Avigilon Unity Access (formerly Access Control Manager) **6.44.4.1 Release Notes**

Version 6.44.4.1 – Released Jul 14, 2023

Security and stability improvement updates are included with the latest version of Avigilon Unity Access.

Files Released

Access Control Manager Physical Appliance Files

- ACM-6.44.4.1-20230619-220155.upgrade

Access Control Manager Virtual Appliance Files

- ACM_VM_VMware_6.44.4.1 .zip
- ACM_VM_Hyper-V_6.44.4.1 .zip

Upgrade Path

ACM can be upgraded to ACM 6.44.4.1 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.

NOTE: ACM 6.44.4.1 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 through 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 6.44.4.1)

3. Upgrades are supported on ACM Professional (Dell OptiPlex XE2, XE3, XE4) 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 6.44.4.1 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 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 6.44.4.1 upgrade
    e. Wait for the system to reboot
    f. After upgrade is complete, login to open ACM 6.44.4.1
    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_6.44.4.1.ova in ACM_VM_VMware_6.44.4.1.zip requires a minimum of vSphere version 6.5

Hyper-V

- Using ACM Virtual Appliance ACM_VM_Hyper-V_6.44.4.1.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 6.44.4.1 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
2. For the ACM 6.44.4.1 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 6.44.4.1 and save to secure location.
2. For the ACM 6.44.4.1 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.44.4.1 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 6.44.4.1 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 the 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 - 6.44.0.17

New Features

1. **Alarm Sounds** - Upload your own sounds for personalized notifications of events
2. Various performance and stability improvements for the integration with ASSA ABLOY Door Service Router (DSR)
3. **Battery Level Report** - The Battery Level report now includes Schlage AD-400, and ASSA ABLOY Aperio locks
4. **ViRDI Enhancements** - Virdi tokens can now be deleted from UNIS directly from within ACM
5. **Stability, security & performance improvements**

Fixed Issues

- Corrected issue where multiple identical events are generated with Schlage IP-Mode locks.
- Corrected an issue where tokens that do not follow the card format constraints get downloaded into ASSA ABLOY DSR and cause various issues.

- Corrected an issue where emails could not be sent to email addresses that contain a dash/hyphen.
- Corrected an issue where ASSA ABLOY DSR access information is out of sync after implementing timed access, causing unsuccessful grant access to valid users.
- Corrected issue when identities with special characters are not imported via CSV collaboration.
- Corrected an issue where door grant events were incorrect after failover, affecting multiple functions such as APB (anti-passback).
- Corrected an issue when using User-Defined fields of type boolean to search for identities does not return correct results.
- Corrected issue where the CPU load increases and the maximum number of transactions stored exceed the defined threshold.
- Corrected issue where restoring a backup file fails because of an ""invalid backup path"" error.
- Corrected issue when the door list in the dashboard page doesn't match the active filter.
- Corrected an issue where no event is generated when crossing disk space thresholds
- Corrected issue when importing identities with a CSV collaboration fails when the file contains UDF (user-defined fields) of type textbox.
- Corrected issue when doors remain offline after the subpanel they are connected to gets installed and communicates properly.
- Corrected issue where commands sent to SALTO locks from ACM are delayed.
- Corrected issue when ACM doesn't initiate communication with Schlage wireless locks in WiFi mode.
- Corrected issue when connecting 1,024 or more SALTO locks to ACM causes ACM to display incorrect door status and high CPU usage.
- Corrected issue when doors remain offline after the subpanel they are connected to gets installed and communicates properly.

Changes - 6.44.2.4

Fixed Issues

- Corrected issue where commands sent to SALTO locks from ACM are delayed.
- Corrected issue when ACM doesn't initiate communication with Schlage wireless locks in WiFi mode.
- Corrected issue when connecting 1,024 or more SALTO locks to ACM causes ACM to display incorrect door status and high CPU usage.

Changes - 6.44.4.1

Fixed Issues

- Stability, security improvements

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