Access Control Manager™ 6.28.0.13 Release Notes

Version 6.28.0.13 – Released Tuesday, February 15, 2021

Files Released

Access Control Manager Physical Appliance Files

- ACM-6.28.0.13-20220212-115505.upgrade

Access Control Manager Virtual Appliance Files

- ACM_VM_VMware_6.28.0.13.zip
- ACM_VM_Hyper-V_6.28.0.13.zip

Note

The upgrade to ACM 6.28.0.13 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 6.28.0.13 is not compatible with previous versions 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 6.28.0.13 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. 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 6.28.0.13 from ACM 6.0.0. The system must first be upgraded to ACM 6.2.0 then to 6.22.0. Please refer to the 6.28.0.13 upgrade release notes for further information.
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. 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.

Note: The upgrade to ACM 6.28.0.13 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, it will take about 2 hours more than usual.

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 6.28.0.13)
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 6.28.0.13 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 the Appliance Software” for ACM upgrade instructions
    d. Follow the instructions to apply the ACM 6.28.0.13 upgrade
    e. Wait for the system to reboot
    f. After upgrade is complete, login to open ACM 6.28.0.13
    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

- Importing ACM Virtual Appliance ACM_VM_VMware_6.28.0.13.ova requires a minimum of vSphere version 6.5

Hyper-V

- Importing ACM Virtual Appliance ACM_VM_Hyper-V_6.28.0.13.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 6.28.0.13 upgrade on a replicated system, the recommendation is to use the Admin account only to perform the upgrade.
2. For the ACM 6.28.0.13 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 6.28.0.13 and save to secure location.
2. For the ACM 6.28.0.13 upgrade on a replicated system, the recommendation is to use the Admin account only to perform the upgrade.
3. For the ACM 6.28.0.13 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 6.28.0.13 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

    <u>NOTE</u>: 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. The Avigilon logo on the ACM login screen and header has changed to Motorola Solutions
2. ACM is now able to communicate with up to 1,024 controllers (from 1,000)
3. Improved error handling for HID Origo integration
4. Stability & performance improvements

Fixed Issues

- Corrected an issue when setting the expiration date of a token to a date greater than January 19, 2038 is causing an overflow in the transactions database.
- Corrected issue preventing the editing of job specifications.
- Corrected issue preventing the editing of identities when their email address contains an underscore.
- Corrected issue when deleting an identity with HID Origo tokens using "Destroy batch" in ACM doesn't delete the associated user in the HID Origo platform.
- Corrected issue where a policy that has been deleted or uninstalled is still applied to previously impacted objects (groups, doors, etc.).
- Corrected issue preventing selecting some doors in the token screen to give 1 free pass.
- Corrected issue where the Areas Identity Report doesn’t show if the identity running the report and the area are in a different partition.
- Corrected issue where the content of a user-defined field is reset (blank) when filled in at the same time as creating an identity.
- Corrected issue where the rest call to execute a collaboration fails to return a valid response after it has successfully run.

ACM Known Issues

- Issue: ACM-ACC Unification performance

  Description: ACM-ACC unification may experience performance issues when connecting a large number of ACC sites to a single ACM with many objects.

  Affected Version: ACM 6.22.0 & ACC 7.14.4 and greater

  Workaround: Connect with your Sales Engineer to better understand expectations and optimize your configuration for best results.

Fix: Scheduled to be corrected in a future release.

- Issue: Soft APB notifications do not report within ACM transactions when using Mercury Security firmware v1.30.0.0662.

  Description: Soft APB events are not reported from Mercury Security LP controllers to ACM with firmware v1.30.0.0662. Hard APB and Timed APB are not affected.
  Also, note that firmware v1.30.0.0662 is for LP controllers only (not compatible with EP controllers).

  Affected Version: Mercury Controller Firmware v1.30.0.0662

  Workaround: Customers using soft APB should NOT upgrade their Mercury Security LP controllers firmware to 1.30.0.0662.

  Fix: Mercury resolved this issue in firmware 1.30.1 but it has not been tested with ACM yet. Scheduled to be integrated and tested in the next release of ACM.

- Issue: Identities with HID Origo tokens deleted in ACM are not deleted from the HID Origo server after the maximum number of users deleted per day threshold has been exceeded.

  Description: A customizable threshold in HID Origo defines the maximum number of users that can be deleted per day. When the number of identities with HID Origo tokens deleted in ACM exceeds this threshold, ACM is unable to delete the corresponding users in HID Origo. Identities are deleted from ACM, but remain unchanged in HID Origo, leaving orphaned users in HID Origo. In addition, it won't be possible to enroll previously deleted identities again (using the same email address) in HID Origo from ACM.

  Workaround: The threshold can be set to a large value to decrease the risk of exceeding it. If the threshold is reached, orphaned users in HID Origo will have to be deleted manually.

  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-1-29-4-0647.crc
- LP1501_1_30_0_0662_FS_2_23.crc
- LP1502-VER-1-29-4-0647.crc
- LP1502_1_30_0_0662_FS_2_23.crc
- LP2500-VER-1-29-4-0647.crc
- LP2500_1_30_0_0662_FS_2_23.crc
- LP4502-VER-1-29-4-0647.crc
- LP4502B_1_30_0_0662_FS_2_23.crc
- M5IC-VER-1-27-5.crc
- m5ic_1_29_2_0635.crc
- ms-ics_1_29_1_0633.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-1-57-12.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
  - mi-rs4_1_29_1_0633.crc

- 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
- mr16in_3_21_12_enc.aax
- MR16OUT-APPL-VER-3-21-10.aax
- MR16OUT-SER2-APPL-VER-1-32-2.aax
- MR16OUT-SER3-APPL-VER-3-21-0.aax
- mr16out_3_21_12_enc.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_3_21_12_enc.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
- mr52_3_21_12_enc.aax
- MR62E-SER3-APPL-VER-3-21-10.aax
- mr62e_3_21_12_enc.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