Avigilon Unity Access (formerly Access Control Manager) **6.42.4.5 Release Notes**

Version 6.42.4.5 – Released May 9, 2023

Files Released

Access Control Manager Physical Appliance Files

- ACM-6.42.4.5-20230505-020349.upgrade

Access Control Manager Virtual Appliance Files

- ACM_VM_VMware_6.42.4.5.zip
- ACM_VM_Hyper-V_6.42.4.5.zip

Upgrade Path

ACM can be upgraded to ACM 6.42.4.5 directly from ACM 6.20.0.20 or newer.
Please refer to the ACM 6 Upgrade Path and ACM 5 Upgrade Path articles for further information.

WARNING: ACM Software can only be upgraded to a higher version. Attempts to downgrade will be blocked or potentially cause loss of data.

NOTE: ACM6.42.4.5 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.

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 6.42.4.5)

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 6.42.4.5 upgrade
8. Identity account may require the inactivity timer set to its maximum value for extended upgrade times to observe status without requiring to log in and observe logs under the 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 6.42.4.5 upgrade
    e. Wait for the system to reboot
    f. After the upgrade is complete, log in to open ACM 6.42.4.5
    g. If the default password has never been changed, there will be a one-time prompt to change your default password.

ACC / ACM Unification

1. With ACM 6.30 new delegations were added to support new REST routes. These REST routes are required for ACC / ACM Unification starting in ACC 7.14.8 with ACM 6.30.
2. If the ACM User used to connect ACM to ACC is a custom role, the role must be changed to support the new REST delegations. Refer to the ACC/ACM Unification Guide for further information.

ACM Virtual Appliance

VMware

- Using ACM Virtual Appliance ACM_VM_6.42.4.5.ova in ACM_VM_VMware_6.42.4.5.zip requires a minimum of vSphere version 6.5

Hyper-V

- Using ACM Virtual Appliance ACM_VM_Hyper-V_6.42.4.5.zip requires a minimum of 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 6.42.4.5 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
2. For the ACM 6.42.4.5 upgrade on a peer-to-peer replicated system, disable the replication on all appliances.
3. Apply the software upgrade to all appliances 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 6.42.4.5 and save it to a secure location.
2. For the ACM 6.42.4.5 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM6.42.4.5 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 6.42.4.5 and save it to a secure location.

2. Appliances 1 and 2 are peer-to-peer; appliances 3 and 4 are failover appliances monitoring 1 and 2 respectively.
3. On appliances 3 and 4, navigate to the appliance replication page, and click on take over button on appliances 3, and 4. Make sure that appliances 3, and 4 take over the control from appliances 1, and 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 the upgrade file to appliances 1 and 2. Apply the upgrade files on 1 and 2
6. Wait till the upgrade finishes successfully on appliances 1 and 2. Accept the EULA.
7. Navigate to appliances 3 and 4's appliance replication tab, and click on the failback button on appliances 3,4. Ensure appliances 1, and 2 take the control back successfully (First try might not succeed, try multiple times). Observe that panels are online on appliance 1
8. Upload the upgrade file to appliances 3 and 4. Apply the upgrade files on 3, 4
9. Wait till the upgrade finishes successfully on appliances 3 and 4. Accept the EULA.
10. Navigate to the appliance replication page on each appliance, 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 updating the Hot Standby last.

Changes - ACM 6.42.0.11

New Features

- **Map refresh** – Map icons have been redesigned to be sharper, scalable, and easily visible on any background. These icons can also be resized to fit specific needs, with four different sizes available.
- **Multifactor authentication (TOTP)** – Operators may configure a second authentication factor to their account for logging into ACM for additional security.
- **Review and update the tokens' status in the mobile app**
- **Stability, security & performance improvements**

Fixed Issues

- Corrected issue where the aspect ratio of photos taken with a mobile device appears distorted in the badge.

- Corrected issue where user-defined fields of type 'boolean' cannot be set to 'false' using identity profiles.
- Corrected issue where user-defined fields labels don't show in the identity page.
- Corrected issue where tokens timestamps are one hour ahead for time zones that do not use DST.
- Corrected issue where tabbing through the Identity fields automatically selects values.
- Corrected issue where REST calls for creating Virdi, Salto, and HID Origo external systems return status 200 instead of 201.
- Corrected issue when a delegation error prevents the user from logging in a freshly imaged ACM.
- Corrected issue where the Audit log is flooded with Pwdlastsuccess timestamps.
- Corrected issue where Schlage ControlBM lock is missing from the Battery Level report.
- Corrected issue in ACM Expedite where tapping "View more" on the 'roles' card in the identity details screen displays the transactions history.
- Corrected issue where objects' status in Door list and Maps pages are not updating properly.
- Corrected issue where no event is logged in ACM when a door grant is issued from ACC.
- Corrected multiple issues with our Integration with ASSA ABLOY DSR:
    - Blank card format showing in the door member list after adding or deleting a card format.
    - Toggling token status from inactive to active generates duplicate identities. (error 500).
    - ACM is aborting the syncing of a large number of doors with ASSA ABLOY DSR (Door Service Router).

Changes - ACM 6.42.2.7

New Features

- **SQL Connection encryption** - ACM automatically attempts to use TLS to secure communications with SQL server for Identity SQL Server pull collaboration; it is recommended to enable TLS in the SQL Server configuration. ACM uses TDS protocol 7.2; use of SQL Server 2005 or newer is required.
- **Stability, security & performance improvements**

Fixed Issues

- Corrected multiple issues with our Integration with ASSA ABLOY DSR:
    - Corrected issue related to ASSA ABLOY Wi-Fi locks going offline and not syncing with ACM due to time zone misconfiguration.
    - Corrected issue when using facility codes outside of the 0-255 range in card formats, caused Assa doors to sync repetitively, leading to quick battery depletion.
- Corrected issue when sending 'Regenerate Access Levels' command, sent access information to the doors that are inconsistent with configured access groups.
- Corrected issue where the operator name was not captured when a manual door grant event in ACC is generated.
- Corrected issue where the door information was missing from the transactions card in the Identity details screen in the mobile application.
- Corrected issue when deselecting the "Multifactor Authentication" checkbox on an identity page that generated an error.

Changes - ACM 6.42.4.5

Fixed Issues

- Corrected an issue where using user-defined fields on a replicated system can result in an incomplete replication and/or incomplete backup recovery.

Firmware Included

HID MERCURY LP INTELLIGENT CONTROLLERS FIRMWARE AVAILABLE

HID Global reported cybersecurity vulnerabilities within firmware running on all Mercury LP Intelligent Controllers prior to version v.1.30.3.
HID Global addressed and validated all issues reported v.1.30.3.

We recommend upgrading all panels to the latest available firmware version.

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-1-30-4-0671.crc
- LP1501-VER-1-30-5-0674.crc
- LP1502-VER-1-30-4-0671.crc
- LP1502-VER-1-30-5-0674.crc
- LP2500-VER-1-30-4-0671.crc
- LP2500-VER-1-30-5-0674.crc
- LP4502-VER-1-30-4-0671.crc
- LP4502B-VER-1-30-5-0674.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-3-21-12.aax
- MR16IN-APPL-VER-3-22-4.aax
- MR16IN-SER2-APPL-VER-1-32-2.aax
- MR16OUT-APPL-VER-3-21-12.aax
- MR16OUT-APPL-VER-3-22-4.aax
- MR16OUT-SER2-APPL-VER-1-32-2.aax
- MR50-SER2-APPL-VER-1-53-15.aax
- MR50-SER2-APPL-VER-1-54-4.aax
- MR50-SER3-APPL-VER-3-21-12.aax
- MR50-SER3-APPL-VER-3-22-4.aax
- MR51E-SER2-APPL-VER-1-8-14.aax
- MR51E-SER2-APPL-VER-1-8-4.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-3-21-12.aax
- MR52-SER3-APPL-VER-3-22-4.aax
- MR52-SER3B-APPL-VER-3-22-4.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