Access Control Manager™ 6.14.0.12 Release Notes

Version 6.14.0.12 – Released Tuesday, December 8, 2020

Files Released

Avigilon Access Control Manager Physical Appliance Files

- ACM-6.14.0.12-20201204-013520.upgrade

Avigilon Access Control Manager Virtual Appliance Files

- ACM_VM_6.14.0.12.zip

Upgrade Path

1. Always perform a configuration and transactions backup of the current version prior to any upgrade and save to secure location.
2. There is no direct upgrade path to ACM 6.14.0.12 from revisions prior to ACM 6.0.0.XX. The system must first be upgraded to ACM 6.0.0.XX and then to 6.14.0.12. Please refer to the 6.14.0.12 upgrade release notes for further information.
3. 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.
4. 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.
5. 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.
6. Please refer to the upgrade release notes for further information.
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 and save to a secure location

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 6.14.0.12)
3. Upgrades are supported on ACM Professional (Dell OptiPlex XE2, XE3) ACM Enterprise (Dell PowerEdge R210, R220, R230, R240 and MBX) 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 VMWare host prior to performing ACM 6.14.0.12 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 labelled “updating appliance software” for ACM upgrade instructions
    d. Follow the instructions to apply the ACM 6.14.0.12 upgrade
    e. Wait for the system to reboot
    f. After upgrade is complete, login to open ACM 6.14.0.12
    g. If the default password has never been changed, there will be a one-time prompt to change your default password.
10. Optional: If any changes to current licensing needs to be made, see section "ACM License Upgrade Instructions (6.14.0.12)"
11. We recommend that you perform a reset/download for all HID panels and sub-panels after upgrade is complete.

ACM Virtual Appliance

➢ Importing ACM Virtual Appliance ACM_VM_6.14.0.12.ova requires a minimum of **vSphere version 6.5**

ACM with ACC Integration Upgrade Instructions

➢ NOTE: Previous versions to 6.14.4.6 of AvigilonAcmIntegrations are not compatible with ACM 6.14.0.12. Avigilon recommends upgrading existing ACM/ACC integrations to current versions of ACM and ACC.

➢ Instructions for installing AvigilonAcmIntegration-6.14.4.6.exe
    a. Download AvigilonAcmIntegration- 6.14.4.6 from https://www.avigilon.com/software-downloads/
    b. Make a backup copy of Avigilon\ACM to ACC Integration\ACM to ACC Alarm Gateway\AlarmConfig.xml
    c. Uninstall previous version of the AvigilonAcmIntegration

d. Reboot the appliance (ACC) that the integration was installed on
e. Install the AvigilonAcmIntegration-6.14.4.6
f. Ensure Vidproxy service is running
g. Login to the upgraded 6.14.0.12 appliance. Navigate to Settings/External Systems, select the Avigilon tab; select the appropriate ACC Integration IP link from the list (may be more than one). Click on the Save button to reinitialize the handshake between ACM and ACC. Wait until the "Avigilon Server was successfully updated" prompt is presented and camera status for each camera shows display of "Online". Verify camera streaming

ACM with replication Upgrade Instructions for Peer-to-Peer (2 or more appliances without Hot Standby)

1. Perform a configuration and transactions backup of ACM and save to a secure location.
2. For the ACM 6.14.0.12 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.14.0.12 upgrade on a peer-to-peer replicated system, disable the replication on all appliances.
4. Apply the software upgrade to all appliances in any order.
5. Allow the upgrade on all appliances to complete and the appliances to reboot and come back online.
6. Accept the EULA for all appliances.
7. 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 and save to a secure location.
2. For the ACM 6.14.0.12 upgrade on a replicated system, Avigilon recommends using the Admin account only to perform the upgrade.
3. For the ACM 6.14.0.12 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 Auto Failover

1. Perform a configuration and transactions backup of ACM and save to a 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 the upgrades finish successfully on appliance 1 and 2. Accept the EULA's.
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 takes the control back successfully (If the first try does 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 the upgrades finish successfully on appliance 3 and 4. Accept the EULA's.
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

Fixed Issues

- Corrected issue preventing operators other than the system administrator to create or upload SSL Certificate.
- Corrected issue preventing from opening identities details page when the appliance is not connected to the Internet.
- Corrected issue preventing applying a door template to a group of doors through a batch update.
- Corrected issue when panels' time is no longer in sync with the timezone because the timezone definition has been modified recently.
- Corrected issue when running the REST command "/doors/show_status.xml" doesn't return the doors' door mode.

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.

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-1-29-1-0633.crc
  - LP1501-VER-1-29-4-0647.crc
  - LP1502-VER-1-29-1-0633.crc
  - LP1502-VER-1-29-4-0647.crc
  - LP2500-VER-1-29-1-0633.crc
  - LP2500-VER-1-29-4-0647.crc
  - LP4502-VER-1-29-1-0633.crc
  - LP4502-VER-1-29-4-0647.crc
  - M5IC-VER-1-27-1.crc
  - M5IC-VER-1-27-5.crc
  - MSICS-VER-1-27-1.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-1-56-15.aax
  - M5-2K-APPL-VER-1-57-12.aax
  - M5-2K_APPL-VER-1-57-6.aax
  - M5-2RP-APPL-VER-1-57-12.aax
  - M5-2RP-APPL-VER-1-57-3.aax
  - M5-2RP-APPL-VER-1-58-6.aax
  - M5-2SRP-APPL-VER-1-57-12.aax
  - M5-2SRP-APPL-VER-1-57-3.aax
  - M5-2SRP-APPL-VER-1-58-6.aax
  - M5-8RP-APPL-VER-1-57-15.aax
  - M5-8RP-APPL-VER-1-57-5.aax
  - M5-8RP-APPL-VER-1-57-9.aax
  - MI-RS4-APPL-VER-1-57-3.aax
  - MI-RS4-APPL-VER-1-57-6.aax
  - 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
  - MR16OUT-APPL-VER-3-20-4.aax
  - MR16OUT-APPL-VER-3-21-10.aax
  - MR16OUT-SER2-APPL-VER-1-32-2.aax
  - MR16OUT-SER3-APPL-VER-3-21-0.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-SER3-APPL-VER-3-21-0.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
- MR62E-SER3-APPL-VER-3-21-0.aax
- MR62E-SER3-APPL-VER-3-21-10.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