Features with CAW 9.2
16 December 2019

New App:
- CAW Connect App

  A mobile app to grant temporary access, view audit trails, set or clear door inter-hub signals.

Software behavior change
- Improves selecting items on listing pages. Add support for Shift-click to select a range of items.

Global Preferences:
- Moves the following RFID card settings from CyberAuditWeb.properties to Global settings
  - display card ID as decimal
  - reverse bytes (for Videx RFID readers)
  - reverse parity bits for 35-bit wiegand cards
- Puts a limit on the size of FlashLock caching. 2 weeks max.
- Moves these properties file settings to people global preferences
  - obscure PIN input on people properties
  - enable PIN to set the require PIN flag for each new person
- CyberKey preferences settings for Portable link by issue number and/or Portable Links by key issue number

Manage System:
- Moves properties file setting for Vault20S obscure PIN entry to subsystem communicator preferences.
- To use the legacy CyberLink, CyberAgent PC, or CyberAgent Android programs, a checkbox must be enabled in database communicator settings in the manage section. This is necessary because these legacy products don't use the new token based authentication which will be discussed later.

Communicators:
- Automatically sets all Flex Hubs to ignore card scans when getting an update from the server. This has been a properties file setting for a number of years and a recommended setting. It enables the flex hub to finish updating people records when a card scan would interrupt it and cause it to start loading all over again.
- ValidiKey will now check with the server for programming missions and keys not cached locally. (dynamic programming)
- Web Authorizer 2 with ability to use both old and new keypads. Enhanced security using TLS 1.2 and uses token based authentication (a shared secret) instead of the serial number alone.
- The original Web Authorizer gets a firmware update to enable it to support dynamic programming for CK-Blue2, CK-AIR2, CK-Flash, CK-Plus. These gen2 CyberKeys all get a firmware update via USB Station to enable them to work with the old keypad on both the original Web Authorizer and the new Web Authorizer 2. Note: dynamic programming occurs when a key record is not found on the Web Authorizer's local cache and instead goes to the CyberAudit-Web server for programming instructions. Supports TLS 1.0.
- Redefines portable links. They are now a software application instance on a PC, Android, or iOS device rather than a piece of hardware like an IR Encoder. CyberAudit-Web issues the installed instance of CyberLink 2, CyberAudit-Link, or FlashLock Assistant, not the device. There is no longer a section called USB Stations. Instead that page just has a link to go to the portable links page. Portable link types are:
  - Android/iOS (CyberAudit-Link) – CyberAgent Android is put into this type
  - Windows (CyberLink)
  - FlashLock Assistant Android/iOS
  - FlashLock Assistant Windows PC

  ...and if enabled…
  - Legacy (IR Encoder)
  - Legacy (USB Station)
  - Legacy (USB CyberKey)
  - Legacy (IrDA port)

Operating Differences:
- Stronger CyberLink and Web Authorizer authentication – CAW server authenticates CyberLink 2 and old Web Authorizers using a shared secret or token instead of the serial number. This is a more secure method of authentication. It has this affect on operations:
    ○ Authorizers must now be added to the system exclusively by USB drive. Existing Web Authorizers must communicate with the CyberAudit-Web system within one year of the server update.
    ○ Portable links (IR Encoders, USB Stations, Android and iOS devices) may only be added to the system by issue number. Existing portable links will be kept but must communicate with CyberAudit-Web within one year of the server update.
    ○ Inserting an issued key into an unknown communicator will no longer automatically issue the portable link. However, the communicator may be automatically issued by *key issue number*, or by *mission number*. User will be prompted to update CyberLink 2 after updating to CAW 9.2.
    ○ To use the legacy CyberLink, CyberAgent PC, or CyberAgent Android programs, a checkbox must be enabled in database communicator settings in the manage section.

Reminders:
- We continue to increase the security of the system which includes the transition to CentOS 7. CAW9.2 is the first version of CAW to be compatible with 7. It is also compatible with CentOS 6. To move a system from CentOS 6 to CentOS 7 a new build is required because RedHat/CentOS doesn't support major version upgrades.
- End of maintenance for CAW 9.0 will occur May/June 2020. We recommend hosting resellers maintain their servers at the latest version and to encourage their self-hosting customers to do the same.