Access Control Manager™ 6.36.0.14 Release Notes

Version 6.36.0.14 – Released Tuesday, October 4, 2022

Files Released

Access Control Manager Physical Appliance Files

- ACM-6.36.0.14-20220917-181558.upgrade

Access Control Manager Virtual Appliance Files

- ACM_VM_VMware_6.36.0.14.zip
- ACM_VM_Hyper-V_6.36.0.14.zip

ACTION REQUIRED

HID MERCURY LP INTELLIGENT CONTROLLERS FIRMWARE AVAILABLE

As a reminder, HID Global was recently informed of cybersecurity vulnerabilities within firmware running on all Mercury LP and EP4502 Intelligent Controllers. HID Global addressed all issues reported, validated fixes and made the new firmware available.

ACM displays a banner on top of every page when there is at least one installed LP controller running firmware earlier than v.1.30.3.

We recommend upgrading all panels to firmware version 1.30.3 or newer.

Note

Upgrading from ACM version 6.26.0.32 or earlier will take longer to complete than usual due to a transaction database update.
On an ENTERPRISE PLUS system with 5,000,000 stored transactions, the transaction update will add about 5 minutes to the usual upgrade time. With 150,000,000 stored transactions, the same system will take about 2 hours more than usual to upgrade.
ACM will not be accessible during this extended upgrade time, please plan accordingly.

Upgrade Path

NOTE: ACM 6.36.0.14 is not compatible with versions prior to 6.14.20.2 of ACC/ACM Integration. The recommendation is to upgrade existing ACC/ACM integrations to current versions of ACM and ACC.
NOTE: ACM 6.36.0.14 is not compatible with versions of the Milestone VidProxy Services prior to 1.2.0.0. Download the latest version of Milestone VidProxy Services from https://www.avigilon.com/software-downloads/.

1. There is no direct upgrade path to ACM 6.36.0.14 from ACM 6.0.0. The system must first be upgraded to ACM 6.2.0 then to 6.36.0.14. Please refer to the 6.36.0.14 upgrade release notes for further information.
2. 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.
3. 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.
4. 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.
5. 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.

ACM Upgrade Instructions

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

1. Manual door modes set thru the UI or via global actions will be reverted to scheduled door modes following the upgrade
2. 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 6.36.0.14)
3. 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)
4. The appliance will be offline from clients and controllers for the duration of the process
5. 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

6. 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
7. ACM Virtual instances should have VMNic1 and VMNic2 connected in the host prior to performing ACM 6.36.0.14 upgrade
8. 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
9. 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 labeled “updating appliance software” for ACM upgrade instructions
    d. Follow the instructions to apply the ACM 6.36.0.14 upgrade
    e. Wait for the system to reboot
    f. After upgrade is complete, login to open ACM 6.36.0.14
    g. If the default password has never been changed, there will be a one-time prompt to change your default password.

ACM Virtual Appliance

VMware

- Using ACM Virtual Appliance ACM_VM_6.36.0.14.ova in ACM_VM_VMware_6.36.0.14.zip requires a minimum of vSphere version 6.5

Hyper-V

- Using ACM Virtual Appliance ACM_VM_Hyper-V_6.36.0.14.zip requires a minimum of Windows Hyper-V Generation2 (Windows 10/Server v1809; Hyper-V Server 2019)

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

1. For the ACM 6.36.0.14 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
2. For the ACM 6.36.0.14 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 6.36.0.14 and save to secure location.
2. For the ACM 6.36.0.14 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.36.0.14 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 6.36.0.14 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 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

1. **Support for Schlage ControlBM wireless lock**
    - Feature parity with Control(B) lock
    - ⚠ Schlage Gateway should be updated to version 1.62.04 or newer prior to connecting a ControlBM lock
2. **Support for Schlage Wi-Fi Locks with Custom Certificates**
3. **ACM Expedite** - new features
    - **Real-time door status**
      Browse to any door to view its state and status (when known). Also, the door transactions preview now refreshes automatically
    - **Dark mode**
      The app follows the device appearance mode
    - **Search in lists**
      Use the search bar to quickly find a door or a global action
4. **Duplicating of roles, delegations, and access groups**
    - Duplicate an existing role, delegation, or access group to create a new instance that is similar to the existing one
5. **Download log files** directly from the ACM UI (Setup & Settings > Appliance > Logs) or with the new REST command
6. Stability, security & performance improvements

Fixed Issues

- Corrected issue where LDAP collaborations skip identities with blank or complex email address
- Corrected issue when filtering the list of identities with the same field multiple times ignores all but the last filter criteria

- Corrected issue where Schlage Wi-Fi locks fail to connect to ACM when custom SSL certificate is added to ACM
- Corrected issue where barcodes on badge preview are not displayed correctly
- Corrected issue where help page is inaccessible
- Corrected issue where large format card format (more than 128 bits) cannot be saved
- Corrected issue where schedules with more than 32 Characters are not downloaded to Salto
- Corrected issue when filtering the token report using Date fields returns inaccurate results due to a difference between displayed local time and stored UTC time
- Corrected issue where the access tab is inaccessible when an identity plasecName is blank
- Corrected issue where HID Origo tokens become inaccessible after HID Origo connection has been deleted.
- Corrected issue where creating a backup with a REST call returns a 500 response after the backup has been successfully created
- Corrected issue where DMP-related events don't include the DMP panel name
- Corrected issue where the REST command to retrieve the details of a group (/groups/<group-cn>.xml) returns an error
- Corrected issue where DMP entities status is not refreshed after the panel goes offline
- Corrected issue where the roles tab displays parent roles that are in another partition than the operator
- Corrected issue where users with special characters in their names are not downloaded from DMP panels
- Corrected issue where "DMP" global actions (DMP intrusion Area, DMP intrusion Zone, DMP intrusion Panel, DMP intrusion output) members are not displayed in ACM Expedite.
- Corrected issue where updating DMP panel properties via REST commands uninstalls the panel

ACM Known Issues

- Issue: DMP Users permissions are not honored when commands are triggered via global linkages

  Description: All commands that ACM issues to DMP panels are using the same DMP user (admin) account: ‘remoteuser’. The rights and privileges of ‘remoteuser’ cannot be edited in ACM nor in DMP.

  Affected Version: ACM 6.34

Workaround: None available.

Status: The issue is being investigated.

- Issue: DMP standalone zones (zones not linked to an area) are not listed in ACM

  Description: DMP Zones can be linked or not to DMP areas at creation/configuration time. ACM only lists the DMP zones that are linked to an area, the other ones are missing.

  Affected Version: ACM 6.34

  Workaround: None available.

  Status: Scheduled to be corrected in a future release.

- Issue: Aperio AH40 Hub can connect to 32 doors maximum

  Description: ACM prevents adding doors to an Aperio AH40 Hub when 32 doors have already been assigned to this hub.

  Affected Version: ACM 6.26 and newer

  Workaround: None available.

  Status: The issue is being investigated.

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-1-30-3-0668.crc
  - LP1502-VER-1-30-3-0668.crc
  - LP2500-VER-1-30-3-0668.crc
  - LP4502-VER-1-30-3-0668.crc
  - LP4502SBD_BootCodeUpdater_Pkg_00_01_10_#10.crc
  - M5IC-VER-1-27-5.crc
  - M5IC-VER-1-29-2-0635.crc
  - MI-RS4-VER-1-29-1-0633.crc
  - MSICS-VER-1-27-5.crc
  - MSICS-VER-1-29-1-0633.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-1-57-12.aax
  - M5-2K_APPL-VER-1-57-6.aax
  - m5-2k_appl_1_58_4.aax
  - M5-2RP-APPL-VER-1-57-12.aax
  - M5-2RP-APPL-VER-1-58-6.aax
  - m5-2rp_appl_1_59_0.aax
  - M5-2SRP-APPL-VER-1-57-12.aax
  - M5-2SRP-APPL-VER-1-58-6.aax
  - m5-2srp_appl_1_59_0.aax
  - M5-8RP-APPL-VER-1-57-15.aax
  - M5-8RP-APPL-VER-1-57-9.aax
  - m5-8rp_appl_1_58_4.aax
  - MI-RS4-APPL-VER-1-57-6.aax
  - MR16IN-APPL-VER-3-20-4.aax
  - MR16IN-APPL-VER-3-21-12.aax
  - MR16IN-SER2-APPL-VER-1-32-2.aax
  - MR16OUT-APPL-VER-3-21-12.aax
  - MR16OUT-SER2-APPL-VER-1-32-2.aax
  - MR50-APPL-VER-3-20-4.aax
  - MR50-APPL-VER-3-21-12.aax
  - MR50-SER2-APPL-VER-1-53-15.aax
  - MR50-SER2-APPL-VER-1-54-4.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-3-21-12.aax
  - MR52-S3B-3-22-2-ENC.aax
  - MR52-S3B-3-22-3-ENC.aax
  - MR52-SER1-APPL-VER-1-11.aax
  - MR52-SER2-APPL-VER-1-58-11.aax

- MR52-SER2-APPL-VER-1-59.0.aax
- MR62E-APPL-VER-3-21-12.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