Codonics Virtua Disc Encryption

Technical Brief

Overview

This Technical Brief provides instructions for configuring the Codonics Virtua® Medical Disc Publisher to encrypt files recorded to discs.

Operational Description

Disc Encryption is achieved by applying AES-256 encryption to the files placed onto the discs created by Virtua. For Virtua DICOM discs, the encryption feature will properly span multiple discs if needed so that each disc can be run independently. For discs created using Virtua's Direct to Disc feature, disc spanning is not supported. When encryption is enabled, the recording process may be slower, especially for DVDs. Encrypted discs are not IHE compliant.

A decryption utility is included on the encrypted disc and does not need to be installed on the user's computer. The decryption utility will place files onto the user's computer in a temporary folder and then automatically run the program configured in the encrypted autorun.inf file (for most Virtua DICOM discs, this will be the LaunchPad application). When all viewing applications or open files are closed and the disc is removed, this temporary folder will be deleted to eliminate any patient information that was decrypted to the user's hard drive. An adequate amount of free hard drive space (depending on the size of the files to be decrypted) will be needed on the user's computer. Patient data will not be viewable until the entire disc is decrypted.

> **NOTE:** If importing patient data to a computer, the decryption utility will not automatically delete that data upon removing the disc (see Importing Data, below).

Prerequisites

Confirm that each of the following items is available:

- Disc Encryption requires a feature key on Virtua's SmartDrive. Contact Codonics Technical Support or your Codonics Representative to obtain the proper key.
- 3.1.2 software or later is installed on Virtua.
- User systems running Windows 2000®, XP® or Vista®.

> **NOTE:** Due to inclusion of the encryption software on each disc, the maximum space available on CDs is 600MB and DVDs is 4GB. This might cause the creation of additional discs.

Setting Up Disc Encryption

1. Add the Disc Encryption Feature Key to Virtua by entering the key on the Utility tab in the user interface.
2. Access profiles on the SmartDrive by either removing it from Virtua and mounting it in a PC or remotely accessing the files (see Operating Software 3.1.0 Release Notes, Codonics Part No. 901-204-001).
3. Set the doEncryption Profile option to **true** in encryption profile \profiles\encryption\encryption.default.txt.
4. Set the encryptionSetting Profile option to the desired password setting; default setting is **patient_DOB**.
5. Set the encryptionProfileName Profile option to **default** in each desired job profile at \profiles\job.

Encryption Profile Settings

Below is a list of the Encryption Profile parameters that must be defined in the encrypt.default.txt file.

Parameter: **doEncryption**
Settings: **true, false**
Default: **false**
Description: Enables or disables encryption.

Parameter: **encryptionType**
Settings: **7Zip**
Description: Identifies the type of encryption. 7Zip is the only valid setting.

Parameter: **encryptionSetting**
Settings: **patient_dob, patient_id, accession_number, *plain text***
DOB Format: *yyyymmdd* (ex. 20090528 for May 28, 2009)
Description: Identifies the password to be used. Passwords can be generated automatically using Patient ID, Patient Date of Birth or Accession Number of the first patient on the disc, or can be set manually with a text string containing only English characters. Passwords can be up to 64 characters long.

Study Information (including Patient Name, Patient ID, Study Date, Modality, etc.) and the Disc ID are included in a readme.txt file on the unencrypted portion of an encrypted disc. This is made available in case the label becomes unreadable or the password needs to be retrieved by cross referencing the Disc ID with the password list in the Virtua's \logs folder (see Password Retrieval, below).

CODONICS®

The Study Information Section can be excluded by setting the following parameter:

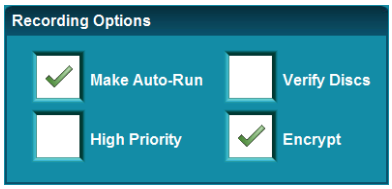
Parameter: **doIncludePlaintextStudyInfo**
Settings: **true** or **false**
Default: **true**
Description: If **false**, Virtua will exclude the Study Information Section from the readme.txt file.

The following is a sample Encryption Profile:

encrypt.default.txt
doEncryption = true
encryptionType = 7Zip
encryptionSetting = patient_dob
doIncludePlaintextStudyInfo = true

Manual Override

When manually submitting a job, the encryption setting can be changed on the Job Confirmation page. The encryption option is accessed by clicking the Edit Options button that is on the confirmation page. This change will only impact the current job. Note that the encryption box will not be available (disabled) if a selected job profile has the encryptionProfileName option set to **none**.



Encrypting Direct to Disc Content

Encryption of D2D jobs can be configured via the Job Profile specified by the Hot Folder profile (which in turn specifies an Encryption Profile). Alternatively, encryption of D2D jobs can be specified via a D2D Control file.

When placing a Virtua encrypted disc sent via D2D into a PC, the contents will be decrypted to the computer's temporary folder. If the encrypted contents contains an autorun.inf file, the autorun target will be launched after decryption is complete.

> **NOTE:** Not all viewing programs that run from a disc can properly run when launched from the user's temporary folder. If a viewing application does not run, please contact the viewer manufacturer.

The following options have been added to the D2D control file to override the encryption configurations of the Hot Folder:

Parameter: **doEncryption**
Settings: **true** or **false**
Description: Overrides the **doEncryption** parameter of the Encryption Profile. If **true**, the job will be encrypted (unless the encryption profile is set to **None**). If **false**, the job will not be encrypted.

Parameter: **encryptionPassword**
Settings: See Encryption Technical Brief.
Description: Overrides the **encryptionSetting** parameter of the Encryption Profile.

Parameter: **encryptionProfile**
Settings: The name of an Encryption Profile on the SmartDrive, or **None**.
Description: Overrides the **encryptionProfile** parameter of the Job Profile.

Parameter: **encryptionAutorun**
Settings: Windows® command with required parameters
Example: ***oem_viewer.exe /fullscreen***
Description: If the content to be encrypted does not contain an autorun.inf file, this parameter can be specified and Virtua will create an autorun.inf file that will run a specified command when the encrypted contents are decrypted to the user's temporary folder.

For more information on this feature, see the Direct to Disc Technical Brief (Codonics Part No. 901-171-002).

Password Retrieval

A list of the passwords used for each disc is contained in the log.job.csv file that is located in the \logs folder of the SmartDrive. This file is named with a .csv extension to facilitate examination with Microsoft Excel®.

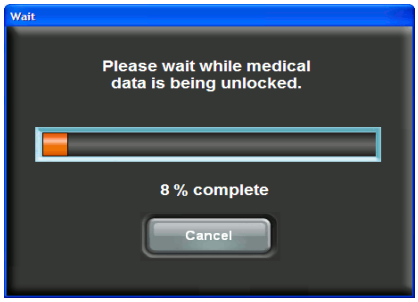
Using Encrypted Discs

Discs created with encryption will have a lock icon on the lower right side of the printed label and text at the bottom stating "Locked CD *x* of *y*" or "Locked DVD *x* of *y*." To enable the lock icon graphic on disc labels, Virtua units upgraded to 3.1.0 Operating Software or later need to replace the old labels in the SmartDrive \labels folder. Contact Codonics Technical Support for additional information.

Viewing Data

After placing the disc in a computer, the password entry dialog box will appear. Type the password (case-sensitive) and then select **View**. If the password is unknown, contact the originating facility shown on the disc label or listed in the README.TXT file on the disc.

If the correct password is entered, the patient data will be decrypted to a temporary folder on the computer.

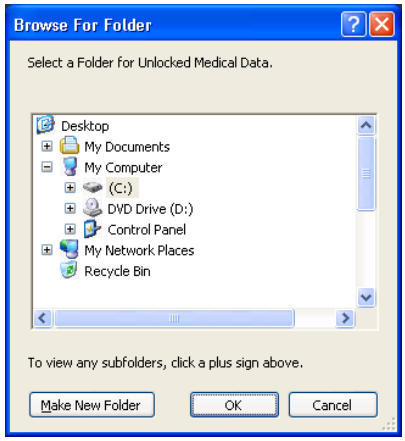


The LaunchPad will display after decryption is complete. The amount of time to decrypt a disc can vary significantly depending on the amount of data to be decrypted and the computer doing the decryption. Typical* decryption times for a typical CD (150 MB of data) is around 1-2 minutes, a full CD can be in excess of 6 minutes, while a full DVD can take over 30 minutes.

* Pentium® P4 processor @ 3.4 GHz, 1 GB RAM

Importing Data

To decrypt the disc contents to a specific location on the end user's computer, type the password and click the **Extract** button. If the correct password is entered, a Browse for Folder dialog will be displayed. Choose a folder, click **OK** and the patient data will be decrypted to the selected folder on the computer.



If files already exist in the selected folder, a warning dialog will be displayed. If the user chooses **OK**, existing files may be overwritten by the decrypted files.

> **CAUTION:** Do not remove a disc while the extraction process is underway since this could result in a partial study to be transferred without the user's knowledge.

Known Issues

- **List of Virtua viewers supported.** The following optional viewers for Virtua systems will work with encryption:
  - Clarity™ Viewer
  - Clarity™ 3D/Fusion Viewer
  - eFilm Lite™
  - MIMVista® MIMviewer®
- **Other viewers, including viewers recorded using the Direct to Disc (D2D) interface, may not function correctly when run from a temporary folder.** If a viewer does not run, please contact the viewer manufacturer. It is strongly recommended that sites using D2D test encrypted discs made by Virtua to ensure that the viewer works before providing encrypted discs.
- **Password requirements.** Passwords with non-English characters may not be interpreted consistently. A job will not record if the password is longer than 64 characters.

Technical Support

If problems occur that are not covered by this Technical Brief, contact Codonics Technical Support between the hours of 8:30AM and 5:30PM EST (weekends and U.S. holidays excluded).

Phone: 440-243-1198
Email: support@codonics.com
Website: www.codonics.com

Get it all with just one call 1-800-444-1198

CODONICS®
We bring the future into focus

17991 Englewood Drive
Middleburg Heights, OH 44130 USA
(440) 243-1198
(440) 243-1334 Fax
Email info@codonics.com
www.codonics.com

Codonics Limited KK
New Shibaura Bldg. F1
1-3-11, Shibaura
Minato-ku, Tokyo, 105-0023 JAPAN
Phone: 81-3-5730-2297
Fax: 81-3-5730-2295