Access Control Manager™ 5.12.2.29 Release Notes

Version 5.12.2.29 – Released Friday, March 22, 2019

Files Released

Avigilon Access Control Manager Physical Appliance Files

- 5.12.2.29-64 bit OS and Application Upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_5.12.2.29.ova
- ACM_VM_5.12.2.29.zip

Upgrade Path

1. There is no direct upgrade path to ACM 5.12.2.29 from revisions prior to ACM 5.12.0, SR1 or SR2. If not at ACM 5.12.0 or one of the service releases, ACM must first be upgraded to 5.12.0 SR2 and then to 5.12.2.29
   The upgrade package for ACM 5.12.0 SR2 is available at ftp://ftp.avigilon.com/ACM/5.12.0_SR2/
   The release notes for ACM 5.12.0 SR2 are available at ftp://ftp.avigilon.com/ACM/5.12.0_SR2/ACM 5 12 0 SR2 Customer Release Notes.pdf

2. 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

3. 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

4. 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 - ACM 5.12.2 includes OS upgrade to 64 bit

Perform a full backup (configuration and transactions) of ACM 5.12.0 prior to applying this upgrade

- DO NOT PROCEED WITHOUT AN ACM 5.12.0 BACKUP
- DO NOT POWER CYCLE THE APPLIANCE DURING THE UPGRADE PROCESS (UPS RECOMMENDED)
- 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 5.12.2)
- Upgrades are supported on ACM Professional (Dell OptiPlex XE2) ACM Enterprise (Dell PowerEdge R210, R220, R230 and MBX) and Enterprise PLUS (Dell PowerEdge R330)
- The appliance will be offline from clients and controllers for the duration of the process
- ACM 5.12.2 does not support licensing for Dedicated Micros, please contact technical support for new license prior to upgrade
- This upgrade may take significantly longer to complete than our previous upgrades. The duration of the upgrade process is directly proportional to amount of data stored on the appliance
- 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 VMWare host prior to performing ACM 5.12.2 upgrade
- The new ACM 5.12.2 upgrade monitor that is running during the upgrade has been set to communicate over port 8888, modifications may be required for any external service ports that have been set to use port 8888 on the ACM appliance page until the upgrade completes
- ACM 5.12.2 includes 64 bit OS with different TLS fingerprint and in some cases network switches may not recognize it as valid destination for static IP already allocated to ACM in previous release. Refreshing cache on the switch resolves this issue of inability to connect to ACM after reboot during upgrade process.

NOTE: Please be patient and do not reboot or power off the appliance during the upgrade

- The upgrade from ACM 5.12.0 to ACM 5.12.2 includes an upgrade to the operating system from 32 bit Linux to 64 bit Linux which requires the databases to be migrated. This upgrade may take between 1 to 12 hours (depending on the size of databases) to complete based on QA testing, (see examples below) please plan accordingly
- For smaller systems the following may be used as estimates based on Avigilon engineering testing

  - Readers=20, Identities=800, Identity photo file size=0, Stored transactions=500,000, Appliance=ACM Professional, Upgrade time=15 minutes, Post upgrade Re-index=1 minute
  - Readers=32, Identities=1000, Identity photo file size=2MP, Stored transactions=1,000,000, Appliance=ACM Professional, Upgrade time=20 minutes, Post upgrade Re-index=2 minutes
  - Readers=200, Identities=3000, Identity photo file size=2MP, Stored transactions=10,000,000, Appliance=ACM Enterprise, Upgrade time=50 minutes, Post upgrade Re-index=45 minutes
  - Readers=800, Identities=10,000, Identity photo file size=2MP, Stored transactions=50,000,000, Appliance=ACM Enterprise, Upgrade time=2 hours, Post upgrade Re-index=4 hours
  - Readers=2000, Identities=30,000, Identity photo file size=5MP, Stored transactions=100,000,000, Appliance=ACM Enterprise PLUS, Upgrade time=2 hours, Post upgrade Re-index=8 hours

    - Upgrades include drive re-partitioning, a full OS upgrade from 32bit to 64bit, database migrations and feature upgrades
    - Upgrade times provided are intended as guidelines for typical systems. Upgrade time will vary based on system configurations and data
    - Upgrade times are based on tests conducted in Avigilon Engineering Labs
    - Post upgrade re-index includes time for data in ACM databases to be fully available for reporting purposes

- For ACM systems with large databases , please contact Tech Support to obtain more precise estimates of upgrade times. As with previous ACM upgrades, doors will continue to operate as usual during the upgrade and transactions will cache on controllers and transfer to ACM once the upgrade is complete
- 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

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
d. Follow the instructions to apply the ACM 5.12.2 upgrade
e. Wait for the system to reboot
f. After reboot, the ACM 5.12.2 Upgrade Monitor loads. Note, ACM will reboot a second time during this process
g. After upgrade is complete, click "Login" on the ACM 5.12.2 Upgrade Monitor to open ACM 5.12.2

Please contact Tech Support if error occur during upgrade for troubleshooting or to restore the system to the previous version

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 Virtual Appliance

- Importing the new ACM Virtual Appliance ACM_VM_5.12.2.29.ova requires a minimum of ***VSPhere version 6.5***
- For existing ACM using VMWare, Avigilon engineering recommends setting the VM to 64bit prior to the ACM 5.12.2 upgrade

ACM with ACC Integration Upgrade Instructions

➢ NOTE: Previous versions to 5.8.4.13 of AvigilonAcmIntegrations are not compatible with ACM 5.12.2. 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 ftp://ftp.avigilon.com/ACM_Integrations/
    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 5.12.2 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. For the ACM 5.12.2 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade
2. For the ACM 5.12.2 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. For the ACM 5.12.2 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade
2. For the ACM 5.12.2 upgrade on a hot standby replicated system, manually failover to let the secondary appliance take over the session
3. Disable replication on both appliances
4. Apply the upgrade to the primary appliance and accept the EULA once it completes
5. On the secondary appliance replication page, click “Fail back” and make sure the primary appliance takes over the session
6. Upgrade the secondary appliance and accept the EULA once it completes
7. Re-enable replication on both appliances

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

1. Appliance 1 and 2 are peer to peer; appliances 3 and 4 are failover appliances monitoring 1 and 2 respectively
2. 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
3. Navigate to appliance replication tab on each appliance. Uncheck enable replication and save the configuration on each appliance
4. Upload upgrade file to appliance 1 and 2. Apply the upgrade files on 1 and 2
5. Wait till lfs to yocto upgrade finishes successfully on appliance 1 and 2. Accept the EULA.
6. 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 (First try might not succeed, try multiple times). Observe that panels are online on appliance 1

7. Upload upgrade file to appliance 3 and 4. Apply the upgrade files on 3, 4
8. Wait till lfs to yocto upgrade finishes successfully on appliance 3 and 4. Accept the EULA.
9. 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 5.12.2.29 The HID firmware is part of the ACM 5.12.2.29 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 5.12.2.29, 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

- 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"
- 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 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 **http://avigilon.com/support-and-downloads/for-software/acc/integration-and-plug-in-downloads/**
    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 5.12.2 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 VidProxyImage URL, this must be http://0.0.0.0:9000/VidProxyImageService, 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

Platform Enhancements

- ACM 5.12.2 is the first release built on 64-bit linux. As such, the upgrade process will perform additional disk re-partitioning and database migrations as outlined in sections above

Functional Features

- Added functionality to create new templates for ease of new hardware configuration
  - Added templates for readers, inputs and outputs
  - Added wiring templates for controllers and sub-panels
- Enhanced subpanel bulk add for new subpanels and doors from templates
  - Added bulk add wizard to add new panels and subpanels using templates
  - Added controls to change order of subpanels added
  - Added interface to name new doors created with a template with propagating name to readers, inputs and outputs
- Added support for the Mercury LP Series controllers
  - AC-MER-CONT-LP1501 - Series 3 One door controller expandable to 17 doors with PoE+
  - AC-MER-CONT-LP1502 - Series 3 Two door controller expandable up to 64 doors
  - AC-MER-CONT-LP2500 - Series 3 Expandable controller up to 64 doors
- Added support for the Mercury AC-MER-RIM-MR62E reader module
- Added functionality to create Schedule Door Mode Overrides from the Doors Listing page for doors on Mercury controllers running firmware v1.27.1 or greater
  - Added button to create Overrides on one or more doors in the Doors tab
  - Added Override window to specify the following for each Override:
    - Override name
    - Door mode
    - Start time
    - End time
    - Notes
  - Added Override indicator on Doors tab to display active and scheduled (past or future) Overrides
  - Added Override indicator on Maps to display active and scheduled Overrides
  - Added button to display Override listings page on top right corner
  - Added Override listings page to display all overrides
- Added functionality to create backups and download to a local drive via the browser
- Enhanced search function on text, integer, date and internal number fields
  - Added ‘Not Equals,’ ‘Is Empty,’ for text and integer fields
  - Added ‘Not equals’, ‘Greater than,’ and ‘Less than’ for integer fields
  - Added ‘Not Equals,’ ‘Greater than,’ ‘Equals’ and ‘Less than’ for Integer number search
  - Changed ‘during’ to ‘equal’ for date fields
- Enhanced support for additional Card formats
  - Increased number of supported card formats per panel to 16
  - Increased number of supported card formats per appliance to 128

- Added functionality to monitor real-time hardware status
    - Replaced Hardware Status Tab with Dashboard tab under Monitor tab
    - Added tooltips for current Appliance status
    - Added Dashboard Panels listings page with sortable columns
    - Added accordion view for subpanels, inputs and outputs under Panels
    - Added Dashboard Doors listings page with sortable columns
- Added Upgrade Monitor with visual status of upgrade progress
- Refreshed the ACM Professional Appliance to the Dell OptiPlex XE3 (coming Q2 2019)
    - Improved processor and RAM
    - Reduced size
    - Next generation platform

Performance Enhancements

- Scalability Improvements relating to the downloading of Token information to panels
- Improved efficiency of Area based tracking
- Optimizations for Enterprise Plus appliance to take advantage of additional available memory
- OpenLDAP configuration database upgrade
- Scalability improvements when issuing commands to panels

Security Enhancements

- ACM will now accept minimum of TLS v1.2 connections, (TLS v1.1 and lower are no longer supported) Upgrades of connected solutions are required
- CVE-2016-0800
- CVE-2014-3566
- CVE-2013-2566
- CVE-2015-2808
- CVE-2015-4000
- CVE-2016-2107

Changes
Fixed Issues

- Corrected an issue where paired master doors on HID panels configured with Hard Area APB allowed an identity/token into a second area although the identity/token did not exit the first area.
- Corrected an issue where the Alarm report failed to generate when an Operator account mentioned in the report is deleted from the system.
- Corrected an issue where the Monitor search did not return any results when searching for sources with capital Cyrillic letters.
- Corrected an issue where searching transaction reports by full name did not return any results.
- Corrected an issue where the Windows Share Backup failed when the user password contains a dollar symbol.
- Corrected an issue where the identity CSV collaboration failed if SMBv1 was disabled on the host file server.
- Corrected an issue where identity profile update background jobs failed when an identity profile contains a forward slash symbol.
- Corrected an issue where doors did not appear on the door listings page when the panel name included a backslash symbol.
- Corrected an issue where panels could not be filtered by appliance or group.
- Corrected an issue where a new door created from a template had blank door processing attributes if there was only one vendor enabled.
- Corrected an issue where scheduled identity summary CSV reports do not process selected filters.
- Corrected an issue where Transaction reports were not saved if entries contained quotation marks.
- Corrected an issue where a field with a single word did not line wrap correctly.
- Corrected an issue where the group drop down list ignored partitioning on the identity search page.
- Corrected an issue where the schedule for a door did not download when the door was switched to a different panel.
- Corrected an issue where the LDAP collaboration failed to import long user list items.
- Corrected an issue where corporate card formats were processed incorrectly for HID panels.
- Corrected an issue where backups could not be created on a hidden shared folder.
- Corrected an issue where a USB badging camera did not connect when using newer versions of supported browsers.
- Corrected an issue where a reader could not be added to a door while using the Russian language locale.
- Corrected an issue where a badge with an empty Name field could be erroneously created.
- Corrected an issue when using HID hardware that "Occupancy count reached up limit" and "Occupancy count reached max" events are generated multiple times.

- Corrected issue where duplicate configuration of external domains were allowed.
- Corrected issue where integration to Milestone XProtec failed.
- Corrected issue when using HID hardware where area count cannot achieve maximum occupancy after panel reset.
- Corrected issue with Mercury panels going offline during role information update when using Mercury firmware prior to 1.27.1.
- Corrected error when searching for values in identity search using empty "Contains" search.
- Corrected issue with incorrect door status display when issuing door commands from a map UI to wireless locks that do not have extended mode activated.
- Corrected issue preventing migrating ACM EC with FW 1.8.2.2.
- Corrected issue where Grant via Operator Report does not return results.
- Corrected issue where identity search with special characters resulted in inconsistent results.
- Corrected an issue where hardware status updates are not reflected in the UI.
- Corrected an issue where the door alarm event count on maps was not counting Normal return events.
- Corrected an issue where the saved string matching search criteria for Access Grant via Operator Report displayed extra characters next to the search string.
- Corrected an issue where a badge type assigned to one or more users could be erroneously deleted.
- Corrected an issue where ACC events did not display correctly in global linkages.
- Corrected an issue where video servers linked to a global linkage could be deleted.
- Corrected an issue where a CSV identity without internal number was erroneously imported.
- Corrected an issue where door state was reported as closed rather than unknown when the panel was offline.
- Corrected an issue where trigger variable for macros allowed invalid selection.
- Corrected an issue where door and panel statuses from an appliance without a time server were not displayed after the appliance rebooted.
- Corrected an issue where the advanced filters on the door listing page was inconsistent with the basic filter.
- Corrected an issue where the door elevator tab data REST calls were missing the XML format tags.
- Corrected an issue where the Input/Output mask status was not updating in real time on the Hardware Status page.
- Corrected an issue where the Door Number drop down list for a PIM or Gateway displayed an incorrect option when there are two or more PIMs or Gateways associated with a panel.
- Corrected an issue with the Token Report displaying only Active Tokens when no token status was specified.
- Corrected an issue where elements on the Badge designer preview was not deleted dynamically.

- Corrected an issue where the Badge Designer allowed invalid values for badge photo dimensions.
- Corrected an issue with the instructions icon shortcut in Events Monitor not displaying instructions every time.
- Corrected an issue where Door Templates did not deassign partitions to doors.
- Corrected an issue where a user could view doors from all partitions on the Group page.
- Corrected an issue where non-applicable Door Processing Attributes were displayed on the Door Edit page for NDE, LE or SimonsVoss doors.
- Corrected an issue with the Maximum Active Tokens search in Identity Search displaying invalid search criteria.
- Corrected an issue where the Destroy Batch button became unavailable after identity deletion and search.
- Corrected an issue where extra events were generated when changing a door mode from the Door listings page.
- Corrected an issue where uninstalling an LE or NDE door erroneously generated an "Secure Channel not enabled" event.
- Corrected an issue where the Door List screen did not display extended door mode for wireless locks.
- Corrected an issue where double card taps on wireless doors were not displayed correctly on the Events page.
- Corrected an issue where door names containing special characters were displayed incorrectly.
- Corrected an issue where the background color of a text field in badge designer was not the same as the badge background color.
- Corrected an issue where GMT offsets with half hour offsets did not display on the Events monitor.
- Corrected an issue where the panels could not be filtered by appliance or group on the Panels page.
- Corrected an issue where manually executed Bosch intrusion global actions were not logged in the event monitor.
- Corrected an issue where the display indicators for a door under manual command or priority did not display properly after hot standby failover.
- Corrected an issue where a scheduled job to update SimonsVoss wireless doors failed repeatedly.
- Corrected an issue where the user issued command indicator on a wireless door was removed in error after uninstalling a policy on the door.
- Corrected an issue where 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.
- Corrected an issue where the privacy button on AD-400 wireless locks does not lock the door when the lock is connected to a Mercury panel with firmware version 1.25.6, Mercury firmware 1.26.4 and later corrects issue.
- Corrected an issue when rebooting a panel caused door modes to revert to default configuration during a global action.

- Corrected an issue causing door modes to revert to default configuration after panel reset/download or parameter download during a priority global action.
- Corrected an issue where door modes revert to default configuration when doors are uninstalled during a priority global action.
- Corrected an issue where barcode fonts for badge designs do not display correctly after upgrade to ACM 5.12.2.25
- Corrected an issue where fonts for badge designer were missing from badge designs after upgrade to ACM 5.12.2.25
- Corrected an issue where ODBC connections stopped working after upgrade to ACM 5.12.2.25
- Corrected issue where Schlage AD300 toggled online/offline status when AD300 & AD400 are communicating with the same Engage gateway

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: 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: 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: ACM 5.12.2 - Mercury MR62e VER-3-21-0
  Workaround: Reset/download the panel.
  Fix: Scheduled to be corrected in a future Mercury firmware release

Firmware Included

Controller Firmware:

- **HID VertX V1000/V2000**
  - rcp-update-1.8.2.4
- **Mercury Security**
  - EP1501-VER-1-26-9.crc
  - EP1501-VER-1-27-1.crc
  - EP1502-VER-1-26-9.crc
  - EP1502-VER-1-27-1.crc
  - EP2500-VER-1-26-9.crc
  - EP2500-VER-1-27-1.crc
  - LP1501-VER-1-26-9.crc
  - LP1501-VER-1-27-1.crc
  - LP1502-VER-1-26-9.crc
  - LP1502-VER-1-27-1.crc
  - LP2500-VER-1-26-9.crc
  - LP2500-VER-1-27-1.crc
  - M5IC-VER-1-26-9.crc
  - M5IC-VER-1-27-1.crc
  - MSICS-VER-1-26-9.crc
  - MSICS-VER-1-27-1.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:

- **Mercury Security**
  - M5-16DO-APPL-VER-1-32-2.aax
  - M5-16DOR-APPL-VER-1-32-2.aax
  - M5-20IN-APPL-VER-1-32-3.aax
  - M5-2K-APPL-VER-1-57-12.aax
  - M5-2RP-APPL-VER-1-58-6.aax
  - M5-2SRP-APPL-VER-1-58-6.aax
  - M5-8RP-APPL-VER-1-57-15.aax
  - MI-RS4-APPL-VER-1-57-6.aax
  - MR16IN-SER2-APPL-VER-1-32-2.aax
  - MR16IN-SER3-APPL-VER-3-21-0.aax
  - MR16OUT-SER2-APPL-VER-1-32-2.aax
  - MR16OUT-SER3-APPL-VER-3-21-0.aax
  - MR50-SER2-APPL-VER-1-53-15.aax
  - MR50-SER3-APPL-VER-3-21-0.aax
  - MR51E-SER2-APPL-VER-1-7-6.aax
  - MR51E-SER2-APPL-VER-1-8-4.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
  - MR62E-SER3-APPL-VER-3-21-0.aax
  - MRDT-APPL-VER-1-63-8.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