

Access Control Manager™ 6.30.0.18 Release Notes

Version 6.30.0.18 – Released Sunday, March 13, 2022

Files Released

Access Control Manager Physical Appliance Files

- ACM-6.30.0.18-20220310-000858.upgrade

Access Control Manager Virtual Appliance Files

- ACM_VM_VMware_6.30.0.18.zip
- ACM_VM_Hyper-V_6.30.0.18.zip

Note

HID Mercury LP controller firmware 1.30.2 that is included in ACM 6.30 contains critical security fixes.

We strongly recommend that all LP controllers are updated to this version in a timely manner.

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 6.30.0.18 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 6.30.0.18 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 6.30.0.18 from ACM 6.0.0. The system must first be upgraded to ACM 6.2.0 then to 6.22.0 and finally to 6.30.0.18.
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.

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 6.30.0.18)
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 6.30.0.18 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 6.30.0.18 upgrade
 - e. Wait for the system to reboot
 - f. After upgrade is complete, login to open ACM 6.30.0.18
 - 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_6.30.0.18.ova requires a minimum of vSphere version 6.5

Hyper-V

- Importing ACM Virtual Appliance ACM_VM_Hyper-V_6.30.0.18.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 6.30.0.18 upgrade on a replicated system, Motorola Solutions recommends using the Admin account only to perform the upgrade.
2. For the ACM 6.30.0.18 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 6.30.0.18 and save to secure location.
2. For the ACM 6.30.0.18 upgrade on a replicated system, Motorola Solutions recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.30.0.18 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 6.30.0.18 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

1. New REST commands for canned macros
 - New REST call for canned macros by either door or input DN.
 - New REST call to get the details of a canned macro by its DN.
2. Dynamic Host Configuration Protocol DHCP (new installations only)
 - DHCP is only supported on port 1 and is enabled by default. The appliance gets its IP address from the DHCP server and the IP is displayed in the console when the appliance boots.
3. New with ACM 6.30.0.18 for ACM Expedite 1.4
 - View & control doors: easily grant access or review transactions of a door
 - Favorites: pin global actions or doors at the top of the list
 - Landscape mode (screen rotation) and support for tablets
 - Simplified navigation pattern (cards design)
 - Improved error handling
 - Motorola Solutions branded
4. Stability & performance improvements

Fixed Issues

- An error message is displayed when the user enters invalid credentials to connect to a SALTO server from the external systems page.
- Correct issue rest/identities.xml returns an inconsistent number of results.
- Corrected issue preventing assigning a profile to an identity after one of the roles linked to the profile has been deleted.
- Corrected issue when changes made to user-defined fields from ACM are not saved.
- Corrected issue where a door, set to a non-default mode by a priority global action, returns to default mode after a command triggers a download to the panel the door is connected to.
- Corrected issue where card swipes no longer generate events in ACM after a panel has been changed from LP1501 with downstream to no downstream.
- Corrected issue where downloading an identity with HID Origo tokens to all connected panels generates an error.
- Corrected issue where roles are removed from identities when the SQL collaboration has been interrupted in the middle of processing.

- Corrected issue where soft APB notifications do not report within ACM transactions. Requires Mercury Security firmware v1.30.2.0665 or later.
- Corrected issue where the monitor dashboard goes to an endless loop when schedule name contains a quote or a single quote.

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: Anything prior to ACM 6.30 & ACC 7.14.8

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

Status: Significant performance improvements with ACC 7.14.8 & ACM 6.30. See [ACC™ and ACM™ Unification Guide](#) for more details.

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-1-29-6-0654.crc
 - LP1501-VER-1-30-2-0665.crc
 - LP1502-VER-1-29-6-0654.crc
 - LP1502-VER-1-30-2-0665.crc
 - LP2500-VER-1-29-6-0654.crc
 - LP2500-VER-1-30-2-0665.crc
 - LP4500-VER-1-29-7-0658.crc
 - LP4500-VER-1-30-2-0665.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

- o MSICS-VER-1-27-5.crc
- o MSICS-VER-1-29-1-0633.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

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 MR16IN-APPL-VER-3-20-4.aax
 - o MR16IN-APPL-VER-3-21-12.aax
 - o MR16IN-SER2-APPL-VER-1-32-2.aax
 - o MR16OUT-APPL-VER-3-21-12.aax
 - o MR16OUT-SER2-APPL-VER-1-32-2.aax
 - o MR50-APPL-VER-3-20-4.aax
 - o MR50-APPL-VER-3-21-12.aax
 - o MR50-SER2-APPL-VER-1-53-15.aax
 - o MR50-SER2-APPL-VER-1-54-4.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-3-21-12.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 MR62E-APPL-VER-3-21-12.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