activate) and log in.
2. Select the Upload Type **Generate License**, then click **Choose File**.
3. Select the .key file, then click **Upload**.
4. In the success message, click **here** to download the license file: capabilityResponse.bin.



5. Copy the .bin file to a computer running the ACM system.

#### In the ACM system:

1. In the Add Licenses dialog, click **Choose File**.
2. Select the .bin file and click **Open**.
3. Click **Activate Licenses**.

## ACM Virtual Appliance

- Importing ACM Virtual Appliance ACM\_VM\_6.0.0.24.ova requires a minimum of **vSphere version 6.5**

## ACM with ACC Integration Upgrade Instructions

- NOTE: Previous versions to 6.14.4.6 of AvigilonAcmlIntegrations are not compatible with ACM 6.0.0.24. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.
- Instructions for installing AvigilonAcmlIntegration-6.14.4.6.exe

- a. Download AvigilonAcmlIntegration- 6.14.4.6 from  
[https://partners.avigilon.com/prm/api/objects/v1/asset/u1bwvrqy6fpm/\\_download?v=2](https://partners.avigilon.com/prm/api/objects/v1/asset/u1bwvrqy6fpm/_download?v=2)
- b. Make a backup copy of Avigilon\ACM to ACC Integration\ACM to ACC Alarm Gateway\AlarmConfig.xml
- c. Uninstall previous version of the AvigilonAcmlIntegration
- d. Reboot the appliance (ACC) that the integration was installed on
- e. Install the AvigilonAcmlIntegration-6.14.4.6
- f. Ensure Vidproxy service is running
- g. Login to the upgraded 6.0.0.24 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 for Peer-to-Peer (2 or more appliances without Hot Standby)**

1. Perform a configuration and transactions backup of ACM 5.12.2
2. For the ACM 6.0.0.24 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.0.0.24 upgrade on a peer-to-peer replicated system, disable the replication on all appliances.
4. Apply the software upgrade to all appliances in any order.
5. Allow the upgrade on all appliances to complete and the appliances to reboot and come back online.
6. Accept the EULA for all appliances.
7. 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 5.12.2
2. For the ACM 6.0.0.24 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.0.0.24 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 Auto Failover**

1. Perform a configuration and transactions backup of ACM 5.12.2
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 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 the upgrades finish successfully on appliance 1 and 2. Accept the EULA's.
7. Navigate to appliance 3 and 4's appliance replication tab, click on fail back button on appliance 3,4. Make sure appliance 1, 2 take the control back successfully (If the first try is 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 the upgrades finish successfully on appliance 3 and 4. Accept the EULA's.
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.*

### **HID Firmware Upgrade**

For systems with HID VertX EVO field hardware, Avigilon recommends upgrade to ACM 6.0.0.24. The HID firmware is part of the ACM 6.0.0.24 upgrade package and will allow you to update the HID VertX EVO field hardware with HID firmware version 3.7.0.108

- After upgrading the ACM to version 6.0.0.24 upgrade HID VertX EVO V1000 with RCP 1.8.2.4. The HID firmware version 3.7.0.108 will be automatically updated as a part of the RCP 1.8.2.4
- Repeat the upgrade for HID VertX EVO V2000 with RCP 1.8.2.4 and HID firmware version 3.7.0.108 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

- Bosch requires an Application Passcode to 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"
- This passcode must be set in both ACM and RPS. If it does not match the panel will fail to connect

*Notes:- For G-series Bosch panels, a number of issues have been noted. Avigilon recommends upgrading the Bosch firmware to minimum 3.04.015*

## ACM with Milestone Integration Installation Instructions

1. All versions below ACM 5.12.2.29 are incompatible with Milestone Vidproxy 1.0.0.0\_2018R3.
2. Instructions for installing Milestone Vidproxy 1.0.0.0\_2018R3
  - a. Install Microsoft .NET version 4.6.2 if it is not already installed on the computer.
  - b. Download MilestoneVidproxy-1.0.0.0\_2018R3 from [https://partners.avigilon.com/prm/api/objects/v1/asset/pbzpdt6iksgx/\\_download](https://partners.avigilon.com/prm/api/objects/v1/asset/pbzpdt6iksgx/_download)
  - c. Run the installer InstallVidProxyService.msi
  - d. Run the installer InstallVidProxyImageService.msi
  - e. Open up the windows Services page, and verify that both VidProxyImageService and VidProxyService have installed and started
  - f. Ensure the active firewall on the windows server hosting VidProxy and Milestone is configured to allow incoming and outgoing traffic for VidProxyService on port 8000, and incoming and outgoing traffic for VidProxyImageService on port 9000
  - g. Go to C://Program Files/Avigilon/VidProxyService/
  - h. Run VidProxyConfig.exe as Administrator
    - i. Modify the ImagePath, this is where VidProxy will store some temporary files, ensure the path is fully qualified and a valid folder.
    - ii. Modify RCServerIP to the IP of the ACM appliance
    - iii. Ensure the ExternalSystemType is set to "Milestone"
    - iv. Set the RCWebUserName to a valid ACM user
    - v. Set the RCWebPassword to a valid ACM user password
    - vi. Modify the x509cert filename to point to a valid x509 certificate file
    - vii. Save Settings.
    - viii. Press "Done" or close the window.
  - i. Open the windows Services Page again, and restart VidProxyService and VidProxyImageService
3. Login to ACM 6.0.0.24 with account with required delegations

- a. Navigate to Settings/External Systems
- b. Select the Milestone tab
- c. Select Add Milestone Server
- d. Set a Name for the server
- e. Set the Address, this must be the IP of the Milestone XProtect server
- f. Set the Port, this must be the XProtect webserver port used to access their web client
- g. Set the User Name, this must be the username used to login to the XProtect client, this must match the login used for XProtect exactly, including the domain if one is used
- h. Set the Password, this must be the password for the XProtect client
- i. Set the VidProxy URL, this must be http://0.0.0.0:8000/VidProxy, where 0.0.0.0 is the IP of the Vidproxy server
- j. Set the VidProxylmage URL, this must be http://0.0.0.0:9000/VidProxylmageService, where 0.0.0.0 is the IP of the Vidproxy server
- k. Check installed
- l. Save
- m. Verify that the flash string indicates that the external system was installed properly
- n. Verify that the status of the newly created server says "Backend Up"
- o. Click on the Address of the external system to see the edit page, and verify that cameras are displayed

## New Features

### Functional Features

- Introducing Avigilon's new licensing portal. Added functionality to support:
  - ACM 6 Licensing Automatic Add
  - ACM 6 Licensing Automatic Remove
  - ACM 6 Licensing Manual Add
  - ACM 6 Licensing Manual Remove
  - ACM 6 Licensing Post Upgrade
  - ACM 6 Licensing New Out of Box Appliance

*Note: ACM 5 appliance and virtual part numbers have been discontinued except for add on licenses, available for sale until March 03, 2020.*

*ACM 6 part numbers will no longer need Mercury/HID hardware licensing part number (AC-SW-MER-RDR and AC-SW-HID-RDR)*

- Added support for Mercury certificates
  - ACM includes CAs for default certificates in Mercury controllers
  - Install Certificates in ACM for custom CAs where appliance validates controllers
  - Panel may have a certificate installed to match loaded peer certificate on appliance where panel validates appliance (peer to peer)

- Enhanced support for encrypted communications between controllers and ACM
  - Mercury controllers have TLS Required selected by default for new panel adds
  - Added new Security column on panel status for TLS Required and Certificate Required
  - Added option to run ACM in FIPS 140-2 compliant mode  
*Note: Enabling this limits the available cipher suite for your ACM installation to ciphers that are only supported on the newer Mercury LP series controllers. This mode should not be enabled if your site uses other controllers.*
- Added support for large card formats (128 bit Card Format)
  - Added default 128 bit large card format to support PIV Cards
  - Added Enable PIV Cards column on panel report
- Extended Mercury support for In/Out OSDP reader per door:
  - Two OSDP reader support for AC-MER-CONT-MR50 Series 3 only
  - Four OSDP reader support for AC-MER-CONT-MR52 Series 3 only
  - Four OSDP reader support for AC-MER-CONT-LP1502
  - Four OSDP reader support for AC-MER-CONT-LP4502
  - Four OSDP reader support for AC-MER-CONT-MR62e
- Increased Mercury controller poll delay Interval option for up to 60,000 milliseconds
- Added limited support in ACM for Mercury AC-MER-CONT-LP4502
- Enhanced ease of installation tools
  - Added default templates (Door, Wiring, Input, Output, Reader)
  - Added new paired door templates (AC-MER-CONT-LP1502, AC-MER-CONT-LP4502, AC-MER-RIM-MR62E)
  - Added functionality for In/Out reader bulk update (AC-MER-CONT-LP1501, AC-MER-CONT-LP1502, AC-MER-CONT-LP4502, AC-MER-CON-MR52, AC-MER-CON-MR50 and AC-MER-RIM-MR62E)
- Updated Avigilon Logo on login page
- Changed naming convention of Mercury panel and subpanel models to match Mercury part numbers

#### Security Enhancements

- CVE-2017-1000405



## Changes

### Fixed Issues

- Corrected issue where in limited circumstances, an unexpected license deactivation may occur. This could result in invalid license errors leading to uninstalled panels, doors or collaborations.
- Corrected issue with ACM 6.0.0.22 upgrade when a custom certificate had been installed for trusted browsing and the upgrade replaced the custom certificate with the default certificate.
- Corrected issue with badge designer font size when using accented characters.
- Corrected issue with custom fonts being dropped in badge designer when upgrading to latest ACM version.
- Corrected issue with scheduled global actions being overwritten by batch jobs created at a later time.
- Corrected issue with verification screen not showing default ID image when there is no picture uploaded for an identity.
- Corrected issue with option to search identities by groups only appearing for System Admin roles.
- Corrected issue with running reports on custom built delegations not returning any results or selecting more than seven default delegations producing results for the initial seven delegations only.
- Corrected issue where some schedules were not applying correctly on some doors.
- Corrected issue when executing a door trace from a map did not display identity information.
- Corrected issue where maximum active token as defined in System Settings were not being respected by batch updates using identity profiles.
- Corrected issue where ACM became unresponsive with a significantly higher number of supported identities were added and required a restart.
- Corrected issue with CSV export collaboration when using passwords with special characters.
- Correct issue where Invalid Card Schedule was indicated in ACM despite schedule being correct and active.
- Corrected issue with transaction and audit reports where full token number was not displayed for long internal card numbers.
- Corrected issue with unacknowledged alarms on maps not displaying the identity information when the identity button is clicked.
- Corrected issue where a validation error is displayed stating that the Maximum Active Token field data is invalid when entering a non numeric text in Maximum Active Token on an Identity Profile.

- Corrected issue with the collaboration screen not displaying an error for a port number set to 00.
- Corrected validation issue when a profile is applied to identities and the token issue/activate/deactivate date settings are invalid.
- Corrected issue with door status for Schlage wireless doors with unassigned door number appearing online instead of a communication alarm on the door page.
- Corrected issue with IP camera preview not displaying live image and door camera viewer not displaying live video on browsers other than Chrome and Firefox.
- Corrected issue with panel status active alerts count not including battery alarms.
- Corrected issue with icons appearing on the left of text when system language is set to Arabic.
- Corrected issue with an uninstalled policy assigned to a group of doors resulting in the global action door mode being overwritten by the default door mode, when executed on that group of doors.
- Corrected issue with dragging the ACM window causing character wrapping and making buttons non-clickable, for systems set to any language other than Arabic, Mandarin, English US / UK.
- Corrected issue with card formats defined above 64 bits in ACM, when assigned to doors linked to HID VertX V1000 or V2000 panels causing the panels to briefly go offline.
- Corrected issue with status of a panel and its children not being displayed when the panel time is changed to a past time, unless the appliance is rebooted.
- Corrected issue with appliance on vSphere not honoring the time entered in the "Set Date/Time" field and switching over to local time after it has been rebooted.
- Corrected issue with setting a time greater than 4PM in UTC time zone for the "Issue date" of an Identity Profile causing the date to display as the next day on the Identity Edit page.
- Corrected issue with error message associated to deleting doors that belong to a group repeating group names.
- Corrected issue using peer to peer replication appliances where maps status bar disappears on the secondary appliance map and the override indicator is empty even when the door is in active override range.
- Corrected issue with setting up doors on replicated systems causing values of optional fields not being saved when required fields are left blank.
- Corrected issue with secondary appliance not taking over the maps area data from the primary appliance in a replicated system with standby failover appliance enabled.
- Corrected issue with Ldap collaboration certificate validation not working until the collaboration configuration is saved.
- Corrected error message resulting from issuing a REST call for door\_status.

- Corrected error message resulting from playing recorded video from a motion detect event for an Exacq system.
- Corrected error notification for mismatch between subpanel selected in ACM and the physically connected subpanel, to correctly display the connected panel rather than the selected panel.
- Corrected issue with ACM reporting different firmware versions for an Aperio subpanel that is uninstalled from ACM 5.12 and installed on a later ACM version.
- Corrected issue with ACM reboot taking very long due to duplicate transactions being downloaded from panels, resulting in memory issues and multiple alarms needing acknowledgement.
- Corrected error resulting due to subpanels not inheriting the partition from Mercury EP/LP 1501 panels.
- Corrected issue with panel report not displaying the model name for some panels.
- Corrected issue with all camera icons on a map showing the same feed from an Exacq server and disregarding the camera linked to the icon.
- Corrected issue with the identity create action not honoring roles passed using the REST API integration.
- Corrected issue with the dashboard inputs and outputs do not display correct status.
- Corrected issue where Save and Edit do not work for identity image capture.
- Corrected issue connecting to ACM after changing the web server port.
- Corrected issue with elevator access level schedules not being displayed on the panel schedules tab.
- Corrected issue with the Avigilon end user license agreement not being displayed when using locale Arabic.

## ACM Known Issues

- Issue: ACM-ACC Unification - ACM connection keeps on dropping  
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  
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: EP1501 door count not enforced by ACM  
Description: ACM will allow you to assign more number of doors than actually supported by an EP1501.  
Affected Version: ACM 5.12.2.31  
Workaround: Ensure no more than 17 readers configured on an EP1501.  
Fix: Scheduled to be corrected in a future release.
- Issue: Use/Lose not validating for other events  
Description: When use/lose feature is enabled, some events won't generate a last used date despite the card being used on the door, and may cause the card to deactivate once the threshold is reached.  
Affected Version: ACM 5.12.2.31  
Workaround: Apply use/lose exemption on tokens being impacted.  
Fix: Scheduled to be corrected in a future release.
- Issue: Wireless door unable to enter into priority mode  
Description: Priority policy fails to take effect if priority policy is moved from available to member list while the door is in lock function.  
Affected Version: ACM 5.12.2  
Workaround: During a High-Priority Situation, do not allow any configuration, maintenance, or scheduled maintenance operations.  
Fix: Scheduled to be corrected in a future release.
- Issue: Attempting to load LP series firmware onto EP series panels results in download loop  
Description: When attempting to load an LP series firmware version of any panel model onto an EP series panel, the EP series panel goes into an endless online offline download loop.  
Affected Version: ACM 5.12.2  
Workaround: Restarting ACM stops the download loop and allows the EP panel to resume normal operations.  
Fix: Scheduled to be corrected in a future release.

- Issue: Override updates unable to overwrite previous settings  
Description: Override that updates start time and override mode in the same edit does not remove the previous settings.  
Affected Version: ACM 5.12.2.31  
Workaround: Issue a Restore command.  
Fix: Scheduled to be corrected in a future release.
- Issue: MR62e host name change does not take effect in DHCP  
Description: When an MR62e is set for DHCP, a host name change does not take effect without a panel reset/download.  
Affected Version: 5.12.2  
Workaround: Reset/download the panel.  
Fix: Scheduled to be corrected in a future release.
- Issue: HID Door getting dissociated to panel during an LFS-> Yocto upgrade  
Description: When upgrading a system to ACM 5.12.2, HID doors with an active custom door mode of “Unlocked” may result in UI erroneously displaying the door status as secured and generating alarms when the door is open.  
Affected Version: ACM 5.12.2  
Workaround: Reset/download the panel.  
Fix: Scheduled to be corrected in a future release.
- Issue: Viridi Biometric Enrollment Manager will not launch on IE11  
Description: The BE manager using Internet Explorer 11 will not launch and display an error message “BE Manager not running”.  
Affected Version: ACM 5.12.2  
Workaround: Use a browser other than Internet Explorer when launching the BE Manager.  
Fix: Scheduled to be corrected in a future release.

- **Issue:** Area Identity Report (PDF) causes rails error in French and Italian

Description: When trying to generate a PDF of the Area Identity Report, the system may display an error when the system language is set to French or Italian.

Affected Version: ACM 5.12.0

Workaround: Generate a CSV file and convert it to a PDF format.

Fix: Scheduled to be corrected in a future release.

- **Issue:** HID door mode previously set by global action becomes active again when custom schedule modified

Description: When editing a custom schedule (not currently active) that is associated with an HID door with a base mode of "Card Only", the door mode that was previously set by a global action could become active on the door again.

Affected Version: ACM 5.10.0, 5.12.0

Workaround: Restore the doors to put them back into their base door mode.

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-1-27-1.crc
  - EP1501-VER-1-27-5.crc
  - EP1502-VER-1-27-1.crc
  - EP1502-VER-1-27-5.crc
  - EP2500-VER-1-27-1.crc
  - EP2500-VER-1-27-5.crc
  - LP1501-VER-1-27-1.crc
  - LP1501-VER-1-27-5.crc
  - LP1502-VER-1-27-1.crc
  - LP1502-VER-1-27-5.crc
  - LP2500-VER-1-27-5.crc
  - LP2500-VER-1-27-1.crc
  - EP4502-VER-1-27-2.crc
  - EP4502-VER-1-27-5.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
  - Scp2-AES-VER-3-120.crc
  - Scp2-VER-3-120.crc

- o ScpC-AES-VER-3-120.crc
- o ScpC-VER-3-120.crc
- o ScpE-AES-VER-3-120.crc
- o ScpE-VER-3-120.crc

**Sub-Panel Firmware:**

- **Mercury Security**
  - o M5-16DO-APPL-VER-1-32-2.aax
  - o M5-16DOR-APPL-VER-1-32-2.aax
  - o M5-20IN-APPL-VER-1-32-2.aax
  - o M5-20IN-APPL-VER-1-32-3.aax
  - o M5-2K-APPL-VER-1-56-15.aax
  - o M5-2K-APPL-VER-1-57-12.aax
  - o M5-2K\_APPL-VER-1-57-6.aax
  - o M5-2RP-APPL-VER-1-57-12.aax
  - o M5-2RP-APPL-VER-1-57-3.aax
  - o M5-2RP-APPL-VER-1-58-6.aax
  - o M5-2SRP-APPL-VER-1-57-12.aax
  - o M5-2SRP-APPL-VER-1-57-3.aax
  - o M5-2SRP-APPL-VER-1-58-6.aax
  - o M5-8RP-APPL-VER-1-57-15.aax
  - o M5-8RP-APPL-VER-1-57-5.aax
  - o M5-8RP-APPL-VER-1-57-9.aax
  - o MI-RS4-APPL-VER-1-57-3.aax
  - o MI-RS4-APPL-VER-1-57-6.aax
  - o MR16IN-APPL-VER-1-32-1.aax
  - o MR16IN-APPL-VER-1-32-2.aax
  - o MR16IN-APPL-VER-3-20-4.aax
  - o MR16IN-SER2-APPL-VER-1-32-2.aax
  - o MR16IN-SER3-APPL-VER-3-21-0.aax
  - o MR16OUT-APPL-VER-1-32-1.aax
  - o MR16OUT-APPL-VER-1-32-2.aax
  - o MR16OUT-APPL-VER-3-20-4.aax
  - o MR16OUT-SER2-APPL-VER-1-32-2.aax
  - o MR16OUT-SER3-APPL-VER-3-21-0.aax
  - o MR50-APPL-VER-1-52-14.aax
  - o MR50-APPL-VER-1-53-3.aax
  - o MR50-APPL-VER-3-20-4.aax
  - o MR50-SER2-APPL-VER-1-53-15.aax
  - o MR50-SER3-APPL-VER-3-21-0.aax
  - o MR51E-APPL-VER-1-5-12.aax
  - o MR51E-APPL-VER-1-6-12.aax
  - o MR51E-SER2-APPL-VER-1-7-6.aax
  - o MR51E-SER2-APPL-VER-1-8-4.aax

- MR52-APPL-VER-1-57-13.aax
- MR52-APPL-VER-1-57-5.aax
- MR52-APPL-VER-3-20-4.aax
- MR52-SER1-APPL-VER-1-11.aax
- MR52-SER2-APPL-VER-1-57-15.aax
- MR52-SER2-APPL-VER-1-58-11.aax
- MR52-SER3-APPL-VER-3-21-0.aax
- MR52-SERIES1-VER-1-11.aax
- MR62E-SER3-APPL-VER-3-21-0.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