

Planning

- Try a 'dry run' first to determine if there are any issues with the data that will need to be corrected. CyberLock tech support is happy to help with dry runs to advise of any issues ahead of the actual migration.
- CyberAudit-Web Enterprise versions after 9.3 cannot restore CyberAudit Professional or CyberAudit-Web Professional databases. It's necessary to migrate in two steps:
 - Restore to CyberAudit-Web Enterprise 9.0 and back up the new database
 - Restore that backup to the current CyberAudit-Web Enterprise
- If CyberLock is doing the database conversion only for the migration, plan on 24 hours for turn around.
 - If CyberLock is doing the full migration and restoring the database to hardware (SE-200 or HP Server)
 - Plan on 48 hours for turn around
 - The order must be fully processed before we can begin
 - Please allow time for shipping as well as the migration
 - Schedule time with Tech Support
 - We are available Monday through Friday although we do not do full migrations on Fridays
 - We would like to start early in our day to ensure all the needed resources are available to address unforeseen issues
- Verify the number and type of communicators noting Web Authorizers, Flex System Hubs, Web Stations, and Single Key Vaults.
- Verify the network settings for the server
 - Will new server use the same network settings as the current (old) server?
- Verify current version of software
- Are they moving to your hosted solution?
 - If so, what CAW version is currently running on your hosting server?
- If the customer is working with their own license, verify customer's annual support is up to date
- Provide information to technical support
- If you are doing the migration on a new CAW server, build or prepare that server with the appropriate network settings.

Migration

- Have customer update all keys to allow plenty of time for the migration before they expire.
- If the new server will be configured with a new IP or DNS name the communicators need to be pointed to the new server IP/DNS prior to shutdown.
 - While all communicators are online, change their networking information in the software. This will cause change icons to appear.
 - Wait for the change icons to clear. The 'green OK' icon will also go away. This indicates the communicators got the new settings.
 - Note: Web Authorizers, Flex System Hubs, Web Stations, and Single Key vaults must be pointed to port 54443. So the server url should be something like `https://<my CAW server url>:54443/CyberAuditWeb/`. Any communicators that don't clear the change icon must be updated manually.

- Back up the database and stop the old system. To prevent 'orphaned' audit trails and settings the customer will stop using the current software and communicators until the new system is in place.
- If we are converting the database at CyberLock:
 - Tech Support will send a link to upload the database backup. Upload the database to be migrated.
 - Let Tech Support know when the upload is completed
 - We'll start work on the scheduled date
 - When the database has been patched, we will send a link to obtain the patched database
 - If we are doing the full migration, we will restore the new database to the new server. We will then ship the server after verifying it is set up correctly.
- Put the new server in place and bring it on line.
- Verify communicators are connected to the new server. This may take a few minutes