



# DISCRETE TECHNOLOGIES

A G T G I C O M P A N Y

## SecureDisc Rimage Edition

Disc Encryption for  
Rimage Publishing Systems



# Introduction to SecureDisc

- Encrypts the *entire disc image*, not just files or folders
- Provides password access control and authentication
- Simple to use – minimal changes to workflow needed
- Two different, free decryption clients for flexibility in deployment
- End user needs the SecureDisc Client and correct password to access an encrypted disc
- Does ***not*** require specialized blank media
- Encrypts with 256-bit AES
- Compatible with Rimage Software Suite 8.0 and higher



# Licensing | Updates | Support

- SecureDisc is licensed per server (control center)
- Software Assurance & Enhancements (SAE) subscriptions cover updates to software
  - Patches within a major revision (ex.: v1.0 to v1.1)
  - SAE rollover to major version release (ex.: 1.1 to 2.0)
  - Per year SAE pricing based on single unit price per unit purchased
  - Two release targets per year
- SAE purchases include
  - E-mail support for 1 year
  - Software updates



# SecureDisc: How it Works

- SecureDisc loads as a transparent proxy between Messaging Server and Production Server
- SecureDisc can be enabled per-job through the User Type flag in the Rimage job API, or turned on for all jobs using forced encryption mode
- When enabled, SecureDisc intercepts the production order before it reaches Production Server
- SecureDisc retrieves the encryption password from one of four sources:
  - Merge field
  - Password file inside the plaintext image
  - Fixed option as set in SecureDisc console
  - SQL database via ODBC (optional)
- SecureDisc automatically encrypts the disc image mentioned in the production order
- After encryption is complete, SecureDisc passes the image back to Production Server to continue the recording process. The entire encryption process occurs transparently within the Rimage workflow



# Server Requirements

- Must be installed on Rimage Control Center (standalone or embedded)
- Windows XP (32-bit), Windows 7 (32/64-bit), Windows Server 2003/2008/2008 R2 (32/64-bit)
- 5MB free disk space for program files
- Rimage Producer Suite version 8.0 and above




# Image Packs

- SecureDisc for Rimage is licensed per encrypted image generated
- Each unique encrypted disc counts against a running total of available pre-paid images
- Licenses are provided as refills or “Image Packs”
- Image Packs may be purchased and applied at any time
- Image Packs that have been applied never expire
  - A running count is kept of every unique encrypted disc image
  - Every unique encrypted image decrements an internal counter
  - Multiple copies of the same unique encrypted image count as one
  - Image Packs are supplied in quantities of 1K, 5K, 10K & 25K

Image licensing status

0	processed
20	remaining

[Get Refill...](#)

  
There are less than 200 images left.  
Please refill soon.



# Applying Image Packs

- SecureDisc for Rimage has a secondary license per encrypted image generated
- After the initial registration, image packs can be added
- Open the SecureDisc Console  
*Start > Programs > SecureDisc for Rimage*
- Click on Get Refill
  - Select an Image Pack (refill) quantity and click Generate
  - E-mail the displayed code to *support@gtgi.com*.
  - When the order has been processed, a refill code will be e-mailed as a reply. Paste the refill code into the lower window and click *Add Refill*

Discrete Refill System

Request a refill

Select the refill size you want, then press "Generate" to get your request code.

50 images  ☐ Deactivate this system

```
<GTGIRegFile Type="Request">
<FileID>76cJZjkLLeULTp19Rc0r6schrTJ5g0cxA6vwW0CsQ=</FileID>
<RegData>lk2nHvfthYZA8R8q4A9Tm/hzoZO3QvY9JXXaM4stHMagWHBym/SMHzSpofic
<RegStats>JlUYbk7BAj7dq9yd1qtnjqnU/+Z7YDhW0B9xTNO9R7jBGgStnetzx+Njj5tOJ4
</GTGIRegFile>
```

Email or FAX this request block to Discrete with your name and contact info to purchase a refill block.

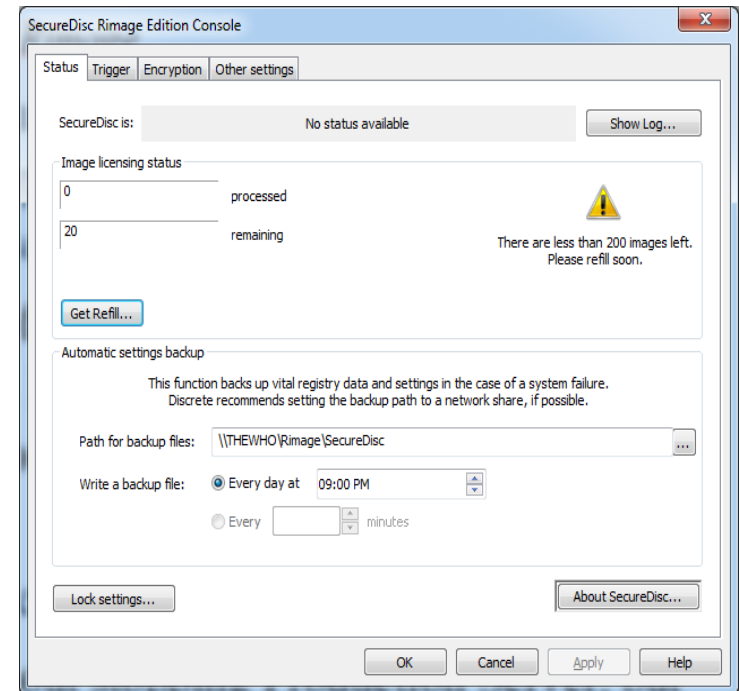
Add a refill

Paste purchased refill block here and press "Add Refill"



# Status

- Open the SecureDisc Console  
*Start > Programs > SecureDisc for Rimage*
- *Image licensing status* displays the number of used and available images.
- *Automatic settings backup* backs up SecureDisc's license status and settings to a file on disc (external HDD or network share)







# Configuration

- SecureDisc Rimage Edition is configured through the SecureDisc Console application
- SecureDisc Console reports system and licensing status, and allows configuration of encryption, networking, and disaster recovery options



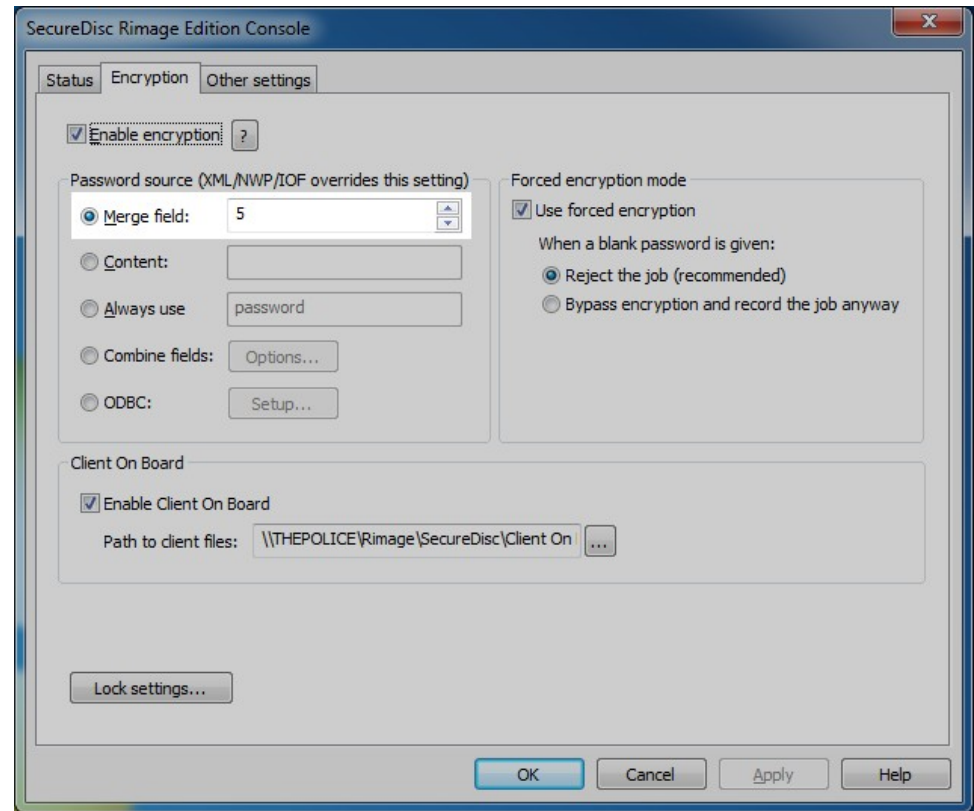
# Integration: Password Sources

- SecureDisc supports several password integration options:
  - *Merge Field* allows the password to be placed in a merge field that is typically used for printing. This is the most popular option and the easiest to integrate
  - If needed, data from two merge fields may be combined with the *Combine Fields option*
  - The *Content* option looks for the password inside of a text file included with the contents of the disc to be encrypted
  - *Always Use* allows the specification of a fixed password that is used for all encrypted discs
  - The optional ODBC source allows password retrieval from an SQL database
- Passwords may be 1-255 characters in length
- Passwords are UTF-16 and may include special characters



# Password Source - Merge

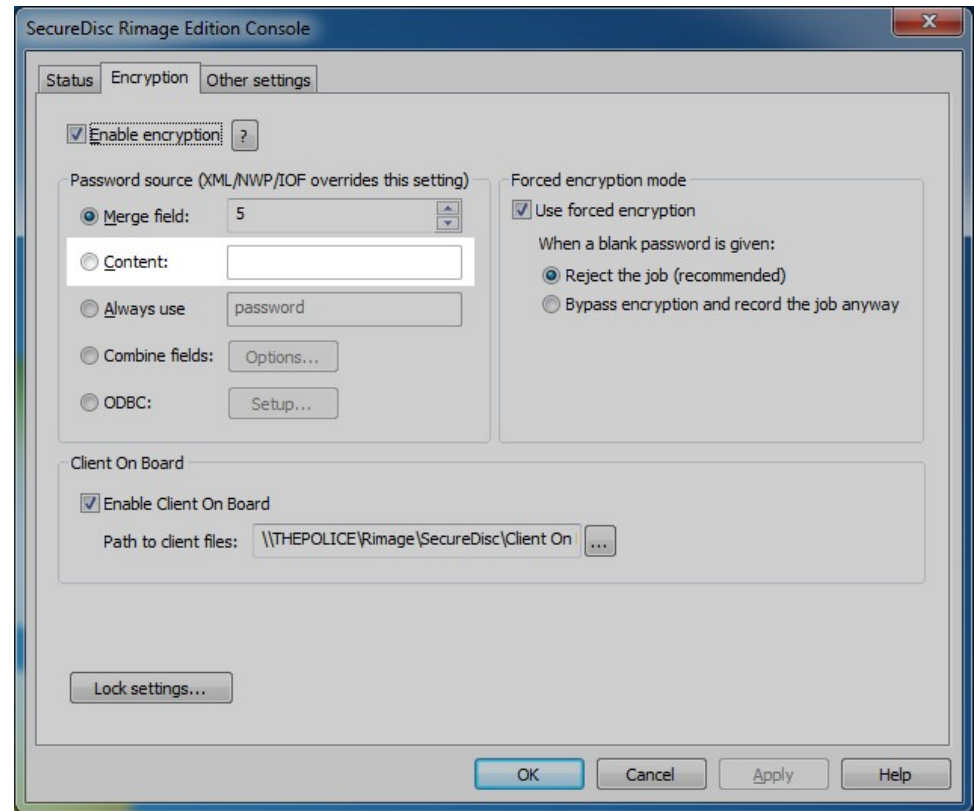
- In the SecureDisc Console, choose the *Encryption* tab, and set *Password options* to *Merge field*
- Set the *merge field* number. This is the field SecureDisc will read the password from. In most integration scenarios, it is typically the last field in an existing merge file format
- If the merge file has a header, fields can be specified by name
- After a disc is encrypted, the selected merge field is blanked inside the merge file before the disc is printed





# Password Source - Content

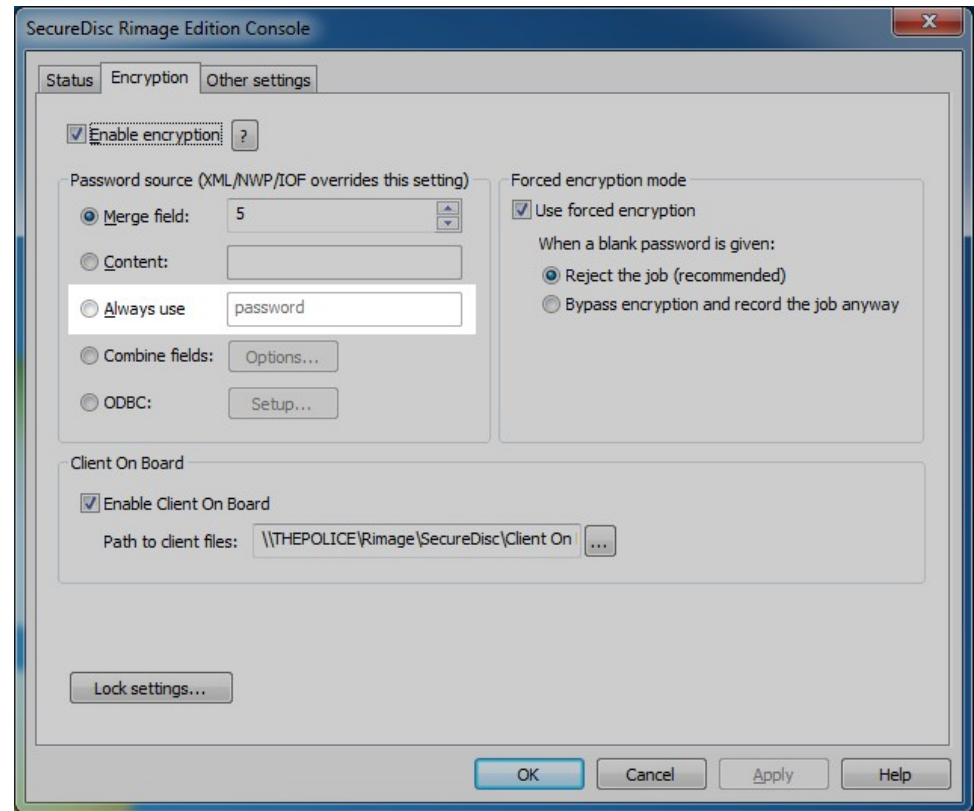
- In the SecureDisc Console, set *Password options* to *Content*
- In the *Content* field, set a file name. This is the name of a file that will be included in the disc content that contains the password. *Password.txt* is typically used
- When generating a job, include a plain text file that contains only the desired encryption password, and name it *Password.txt*
- Include the plain text file in the root folder of the content
- SecureDisc will check the cached disc image for the text file. The file will be blanked after SecureDisc retrieves the password, before encryption takes place





# Password Source - Fixed

- In the SecureDisc Console, set *Password options* to *Always Use*
- In the *Always use* field, set the desired encryption password
- All jobs that have encryption enabled will use the password specified here





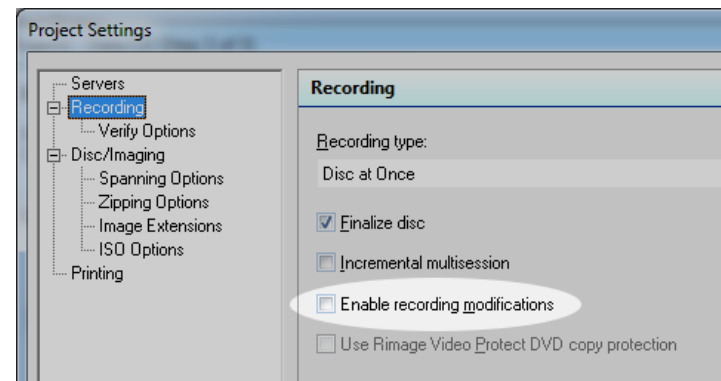
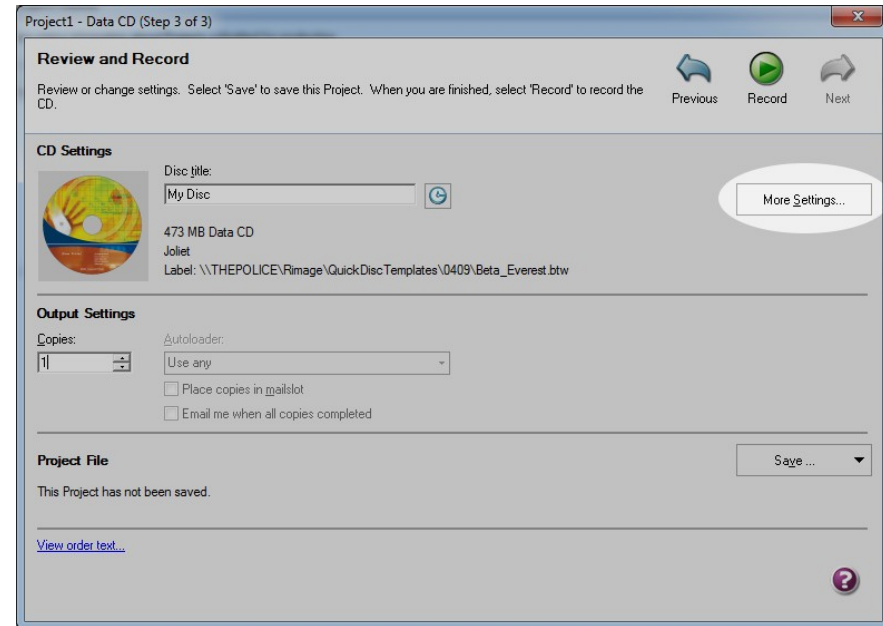
# Integration: Enabling SCD

- Enabling SecureDisc encryption is done on a per-job basis
- The Rimage QuickDisc application can enable encryption natively
- Custom and third-party applications can enable encryption:
  - Through the XML API
  - Through the IOF/POF interface
  - Through Network Publisher



# Enabling SCD - QuickDisc

- Start A QuickDisc DVD or CD job
- Specify password in merge field *or* create a password.txt file to be included with the content *or* set fixed password in console
- On the last page of the QuickDisc wizard click *More Settings*
- In *Recording* settings, check *Enable Recording Modifications*
- Submit job





# Enabling SCD – Rimage API

- 3rd party and custom applications can enable SecureDisc encryption using a special flag
- In all available interfaces (XML, IOF/POF, Netpub) the flag works the same way
- The flag must be set with each job that needs to be encrypted
- To enable encryption specify *User Type* as “1”
- In some cases the previously mentioned password integration options may be overridden by specifying the desired password inside the order API
- To override other password options specify *User Data* as the desired password
- See the Rimage documentation specific to the API your application is using for more information about the proper placement of the *User Type* and *User Data* flags





# Integration: Forced Encryption

- Some 3rd party applications cannot be modified to take advantage of the special flags required to enable SecureDisc encryption
- Encryption can be *forced* using SecureDisc Rimage Edition's forced encryption option
- When encryption is forced, all incoming jobs are encrypted using the password integration type set in the SecureDisc Console
- Jobs that do not meet the requirements for encryption (such as a blank password field) can either be rejected, or passed through without encryption
- Blank password handling can be configured from within the SecureDisc Console



# Reading an Encrypted Disc

- Users must have the SecureDisc Decryption Client installed *and* the correct password to access an encrypted disc
- After entering the correct password, the disc is unlocked and decryption is performed in real time
- There are two types of SecureDisc Client software, the Explorer Client and the Resident Client. Please try both and determine which suits your needs better
- Both types of SecureDisc Client are free to distribute to your end users



# SecureDisc Explorer Client

- Requires no installation, no reboots, and no Administrator rights in almost all use cases
- Files larger than 50,000,000 bytes may require a one-time logon as Administrator and reboot
- Uses built-in Windows networking functions for drive-letter access
- Slower and less compatible than the Resident Client, but better end-user experience
- Recommended for smaller data sets (600 MB or less) and situations where Administrator rights are difficult to get



# SecureDisc Resident Client

- The original SecureDisc Client
- Installs as a filter driver on CD-ROM class devices
- Entirely transparent
- Very fast
- Requires no reconfiguration of viewer software or other proprietary applications
- Requires Administrator rights to install
- System must be rebooted to complete install
- Recommended for large data sets (DVD or Blu-Ray) and situations where Explorer Client cannot work



# Integration Notes

- The log file contains valuable information
  - The log file is plain text and well formatted for easy parsing by an external application
  - Encryption status is always reported in the log



# Thank You

For more information please visit our website

[www.gtgi.com](http://www.gtgi.com)