Legacy (RedCloud) Security Management Software 4.2 Release Notes

---

General Availability – Oct 5th, 2013

The following Legacy (RedCloud) Security Management Software 4.2 Release Notes outline the implemented features, bug fixes, and other changes associated with this release.

Compatibility

- **Web Browser Support**
  - Google Chrome 30
  - Mozilla Firefox 24
  - Internet Explorer 8, 9, 10
  - Apple Safari 5
- **Mercury Firmware - Supported Revisions**
  - EP Line of Controllers - Firmware Version 1.17.6
  - SCP Line of Controllers - Firmware Version 3.12.0
- **Exacq exacqVision Digital Video Servers**
  - Any exacqVision digital video server running Webserver 2.0 or higher
- **Pelco Endura Digital Video Servers**
  - Any Pelco Endura digital video server running version 2.5 or higher with Pelco Endura System Utilities version 2.1.2.0 and RTSP version 2.0.0-828
- **Avigilon Digital Video Servers**
  - Any Avigilon digital video server running Avigilon Control Center 4.12.0.34
- **Milestone Digital Video Servers**
  - Any Milestone digital video server running XProtect Corporate Management Server version 5.0c
- **Salient Digital Video Servers**
  - Any Salient digital video server running Version 4.1

Upgrade Path

All software updates can be downloaded from ftp.avigilon.com/ACM.

All customers must be running RedCloud Version 4.0.0 or higher in order to install Version 4.2. RedCloud recommends performing a database backup on your existing system prior to installing a new version.

Customers running on a RedCloud appliance (Enterprise, Express, or VM) with RedCloud version 4.0.0 or later can upgrade directly to 4.2 using the 4.2 software update file named **Update420-SVN10432** that can be downloaded from the FTP site.

Before installing a series of software updates, perform a complete backup of your system (including configuration and transactions).

To install a software update:

1. From your client, log in to the appliance with an Administrator level account and navigate to **Appliances** > **Software Update**.
2. Browse to the desired software update file and click the **Save** icon to upload the software update file.
3. After saving, click the green check mark icon to apply the update.

   The update process may take several minutes or longer to complete. During this time a progress log will be displayed on the page as the system processes various updates. When the upgrade process completes, the appliance will be restarted.

4. After the update process finishes and reboots the appliance, log out and back in again to your appliance and verify the upgrade completed successfully by navigating to **Appliances** > **About**. The new version information will display at the top of the page.

Additional Upgrade Instructions for Replicated/Redundant Environments:

- Before beginning the installation process, briefly test the two-way replication between the Primary and Hot Standby appliances. One way to do this is to add a 'test dummy' ID or schedule on one of the appliances and modify it on the other to ensure replication is functioning properly. Proceed to the next instruction if you see your changes reflected on both appliances. If you do not see the changes reflected on both appliances, please contact RedCloud Technical Support.
- On the Primary appliance, uncheck the 'Monitor on' flag on the **Appliance** > **Replication** page under 'Redundancy Settings' and click **Save**. This will prevent an unnecessary fail-over during the upgrade period.
- Run the software update on the Primary appliance first followed by the hot standby.

New Features, Bug Fixes, and Updates since Version 4.0.0 (including Versions 4.2, 4.1.2, 4.1.1, 4.1.0, and 4.0.1)

- **New Features Added in 4.2**
  - Backup/restore capability to appliance USB port
  - Logging of failed and successful appliance backups
  - Identity Profiles feature for templating of:
    - identity profile data, address information, account information, defaults
    - Role and group membership of identity
    - User defined data for identity
    - Token properties such as status, issue level, download, issue/activate/deactivate date

        - Scheduled or manual batch update runs of saved identity profiles against groups of identities
    - Video integration of Milestone XProtect Corporate Management Server
    - Video integration of Salient CompleteView Server
    - Mercury Casi Micro/5 Bridging Hardware integration
    - Added ability to browse for and upload license and key files for appliance licensing
    - New Browse functionality for CSV collaboration data sources to allow for local/network browsing
    - New one time CSV collaboration with recurring CSV capability to import role and partition data as well as tokens
    - New Browse functionality for file location on Windows shares used with appliance backups
- **New Features Added in 4.1.2**
    - Mercury Powered Aperio 8:1 Wireless lock hub integration
- **New Features Added in 4.1.1**
    - A token status criteria has been added to Doors/Identity with Access and Identity Doors with Access reports
    - Login and Badge Type criteria have been added to the Identity Summary and Identity Photo Gallery Reports.
    - A new Delegation Comparison report has been added which will allow users to easily compare delegations to see what differs
- **New Features Added in 4.1.0**
    - Ability to run transaction and audit reports for a number of days before the current date
    - An additional selection to the My Account page for a default Badge Template
    - Two new system settings attributes added to the database and the system settings screen. Users can now define pre-roll and post-roll number of seconds for the video playback
    - System settings number of video windows count added: minimum 1 window and maximum 10 is set
    - Search box added to Events page
    - 'Issue Date' import for Identities added to Identity collaborations
- **New Features Added in 4.0.1**
    - A Partition assignment feature was added to the CSV Recurring collaboration
    - Added a search capability to the HW status screen: users can limit the panels and doors shown on the screen to those in a selected group
- **Ruby on Rails Security Vulnerability Fixes**
    - CVE-2013-1854, CVE-2013-1855, CVE-2013-1856, CVE-2013-1857 fixes are included in version 4.2
    - CVE-2013-0155 and CVE-2013-0156 fixes are included in versions 4.0.1 and above
- **System Configuration and Administration Related Fixes and Updates**

- Email Global Action now able to be sent if executed manually or as part of an Action Group as of 4.2 release
- In previous versions of 4.*x*, users were not able to type in search criteria at the top of the listing screens and press the <Enter> key to execute the search. This has been fixed in 4.2
- Elevator Access Level page is now consistently sorted by output number
- In previous versions of 4.*x*, the **Settings** > **System Settings** > **External Domains** > Certificate list was not shown in the version 4.*x* style. This has been updated in 4.2
- In previous versions of 4.*x*, only the elevator inputs from the first elevator input panel were shown on the **Door** > **Elevator** tab for input/output naming. This has been fixed in 4.2
- In previous versions of 4.*x*, the **Add** button at the top of many configuration pages were not functioning. This has been fixed in 4.2
- In 4.0.0, Elevator Input and Output Panels were not available for selection as Door Elevator Hardware. This was fixed as of 4.0.1.
- In 4.0.0, the use of '(', ')', and '/' characters in user-defined list entries caused a rails error on deletion. This was fixed as of 4.0.1.

- **Identity Related Fixes and Updates**
  - Missing issue level default for Tokens added through a collaboration no longer causes validation errors when saving edits to Tokens
  - Previous versions of 4.*x* were missing the 'Default Role' page. This has been restored
  - In previous versions of 4.*x*, the **Save** button at the top of the Identity Edit page did not do anything when clicked. This has been fixed.
  - In 4.0.1, Badge Designer did not work properly in IE9. This was fixed as of 4.1.0
  - Adding a token with a leading zero in the internal number no longer generates a rails error
  - Auto-resizing of text fields in Badge Designer was enhanced as of 4.0.1

- **Report Related Fixes and Updates**
  - The Transaction Report filter for Full Name now works.
  - In previous versions of 4.*x*, the Holiday Report grid view search did not work properly. This has been fixed in 4.1.1
  - Holiday and Group Reports in 4.1.0 had invalid fields and incorrect labels displayed. This has been fixed in 4. 1.1
  - Area, Access Group, Event, and Event Type reports in 4.1.0 were missing data. This has been fixed in 4.1.1
  - In previous versions of 4.*x*, an attempt by a logged-in user to schedule a Custom Report without having his role assigned the Custom Report Schedule delegation, logged a rails error and the Job Specification window hung without any error message being displayed to the user as to the source of the problem. This has been fixed in 4.1.1
  - In previous versions of 4.*x*, the user was not returned to the Custom Reports list after editing and saving or cancelling a Custom Report, but was instead taken to the Standard Reports listing page. This has been fixed in 4.1.1

- The Camera, Alarm, Audit Log, and Transaction Log Reports have undergone various improvements.
- In previous versions of 4.*x*, filters did not work in the Search page under Monitoring and the 'Panel Date' column did not contain any data. This has been addressed in 4.2
- In the Tokens Pending Expiration Report, only active Tokens with an expiration date less than or equal to the number of days entered in the filter criteria are now shown.
- The performance of the Identities Access to Doors Report has been significantly improved
- In previous versions of 4.*x*, the identity-based reports in the UI (non-reports page) had old pre-4.*x* style formatting. This has been resolved in 4.1.1

- **Identity Collaboration Related Fixes and Updates**
  - Tab delimiter now functional for CSV collaborations as of 4.2 release
  - Single Role and Partition assignments in CSV collaborations now accept chars '(', ')', '*', or '\' in name as of 4.2 release
  - As of the 4.0.1 release, for the LDAP collaboration BLOB import, if the BLOB data for a record is not JPEG data, then the attempt to decode it if the result is JPEG data, use the result for the imported BLOB.
  - As of the 4.0.1 release, for the LDAP collaboration BLOB import, rather than searching up all results including all attribute values in one big search (which for blobs is certain to chew up available memory if there are a larger number of results), do an initial search for the result set with no attribute values at all. Then as each record in the result set is processed, search up the attribute values for that given record.
  - As of the 4.0.1 release, for the LDAP collaboration, rather than opening a connection to the customer LDAP database at the beginning of a collaboration run and using it for all steps, we will open a connection at the beginning of each step (role, identity, token, blob, udef) and close it at the end of the step. We were running into an issue with some LDAP databases when large searches were done that took a long time to process. We would not hit the customer LDAP database again for a long time and there was a timeout in the connection due to inactivity.
  - As of the 4.0.1 release, the LDAP collaboration token import now has .eq.system support to set the deactivation date for tokens added by the collaboration to be the token expiration offset from current day. Rather than entering an attribute name for the deactivation date field for tokens, you can enter .eq.system which will cause any tokens added using the collaboration to get their expiration date set to the system setting token expiration offset from current day

- **Replication / Redundancy Related Fixed and Updates**
  - Before 4.1.0, hardware status screens showed incorrect status while being viewed on an appliance that was not currently active managing the hardware. As of 4.1.0, status is now longer shown for such hardware

- **System Processing Related Fixes and Updates**
  - An issue where the icense check could sometimes be done based on fingerprint and date not in current license was fixed in version 4.2
  - An issue with slow subpanel firmware downloads to mercury subpanels was fixed in version 4.2
  - The expire cards nightly process was not being run in 4.0.0 or 4.0.1. This was fixed as of the 4.1.0 release

- Mercury Macro commands can be grouped as a, b, c, or d for purposes of processing commands conditionally. The Macro command 'Delay' was always being downloaded as belonging to Group A regardless of its actual group assignment. This was fixed as of the 4.1.0 release
- As of the 4.0.1 release, the application no longer generates system audit transactions for automatic modification of last door and last grant recording for Tokens and Identities after access grants. The program no longer generates system audit transactions for automatic modification of an Identity last login time after a login.
- As of the 4.1.0 release, ntpd is run every hour if a time server is configured on a Red Cloud appliance (non-Ubuntu)
- In 4.0.0, icons on maps that have unacknowledged alarms did not have the alarm count display on the icon flash in IE9 as they do in other browsers. This was fixed as of 4.0.1
- Issue with upgrades being run when EULA not signed causing LDAP database corruption was fixed.

Known Issues

- Image capture on the Apple Safari web browser platform currently does not work. Image capture is working properly on the Mozilla Firefox and Internet Explorer platforms.
- The Badge Preview function in Identities displays poor resolution of the badge layout. However, a high-resolution badge is correctly printed during the printing process.
- The Classic version of the RedCloud appliance cannot be upgraded to Version 4.2. For available hardware upgrade options and pricing please contact us for further information.

- The Express version of the RedCloud appliance can be upgraded to Version 4.2.

- If the existing firmware revision in a Mercury EP controller is greater than version 1.16.2, less than version 1.18.4, and TLS is enabled, occasional communication loss may be experienced during times of high activity such as a full download. Also, it may not be possible to complete a firmware download to the EP controller. As a workaround, TLS can be disabled, the firmware download completed, and then TLS can be re-enabled for the EP panel.