

Access Control Manager™ 6.26.0.32 Release Notes

Version 6.26.0.32 – Released Monday, December 6, 2021

Files Released

Avigilon Access Control Manager Physical Appliance Files

- ACM-6.26.0.32-20211202-051402.upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_Hyper-V_6.26.0.32.zip
- ACM_VM_VMware_6.26.0.32.zip

Upgrade Path

NOTE: ACM 6.26.0.32 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 6.26.0.32 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 6.26.0.32 from ACM 6.0.0. The system must first be upgraded to ACM 6.2.0 then to 6.22.0.
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

- 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 6.26.0.32)
- 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 6.26.0.32 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 6.26.0.32 upgrade
 - Wait for the system to reboot
 - After upgrade is complete, login to open ACM 6.26.0.32
 - 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_6.26.0.32.ova requires a minimum of vSphere version 6.5

Hyper-V

- Importing ACM Virtual Appliance ACM_VM_Hyper-V_6.26.0.32.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 6.26.0.32 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
2. For the ACM 6.26.0.32 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 6.26.0.32 and save to secure location.
2. For the ACM 6.26.0.32 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.26.0.32 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 6.26.0.32 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

- Adding support for ASSA ABLOY Aperio Gen5 AH20 and AH40 hubs
 - Connect up to 64 Aperio wireless locks and devices to Mercury hardware via IP/ethernet on a single AH40 hub. Note that the AH40 is supported with the following Mercury Security Intelligent controllers: LP1501, LP1502, and LP2500. Support for LP4502 will be added in a future release.
 - Requires Mercury controllers to run 1.30.0.662 firmware or later
- Adding support for Schlage LEB & NDEB locks in RS-485 Gateway mode
 - In RS-485 mode, the ENGAGE gateway is connected to Mercury controller or subpanel via RS-485

- Requires Mercury controllers to run 1.30.0.662 firmware or later
- Integration with HID ORIGO Credential Management (requires HID Origo account)
 - Administrators can now save more time and effort with the ability to issue mobile credentials directly from the ACM system.

Fixed Issues

- Performance & security improvements
- Corrected issue when using Nimbus Sans L font in the badge designer displays incorrect characters.
- Corrected issue when pressing 'ENTER' while defining a user-defined list clears the entire list.
- Corrected issue when ACM is showing a door online after it has been deleted from SALTO Pro Access Space.
- Corrected issue where the "normal forced door" event is not displayed in the event monitor page when an ASSA ABLOY IP-enabled door returns to its normal state after it has been forced.
- Corrected issue when incorrect events are displayed in the event monitor when a custom schedule, setting the door to unlock mode becomes active for Schlage wireless locks connected in IP-Gateway mode.
- Corrected issue when operators are logged out of ACM Verify Virtual Station when pairing a device.
- Corrected issue where global actions were missing in ACM Expedite.

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: Soft APB doesn't work with 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 is aware of the issue and is working on a fix.

- 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

- o M5IC-VER-1-27-5.crc
- o m5ic_1_29_2_0635.crc
- o ms-ics_1_29_1_0633.crc
- o MSICS-VER-1-27-5.crc
- o pivCLASS-Embedded-Auth-Removal_Pkg_01_00_00_#14.crc
- o pivCLASS-Embedded-Auth_Pkg_05_10_27_#145.crc
- o Scp2-AES-VER-3-120.crc
- o 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
- o

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-1-57-12.aax
 - o M5-2K_APPL-VER-1-57-6.aax
 - o m5-2k_appl_1_58_4.aax
 - o M5-2RP-APPL-VER-1-57-12.aax
 - o M5-2RP-APPL-VER-1-58-6.aax
 - o m5-2rp_appl_1_59_0.aax
 - o M5-2SRP-APPL-VER-1-57-12.aax
 - o M5-2SRP-APPL-VER-1-58-6.aax
 - o m5-2srp_appl_1_59_0.aax
 - o M5-8RP-APPL-VER-1-57-15.aax
 - o M5-8RP-APPL-VER-1-57-9.aax
 - o m5-8rp_appl_1_58_4.aax
 - o MI-RS4-APPL-VER-1-57-6.aax
 - o mi-rs4_1_29_1_0633.crc
 - o MR16IN-APPL-VER-3-20-4.aax
 - o MR16IN-APPL-VER-3-21-10.aax
 - o MR16IN-SER2-APPL-VER-1-32-2.aax
 - o MR16IN-SER3-APPL-VER-3-21-0.aax
 - o mr16in_3_21_12_enc.aax
 - o MR16OUT-APPL-VER-3-21-10.aax
 - o MR16OUT-SER2-APPL-VER-1-32-2.aax
 - o MR16OUT-SER3-APPL-VER-3-21-0.aax
 - o mr16out_3_21_12_enc.aax
 - o MR50-APPL-VER-3-20-4.aax
 - o MR50-APPL-VER-3-21-10.aax

- o MR50-SER2-APPL-VER-1-53-15.aax
- o MR50-SER2-APPL-VER-1-54-4.aax
- o mr50_3_21_12_enc.aax
- o MR51E-SER2-APPL-VER-1-8-14.aax
- o MR51E-SER2-APPL-VER-1-8-4.aax
- o MR52-APPL-VER-3-20-4.aax
- o MR52-APPL-VER-3-21-10.aax
- o MR52-SER1-APPL-VER-1-11.aax
- o MR52-SER2-APPL-VER-1-58-11.aax
- o MR52-SER2-APPL-VER-1-59.0.aax
- o MR52-SER3-APPL-VER-3-21-0.aax
- o mr52_3_21_12_enc.aax
- o MR62E-SER3-APPL-VER-3-21-10.aax
- o mr62e_3_21_12_enc.aax
- o MRDT-APPL-VER-1-63-0.aax
- o MRDT-APPL-VER-1-63-4.aax
- o MRDT-APPL-VER-1-63-8.aax
- o MS-ACS-APPL-VER-1-0-5.aax
- o MS-ACS-APPL-VER-1-0-6.aax
- o MS-ACS-APPL-VER-1-00-10.aax
- o MS-I8S-APPL-VER-1-0-1.aax
- o MS-R8S-APPL-VER-1-0-2.aax
- o MS-R8S_APPL-VER-1-0-1.aax