Secure*Disc*

Rimage Edition
Administrator's Guide

FOR USE WITH RELEASE 2.8.0 AND HIGHER

Contents

Copyright Information

SecureDisc Rimage Edition Administrator's Guide

While we strive to ensure compatibility with all supported Rimage equipment and operating system versions, there may be unforeseen issues that cause this product to function improperly. If you have installed SecureDisc Rimage Edition and you are having problems, please contact us.

To report errors or omissions in this manual, contact us at (703) 486-0500 or send an email to support@gtgi.com.

March 2016 Edition
SDR Version 2.8.0 and 3.0
Explorer Client version 1.5 and higher
Resident Client version 3.0 and higher

Introduction

SecureDisc Rimage Edition (SDR) is used for protecting content recorded on CD, DVD and/or Blu-Ray media by restricting access to the content via a decryption key. SDR encrypts the entire contents of an ISO or UDF disc image using a FIPS 140-2 validated 256-bit AES (Advanced Encryption Standard) module in CBC mode. The most popular SDR configuration ('Client on Board') adds a decryption client and other files that are accessible prior to decryption.

SDR is comprised of two parts:

- An encryption service installed on the Rimage system (or Control Center) that processes disc production orders prior to passing them on to the Rimage Software Suite.
- A "client" decryption application that is typically deployed on the same disc with the encrypted data and used by the receiver's computer to decrypt (read) the encrypted data

System Requirements

Disc Creation (encryption platform):

- Rimage Producer, Professional or Desktop series running Rimage Producer Software Suite, OfficeNet or Network Software Suite version 8.0 and above
- 20 MB free disk space for program files
- Client application generating disc production jobs (e.g. QuickDisc or third-party software)

Disc Viewing:

Explorer Client

- Windows XP or higher (32-bit or 64-bit; supports Windows 10)
- DVD or CD reader
- Free disk space for caching the contents of the encrypted disc session

Resident Client

- Windows XP or higher (32-bit or 64-bit; supports Windows 10)
- DVD or CD reader
- 1MB of free disk space for program files
- Administrator privileges for initial installation

FIPS Information

- SDR contains an embedded, FIPS 140-2 validated encryption module
- For specific FIPS information, visit http://www.gtgi.com/products/securedisc-rimage-edition

Licensing Process

SecureDisc base licenses, Expansion Modules and Image Packs are licensed per computer system, whether a standalone PC or an embedded Control Center in a robotic system (see Software Activation & Image Packs for details). Both the SecureDisc Explorer Client and SecureDisc Resident Client may be distributed freely, but access to the latest releases of those clients is limited to customers covered by Software Assurance & Enhancements (SAE).

Each Refill request from the SecureDisc Console contains a unique serial number generated from multiple hardware components in the local machine. This serial number will change if the hardware configuration is substantially altered, such as replacement of certain major components (motherboard, etc). If GTGI receives a Refill request that contains a serial number that does not match the requesting customer's base license serial number list, the license request will be denied.

GTGI recognizes that hardware changes may occur for a variety of reasons, and has developed the following policies regarding hardware change scenarios:

Deactivation and License Transfer *[requires SecureDisc Rimage Edition 2.2 or later]*

When replacing an older model with a new system, GTGI will transfer each base license and remaining Image Packs to a new unit. This process consists of deactivating the existing license through a special Deactivation Request that must be sent from the SecureDisc Console. This will deactivate the SecureDisc base license on that system and provide a count of the remaining Image Pack licenses back to GTGI. The customer will then send a Refill request from the new system after downloading and installing the demo version of SecureDisc software from http://www.gtgi.com/demos. GTGI will issue an Image Pack refill for the new system in the amount of the remaining images left from the deactivated system. The old system will no longer be eligible for use with SecureDisc unless the Deactivation and License Transfer process is repeated in reverse.

License Transfer without Deactivation

If the existing hardware system running SecureDisc experiences a catastrophic failure and must be replaced, customer must supply GTGI with documentation of system replacement by the manufacturer or an authorized service provider. Since the Deactivation and License Transfer process could not be completed, GTGI cannot validate the quantity of image licenses remaining on the system. Once the hardware change by the manufacturer has been verified by GTGI, GTGI will transfer the base license to the new system at no charge, but the customer will need to purchase a new Image Pack for the replacement system at standard commercial pricing.

Special Note for SecureDisc 1.x and 2.x Users

GTGI no longer sells Unlimited licenses for any version of SecureDisc, and no longer issues Image Pack refills for SecureDisc version 1.x. Therefore, if a system with an Unlimited license must be replaced under scenario 2 above, the customer ***must*** upgrade to SecureDisc version 2.x or 3.x (SAE customers are eligible for a 50% discount from the commercial price). GTGI will issue a one-time 10,000 Image Pack license at no charge for the new system in place of the original Unlimited license. Additional Image Packs are available at standard commercial pricing.

Software Download & Installation

Download the latest version of SDR from http://www.gtgi.com/demos. Launch the SDR installation program, then follow the wizard's on-screen instructions. After installing the SDR application, set the desired options in SecureDisc Console to begin processing job files. By default, only 10 encrypted images will be available. To receive the image pack that is included with the paid version, simply register the software as described in Software Activation & Image Packs.

IMPORTANT NOTE FOR RIMAGE PRODUCER SUITE 9.0 USERS:

Rimage Producer Suite 9.0 includes a new "Watch Server" that has Network Publisher emulation capability. However, it is not compatible with SDR, as Watch Server is a module running inside of Rimage's Messaging Server, and thus bypasses the SDR proxy.

If you are running Network Publisher jobs and want to use SDR, we recommend using SDR 3.0's new Network Publisher emulation feature.

IMPORTANT NOTES FOR USERS UPGRADING FROM SDR 2.2.x OR EARLIER:

Starting with version 2.5.1, SDR has introduced the following changes:

1. Due to a change in how SDR formats the encrypted disc with Client on Board enabled, **Client on Board discs encrypted with SDR 2.5.1 and higher require a current decryption client** (Explorer Client 1.3 or higher, Resident Client 2.4 or higher) and **cannot be decrypted with older Explorer or Resident Clients.**
2. **SDR's method of operation has changed significantly, which may impact your workflow.** Older versions of SDR implemented encryption using a "ModifyDisc" plug-in DLL that was loaded directly into Rimage's Production Server. Newer versions of SDR use a Windows service that intercepts jobs before Production Server can access them, encrypts the data, then passes a modified job file to Production Server for recording and printing. In order for SDR to process jobs sent from XML API applications (including Rimage QuickDisc), SDR must make a change to the Messaging Server configuration to move the Rimage services to a different communications port. *This requires a reboot immediately after installing SecureDisc!* You may reconfigure this setting in the SecureDisc Console's Trigger tab (versions 2.5.1-2.8.10a), or in the new SecureDisc Service Configuration application (version 3.0).
3. **The SecureDisc Console has been redesigned and some functions are now in new**

locations. Users of earlier versions should note that no features have been removed, only relocated and (in a few cases) renamed for accuracy. For more details, please see the notes labeled 'Prior versions' throughout this document, but primarily concentrated in the SecureDisc Console section.

Technical Notes

SecureDisc options, such as triggering and password source, are set in the SecureDisc Console and must be configured properly for the software to encrypt discs in the automated production process.

Encryption is performed on a disc image prior to processing by the Rimage production software. When triggered, SecureDisc retrieves the password from one of the selected integration methods and runs it through several one-way and other functions. Once an encryption initialization vector (IV) is derived, the cached disc image is encrypted in-place inside of the cache, and a special header, along with an authentication hash, is placed into sector 15 of the image.

If Client on Board (CoB) is enabled, SecureDisc includes additional 'in the clear' (unencrypted) files on the disc. The 'in the clear' files for each disc are the static files contained in a designated folder (by default, Rimage/SecureDisc/Client on Board) which initially contains the SecureDisc Explorer decryption client and an AUTORUN.INF along with any other 'in the clear' files the producer wishes to include. ***Please refer to the Client on Board section for important notes on limitations with this feature.***

Upon completing the encryption process, SecureDisc generates a new XML production job and submits it automatically to the Rimage Producer Software Suite for processing.

Encryption Password Integration

In order for SecureDisc to successfully encrypt a disc image, there must be a methodology to provide the encryption password to the SecureDisc encryption engine. SecureDisc receives passwords from existing infrastructure and does not store passwords once a disc has been encrypted. SecureDisc does not implement its own stand-alone password/key-management system.

There are five methods of encryption password integration:

- **Merge Field**
  This method will extract the password from a specified merge field intended for a label. This method is convenient for integration into an environment that already uses merge fields for disc identification. SecureDisc will “blank” the merge field specified as the password field before the label is printed. This prevents the password from accidentally

being printed on the disc label. The header row used in some merge files is automatically detected based on number of records and copies requested. When using the Merge Field password integration type, add a dummy field to the disc label design (such as the First field) and designate it for password use. This field's position inside generated merge files must be consistent with the field number selected in the SecureDisc Console. Although the password field will be present on the label design, the password itself will not be printed.

When using the named merge fields (header row) method to design labels, name the first merge field *password*, and always place the password in the first field. Select *field 1* in the SecureDisc Console.

- **Content**
  This method extracts the encryption password from a text file included with the content. The password file should contain only the password, should be in ASCII text format, and must be placed in the root (top-level) folder of the disc content to be encrypted. All password files must have the same name on each disc (such as `password.txt`), and the file name must be specified in the SecureDisc Console.

- **Always Use**
  This method is a fixed password option that will encrypt every disc with the password value specified in the SecureDisc Console.

- **Combine Two Merge Fields**
  This method will generate a new password value by combining values from two different merge fields, adding a higher level of security than using a single merge field value. To configure the options associated with this feature, click the 'Configure' button to open the Combined Mode Setup window. The combined value is generated by starting with the value in the *Base merge field* and adding the value from the *Field to append*. See the Merge Field section (above) for more information on selecting the correct merge field number. In addition, there are options to manipulate the data extracted from one or both of the merge fields, which are performed in top to bottom order, as follows:
    - **Remove leading zeros** will strip any numeric zeros from the beginning of the value extracted from the merge field prior to performing any further manipulations
    - **Truncate to [x] characters** will reduce the value extracted from the merge field to the designated number of characters prior to performing any further manipulations
    - **Convert to uppercase** will change all lowercase characters in the value to uppercase
    - **Blank for printing** will “blank” the specified merge field when the label is printed to prevent inclusion of the merge field data on the disc label.

- **Rimage API – XML, Network Publisher (NWP)/Data Publisher (ORD), IOF/POF**
  This method overrides the selected integration type in the SecureDisc Console automatically, and is not explicitly selectable in the SecureDisc Console.
  For all jobs generated with the current API (XML data), SecureDisc checks for the presence of the `UserType=1` flag. If present, SecureDisc will attempt to read the password from the `UserData` field. If the `UserData` value is null (or the field is not present), the password integration type selected in the SecureDisc Console will be used.
  For custom applications that use Rimage's Network (NWP) or Data Publisher (ORD) or legacy API (POF/IOF), enable the Security option in the job file and optionally include the password value following a comma, such as: `Security=1, pass1234`
  This will enable encryption and specify "pass1234" as the password. See the Rimage guide for your particular interface for more information about enabling the security bit.

Encrypting with Rimage QuickDisc

- Using the Project Wizard, select a Data CD or Data DVD job type.
- Select the files to be encrypted and move to the next screen.
- Select a label that meets the label design requirements. If using the 'Merge Field' password integration method, the label must contain a Merge Field of the same numerical value as the setting in the SecureDisc Console (also see Encryption Password Integration). Enter a password in the appropriate Merge Field when prompted to enter merge values after selecting a label.
- Enter a value for the Volume ID (this will be reported by SecureDisc Explorer when viewing the encrypted disc session) and select a quantity (see Encrypting Multiple Copies, below)
- On the final page of the QuickDisc Wizard, click on *More Settings* then click on *Recording*. Check the *Enable recording modifications* box. This is the trigger for Rimage Production Server to pass the job to SecureDisc for encryption.
- Under *Disc*, confirm that the *Use Power Image* check box is cleared. This check box has three possible states: checked, shaded or cleared (white). SecureDisc will only function on the cleared setting.
- Click *OK* to return to the Wizard and submit the job.

Saved QuickDisc Project files retain all the above settings to make it easy for non-technical users to create encrypted discs. See the QuickDisc Help and User Guide features for more information on creating and using QuickDisc Project files.

Encrypting with 3rd Party or Custom Applications

The recording modification option must be enabled on a per-job basis by the 3rd party application to enable encryption. This is typically accomplished through the Rimage XML interface by adding the *UserType* and *UserData* fields to the XML job before sending it to Messaging Server. See the

Rimage XML API Guide for more information. To enable encryption, set `UserType=1`. To include the password in the XML (which overrides the *Password Source* selection in the *Encryption* tab of the SecureDisc Console), specify `UserData=password123.`

For custom applications that use Rimage's Network or Data Publisher (NWP or ORD) or Powertools API (POF/IOF), enable the Security option. For example, in a Network Publisher environment, to enable encryption and specify “password123” as the password, use “`security = 1, password123`” See the Rimage guide for your particular interface for more information about enabling the security bit.

Encrypting Multiple Copies

If a single job has multiple copies enabled, all copies will be encrypted with the password specified for the first copy. Multiple copies made with the same password only count once against the encrypted image count.

Encrypting Spanned Data Sets

SDR fully supports the Rimage Disc Spanning feature as implemented in Rimage QuickDisc, when Client on Board is not enabled. CD Disc Sets can be encrypted using Client on Board providing there is space to add the 'in the clear' session on each disc. This is accomplished by setting the 'Capacity' drop-down in the *Disc* settings to a smaller size than the actual media used. For example, when using 700 MB CDs, set the 'Capacity' to 650 MB. Also, the Explorer Client cannot be used in conjunction with the Rimage Span Restore application on each disc, so we recommend deploying the Resident Client installer on spanned disc sets when using Client on Board.

Forced-Encryption Mode

A forced-encryption environment is typically configured when it is undesirable or impossible for a third party application to enable the “Recording Modifications” (sometimes referred to as “User Type” or “Security”) flag in the Rimage order submission API. Enabling forced-encryption mode will result in SDR attempting to encrypt every production job detected, regardless of source (QuickDisc and/or 3rd party application).

To enable forced-encryption mode, open the SecureDisc Console and select the *Encryption* tab. First, ensure the *Encrypt Data* box is checked. Now check the *Use forced encryption* box. SDR will attempt to encrypt ***all*** jobs detected from the source/s specified in the *Trigger* tab. Because of this forced behavior, all orders sent for production are expected to comply with the requirements for encrypting an order.

Handling Blank Passwords in Forced-Encryption Mode

In forced-encryption mode, SDR provides two ways of handling jobs with blank passwords:

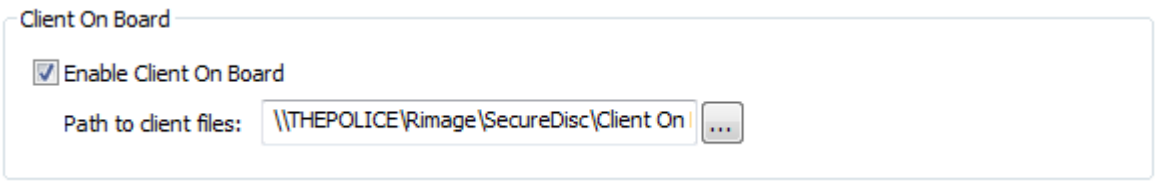
- The first method simply rejects jobs with blank passwords. This is the default.
- The second method will encrypt all jobs with non-blank passwords, but record a job with a blank password in the clear, as if SDR were not present. This method is useful if you use your Rimage system to produce the occasional non-encrypted disc.

The controls to switch the password method are located directly under the “Enable forced encryption” check box:

- Choose “Reject the job (recommended)” to use the first method.
- Choose “Bypass encryption and record the job anyway” to use the second method.

Please note that SDR does not warn about blank passwords when the second method is enabled, which may be a security risk. GTGI recommends using the second method only as needed.

Client On Board (CoB) *[Prior versions: See below for information on changes in CoB implementation]*



NOTE: This function is similar to the Client on Board feature in SDR versions prior to 2.5, but is implemented differently to eliminate some undesired limitations of the prior implementation. Consequently, Client on Board discs encrypted with SDR 2.5.1 and higher require a current (Explorer Client 1.3 or higher) decryption client for successful decryption.

SDR has the ability to add 'in the clear' (unencrypted) files to an encrypted disc during processing. The unencrypted files may include the SecureDisc Explorer Client (which is included by default), the SecureDisc Resident Client installer (if desired), and other static files that do not need to be secured (such as user documentation, disclaimers, etc.). To make the user experience as simple as possible, see the section Automating the Customer Experience Using CoB.

When an encrypted disc made with the CoB feature is inserted into a computer, the disc contents are presented, which will include an encrypted image file (SD_ENCRYPTED.IMG), and the contents of the Client on Board folder. By default, the Client on Board folder contains SCDExplorer.exe (the SecureDisc Explorer Client) and an AUTORUN.INF. Once the SecureDisc Explorer Client has launched (via Windows AutoPlay or manual user launch), the user will be prompted for a password and the encrypted session will be accessible upon validation of the password value.

To use Client On Board:

- Enable the option in SecureDisc Console.
- Select the parent folder that contains the static content to be included. Be sure to include the SecureDisc Explorer Client and/or the Resident Client installer in the folder (see SecureDisc Clients for more details) as well as any other files to provide customer information and/or automation (see Automating the Customer Experience Using CoB). **NOTE: The 'in the clear' files will reduce the amount of available space on a blank disc by the size of the selected folder content.**
- Click on OK to save the settings and exit the Console.

Automating the Customer Experience Using Client-on-Board

When utilizing the Client on Board feature, there are several ways to automate the customer experience of accessing the encrypted contents. There are two parts to automating the user experience, either or both can be used depending on the disc contents and desired behavior.

Automating the Unencrypted Content

The unencrypted content will be all the files present in the '*Path to client files*' setting in the Client on Board section of the SecureDisc Console. By default, this target file (called 'Client on Board') includes an `autorun.inf` file which will launch the SecureDisc Explorer Client (`SCDExplorer.exe`) on Windows systems with AutoPlay enabled (to learn more about `autorun.inf` and Windows AutoPlay, see the Wikipedia entry at: http://en.wikipedia.org/wiki/Autorun.inf).

Since many Windows systems do not have AutoPlay enabled or the AutoPlay settings may have been modified and will not launch `autorun.inf` automatically, some users will still need to navigate to the disc contents and double-click on `SCDExplorer.exe` to initiate the decryption process. You may choose to include a `readme.txt` or similar file in the 'Client on Board' folder to instruct the user to take this action.

Automating the Encrypted Content

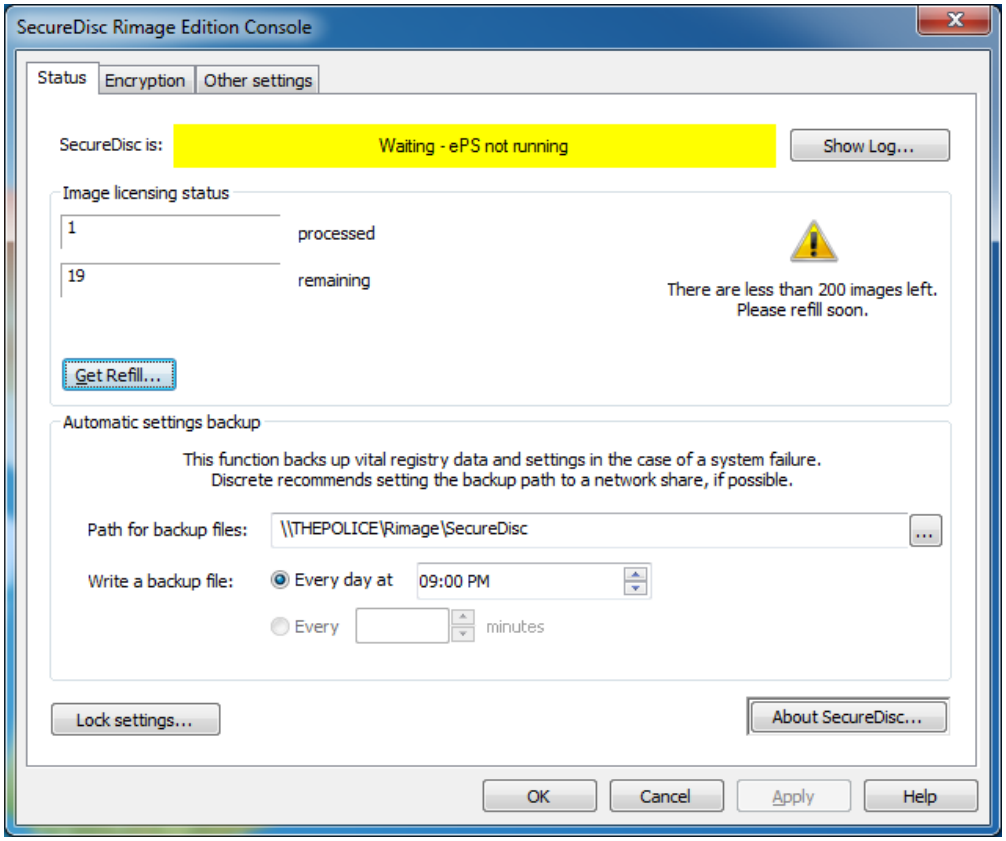
When the correct password value is confirmed by `SCDExplorer.exe`, it will search for the presence of an `autorun.inf` file in the root of the encrypted ISO and if present, will execute the contents of the file silently (the user will not be presented with a confirmation dialog or AutoPlay options). So if the encrypted content was designed to launch automatically via `autorun.inf` in older versions of Windows, the user experience of the encrypted content will be identical to the behavior of the same data on an unencrypted CD launched through the Windows Explorer.

Since many discs do not contain `autorun.inf` in the encrypted content and altering the up-stream production workflow to include a new file may be difficult or undesirable, SCDExplorer.exe can also execute automation of the encrypted content using instructions provided in the unencrypted `autorun.inf` file.

This method allows a specific file or application to be launched automatically from the encrypted ISO just by editing the contents of the `autorun.inf` present in the designated Client on Board folder (default: \Rimage\SecureDisc\Client on Board). To accomplish this, open the default `autorun.inf` file in a text editor such as Windows Notepad and edit the existing `open=SCDExplorer.exe` line by adding `/run` followed by the command line to be executed (including any switches supported by the target application) surrounded by double quotation

marks. Examples:

```
open=SCDExplorer.exe /run “index.html”
open=SCDExplorer.exe /run “myviewer.exe -AL -UN="value1" -PW="value2"”
```



Behavior for example 2: In Windows systems with AutoPlay configured correctly, the Explorer Client will automatically launch once the disc is mounted, request the password, and upon confirming the correct password has been entered, automatically launch the `myviewer.exe` application (providing the file is resident in the root of the encrypted ISO) and activate the command line switches listed. For systems with AutoPlay disabled, the user must launch SCDExplorer.exe manually, but the automation of `myviewer.exe` and the command line switches would still occur automatically after successful password validation.

SecureDisc Console

The SecureDisc Console is accessible through the Start menu:

Start > **Programs** > **SecureDisc Rimage Edition** > **SecureDisc Console**

Status tab

License status

- *Processed* – shows how many encrypted discs have been produced
- *Remaining* – shows how many encrypted discs remain in the current license
- A warning triangle will be displayed when there are less than 200 images remaining

Get Refill...

- Click this button to generate a refill request code. Refer to Software Activation & Image Packs section for more information

Lock settings

- Click on this button to lock the console settings. You will be prompted to choose a password.
- Once locked, the controls on the Configuration tab will be disabled until the lock is removed. Click on “Unlock settings” and enter your password to remove the lock.

About SecureDisc...

- Provides link to SecureDisc version information

Automatic settings backup *[SecureDisc 2.8 and later]*

This feature backs up your SecureDisc unit data and settings to a secure location. Use it whenever possible, as it makes restoring units after a system crash or system restore easier.

- Use the “Path for backup files” field to tell SecureDisc where to store its backup files. This should be a location that will not be destroyed by a system crash or a system restore, such as a network share or a removable disk.
- The “Write a backup file” field sets up a schedule for SecureDisc to write a backup file. This uses the Windows Task Scheduler, and you must have access to the Taks Scheduler's TASKS folder (usually C:\Windows\Tasks) to set or change the schedule.

SecureDisc backup files are written in a format that includes that date and time of the backup in the filename. To recover from a system failure, find the latest backup you have, then contact GTGI support.

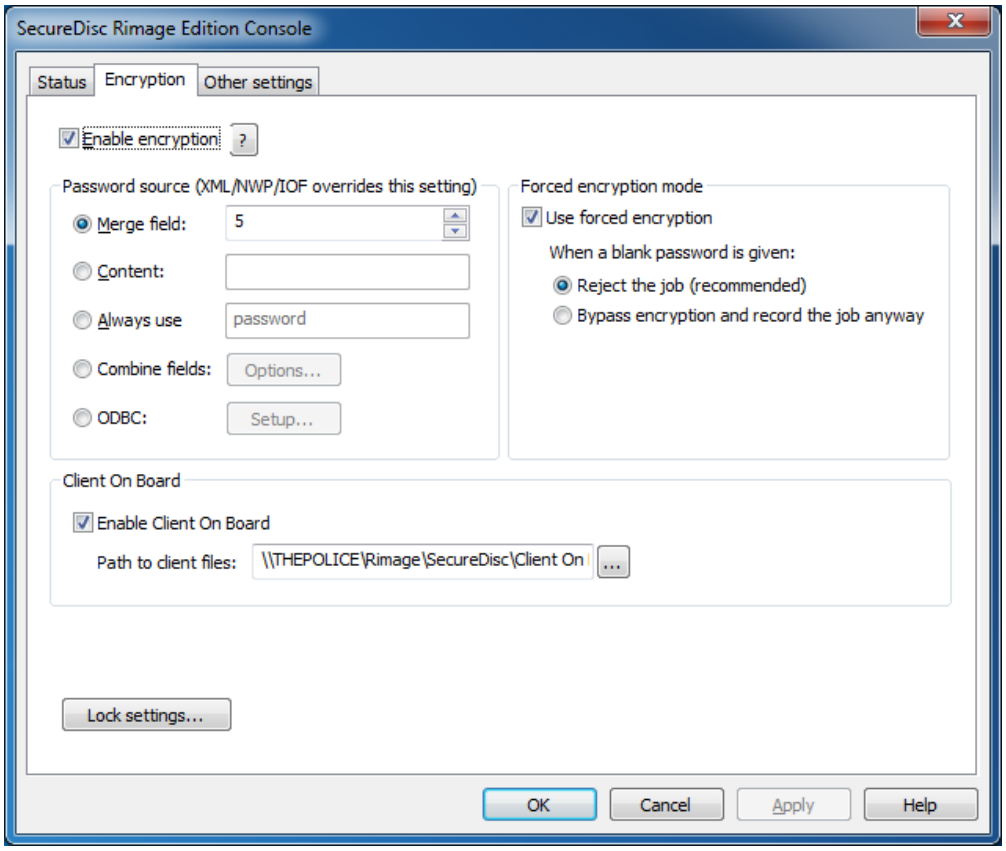
Trigger tab *[SecureDisc 2.5.1-2.8.10a only]*

Listen for Rimage XML orders *[Default status: Enabled]*

- Enables listening for incoming XML job files on port 4664 and output of processed job files to Rimage PSS on port 4665. SDR automatically reconfigures Rimage PSS to port 4665 when this setting is enabled and moves Rimage PSS back to port 4664 when disabled, in order to provide seamless transition for all applications publishing Rimage XML jobs to port 4664. If this setting is disabled, the SecureDisc *Status* tab and the *Status Monitor* application will both have a red bar indicating SecureDisc is inactive.

Network Publisher Emulation *[Default status: Disabled]*

- **Not available in SDR 2.x.** *Please note that this setting does **not** affect how Rimage's Network Publisher software works with SecureDisc.*



Encryption tab *[Prior versions: Replaces the 'Images' tab and most of the settings from the 'Configuration' tab]*

Enable Encryption *[Default status: Enabled]*

- Enables encryption processing. De-selecting this feature passes all job files to the Rimage Producer Software Suite without encrypting. Typically this option is only turned off during troubleshooting in order to remove all encryption processing from production jobs without uninstalling SecureDisc Rimage Edition.

Password Source *[for more details on these options, see Encryption Password Integration]*

- *Merge field* – uses the merge field number specified for the password source
- *Content* – retrieves the password from a file embedded in the content. Specify the password file name here
- *Always use* – encrypts all jobs with the specified password *[Default setting for use in initial testing]*
- *Combine fields* – combines the contents of two merge fields to create a new value. The 'Options' button provides access to the parameters controlling the merging operation.

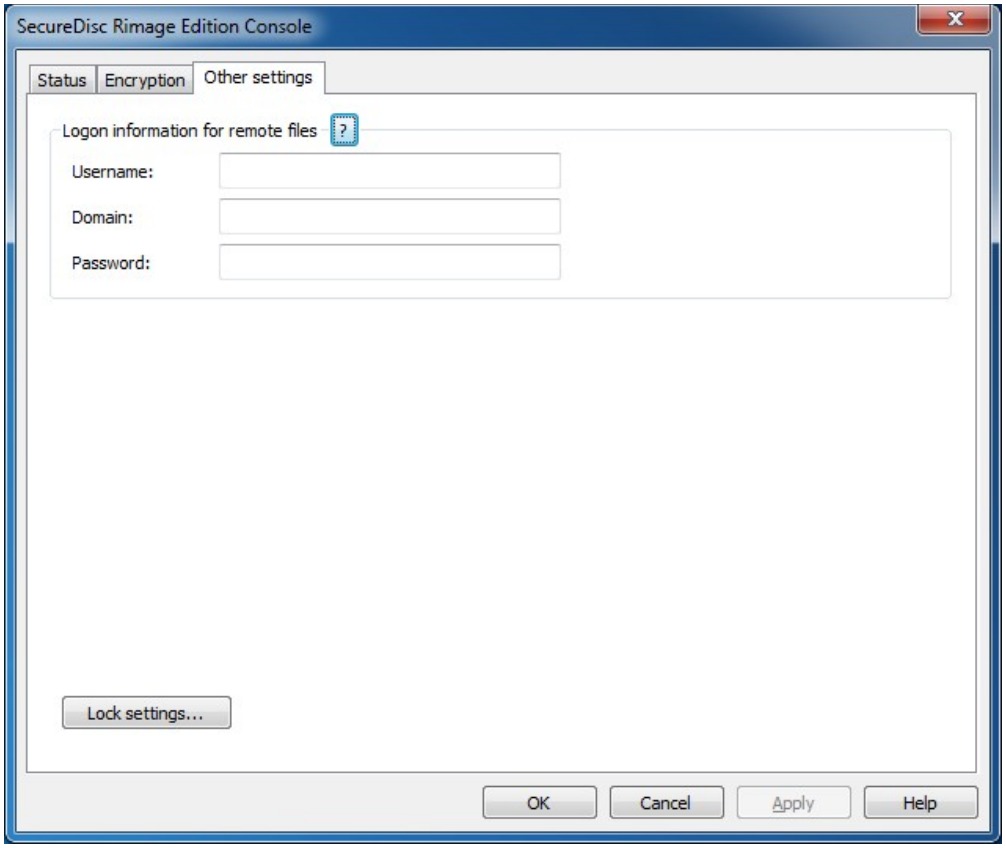
[Prior versions: The 'Combine fields' option is not present prior to SDR release 2.2.8]

Forced encryption mode *[Default status: Disabled]*

- *Use forced encryption* – Turns Forced-Encryption Mode on or off.
- *When a blank password is given:* – Changes how SDR handles blank passwords in forced-encryption mode. See the Forced-Encryption Mode section for more information.

Client On Board *[Default status: Enabled]*

- When enabled, records a non-encrypted session to each encrypted disc. This 'in the clear' session contains the contents of the folder specified. See the Client On Board section for further information.



Other settings tab

Network Logon Information [***Prior versions: Replaces the 'Modifydisc.dll Logon Information' function]***

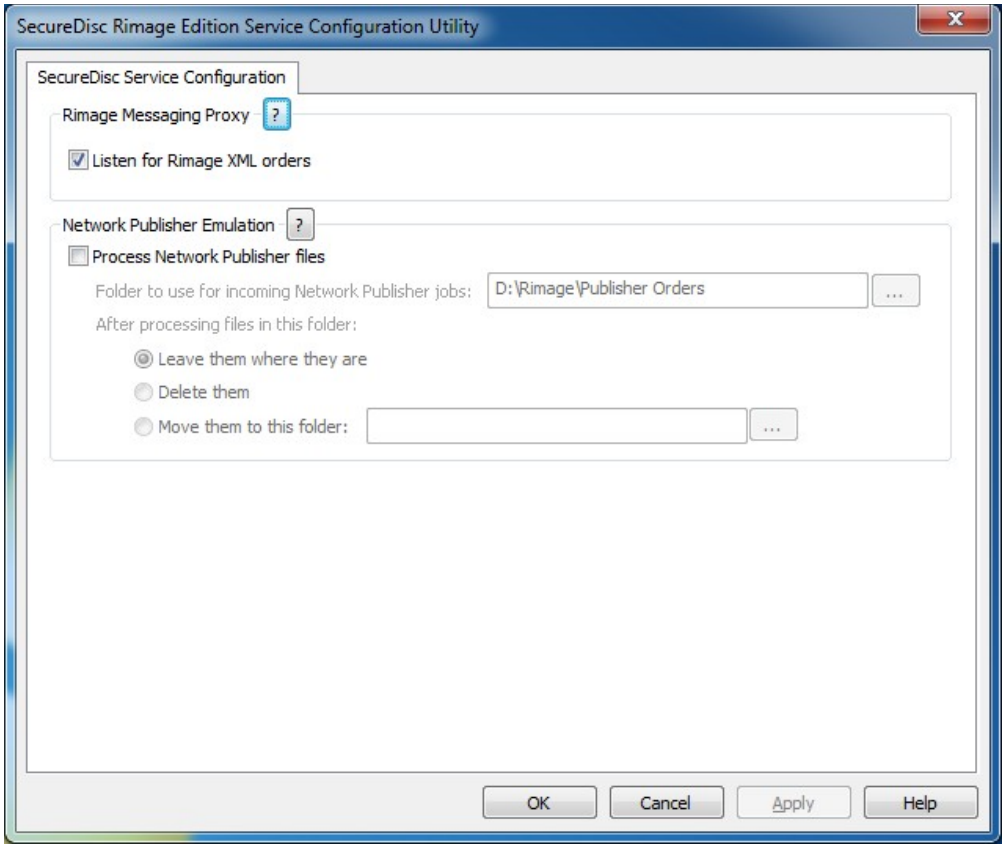
- Enter a *username*, *domain*, and *password* of a domain account that has access to data, merge files and labels stored on a network share point. If no data, merge files and/or

labels are stored on a network share point (all content is local on the PC running SDR), leave these fields blank (default).

Log viewer tab

- Displays the SecureDisc log.
- For assistance with errors, copy and paste the contents of this log into an email to *support@discretetech.com*.

SecureDisc Service Configuration *[version 3.0 only]*



The SecureDisc Service Configuration application takes the place of the Trigger tab in previous versions of SDR. It requires Administrator privileges to run.

Listen for Rimage XML orders *[Default status: Enabled]*

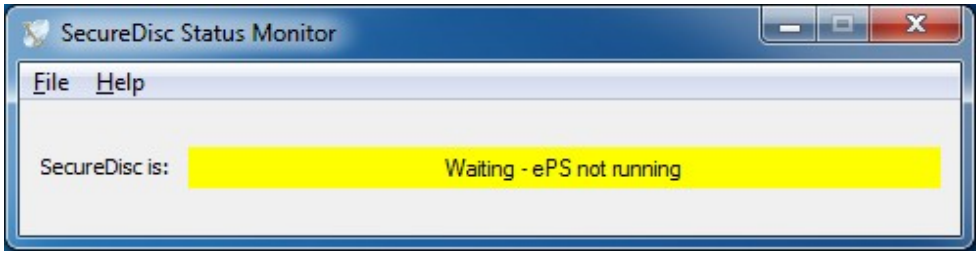
- Enables listening for incoming XML job files on port 4664 and output of processed job files to Rimage PSS on port 4665. SDR automatically reconfigures Rimage PSS to port 4665 when this setting is enabled and moves Rimage PSS back to port 4664 when disabled, in

order to provide seamless transition for all applications publishing Rimage XML jobs to port 4664. If this setting is disabled, the SecureDisc Console *Status* tab and the *Status Monitor* application will both have a red bar indicating SecureDisc is inactive.

Network Publisher Emulation ***[Default status: Disabled]***

- Enables SecureDisc's built-in Network Publisher emulation (NPE). This is meant for newer Rimage machines running Producer Suite version 9.0 and up, where it replaces the Network Publisher emulation in Rimage's Watch Server (which is not compatible with SecureDisc). It can also be used in situations where Rimage's older Network Publisher J (NPJ) software is unavailable or not recommended, and offers several improvements over NPJ, including improved logging.
- Unlike NPJ, NPE runs as a service, meaning that it can be used completely unattended (no console access or remote login required).
- Setting up NPE is similar to NPJ:
  - Point the “Folder to use for incoming Network Publisher jobs” to where your Network Publisher jobs usually go.
  - By default, NPE leaves completed jobs in the same folder, which is the same behavior as NPJ and Watch Server. Optionally, completed jobs can be separated into another folder, or deleted entirely.
- NPE's log is in a rolling text file format, and is located in `\Rimage\Logs\HOSTNAME_SecureDiscNPE.log`.
  - The format for each entry is `[date] channel: message`, one per line. NPE logs both Rimage errors and job progress.
- The structure and details of NWP/ORD files are beyond the scope of this document. Please refer to the Network Publisher documentation for more information.

SecureDisc Status Monitor



The SecureDisc Status Monitor is a small application that runs in the Windows System Tray, and provides information about whether encryption is currently available.

To open the Status Monitor, double-click on the tray icon. The status window (as shown above) will appear. This works identically to the status indicator inside SecureDisc Console, and updates every second.

Status Monitor runs at startup, and can be closed by right-clicking on the tray icon and choosing “Exit”.

Software Activation & Image Packs

Encrypted discs produced using SecureDisc incur a per-encrypted-image charge. SecureDisc keeps a running count of encrypted images produced, and a total of purchased encrypted images available. Encrypted Image Packs (“refills”) may be purchased separately and applied at any time.

Encrypted Image Pack refills may only be used on the server that requested the refill. Refills are applied through the SecureDisc Console. Once a refill is applied it has no time expiration, however, a refill must be applied within 72 hours of generating the original request code.

To register SecureDisc, follow the same process used for applying Image Packs, as outlined below. If the software has not been paid for, you will be contacted by a sales representative for payment instructions.

Applying a Purchased Encrypted Image Pack

- Open the SecureDisc Console
- Select the *Images* tab
- Click on *Get Refill*
- Select the quantity of the Image Pack being requested. If the quantity you have purchased is not listed, select '*other*.'
- Click on *Generate*
- Click on *Copy to Clipboard*
- Paste the XML Request block into an email with your contact information and send to *admin@gtgi.com*. Put *SecureDisc Refill* in the Subject line along with the quantity Image Pack purchased.
- A refill code activating the number of images you have requested will be e-mailed to the address entered providing that full payment for the Image Pack has been received.
- Paste the refill code from the e-mail into the lower block
- Click on *Add Refill*

Software Deactivation & License Transfer

This process enables transfer of a purchased SecureDisc base license and Image Pack from one system to another via deactivation. The most common scenario is upgrading to a new Rimage system and decommissioning the existing system. Completing this process will deactivate the current system for both SecureDisc and any remaining Image Pack licenses and initiate transfer of the activation and Image Pack to a new system.

- Open the SecureDisc Console
- Select the *Images* tab
- Click on *Get Refill*

- Check the *Deactivate this system* box
- Click on *Generate*
- Confirm that you are deactivating this system by clicking the *OK* button
- Click on *Copy to Clipboard*
- aste the XML Request block into an email with your contact information and send to *admin@gtgi.com*. Put *SecureDisc Deactivation* in the Subject line.
- This system is now deactivated and will no longer be able to produce encrypted discs.
- To transfer the base license and remaining Image Pack licenses to another system, download and install the latest version of SecureDisc Rimage Edition from *http://www.gtgi.com/demos*
- Follow the Software Activation & Image Packs procedure to receive a refill code for the new system that will activate the remaining Image Pack licenses from the prior system.

SecureDisc Clients Overview

Accessing the encrypted contents of a disc processed by SecureDisc requires a SecureDisc Client software application. There are two SecureDisc Clients: the Explorer Client and the Resident Client.

The SecureDisc Explorer Client is included in the SDR installation package and automatically configured to deploy on each encrypted disc through the Client on Board feature. This eliminates the need to install the Resident Client on most systems. However, in very rare cases the recipient PC may have issues with the Explorer Client and require the Resident Client to fully interact with the encrypted disc session. For this reason, SDR customers using a version with Client on Board capability may wish to deploy the Resident Client installer package in the unencrypted disc session along with the Explorer Client (please refer to the Client on Board section for details).

SecureDisc Explorer Client

The SecureDisc Explorer Client is compatible with Windows XP and later (both 32-bit and 64-bit, including Windows 7, 8.x, and 10) and does not install on the recipient PC. Typically, it does not require Administrator rights for utilization.* It is designed to provide access to the encrypted session by launching as a memory resident application.

* If your data set includes files larger than 50,000,000 bytes (about 47 MB), all supported Windows versions require a one-time setting change (which requires Administrator log-in and a reboot) to increase the default web folder file size limit. See the Troubleshooting Decryption Issues section for more details on these issues.

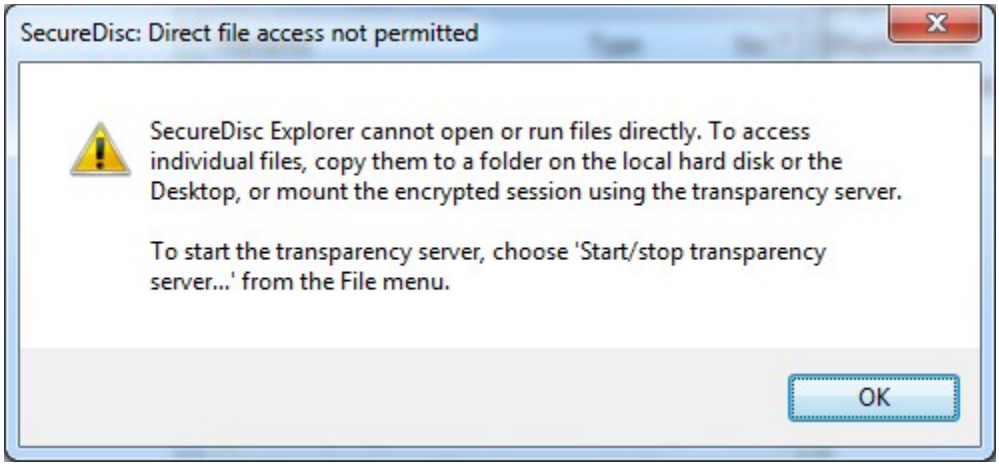
Launching the Explorer Client from a Client on Board encrypted disc

The Explorer Client (SCDExplorer.exe) is typically present as an unencrypted (“in the clear”) file on a disc produced by SDR using the Client on Board feature (unless the SCDExplorer.exe file is manually removed from the folder designated in the 'Path to Client Files' location of the SecureDisc Console). The default configuration iincludes a pre-built parent folder that contains the Explorer Client and a default `autorun.inf` file to launch the Explorer Client automatically on systems with AutoPlay enabled. Please see the Automating the Customer Experience with CoB section for more details on how to customize automated behavior.

If the Explorer Client is not automatically launched, open the disc in Windows Explorer and double-click on SCDExplorer.exe. The Explorer Client will start, check the disc and present a login box. Enter your password here, and either press Enter or click OK.

Once logged in, the Explorer Client attempts to launch a Transparency Server to provide a full

range of interaction with the contents of the encrypted session. If the Transparency Server cannot mount, the Explorer Client presents an 'Explorer style' window that provides a list of the files in the encrypted session. In this mode, files can be copied (singly or in groups) to another location, but they cannot be launched or activated from the encrypted session location. Double-clicking on any file in the SecureDisc Explorer window will produce the following dialog explaining the limitation:



The Transparency Server

The Explorer Client's Transparency Server provides drive-letter access to the encrypted disc's contents using a built-in Web Distributed Authoring and Versioning (WebDAV) server, in conjunction with the WebDAV redirector client (WebClient) included with Windows XP and above. Using the Transparency Server, the encrypted disc contents can be used as if they were on a standard drive, including launching applications, right-click file operations, etc.

The Transparency Server has some limitations related to Microsoft's WebDAV implementation that can affect its ability to mount on certain systems. See the Troubleshooting Decryption Issues section if you encounter any problems.

Tray icon

When the Explorer Client is minimized, the SecureDisc logo will appear in the system tray, next to the clock. Double-click on the SecureDisc logo to restore the Explorer client window, or right-click for more options:

- *Restore*: Restores the Explorer Client window.
- *Start/stop transparency server:* Unmounts the drive letter being used for encrypted-disc access, then stops the Transparency Server. *Make sure any files and folders on the drive letter are closed before using this option.*

- *Exit:* Closes the Explorer Client, unmounts and stops the Transparency Server, and ejects the disc.

Using the Explorer Client to read SecureDisc v1 encrypted discs

This procedure is used in cases where a customer wants to read encrypted discs that were produced with SecureDisc v1 (or SecureDisc v2 with the Client on Board feature disabled), and do not have a Resident Client installed on their system.

In these cases, the customer will need a Client on Board disc encrypted with SecureDisc v2.2 or later in order to read the older disc.

1. First place the Client on Board encrypted disc in the drive and navigate to the file listing.
2. Copy the `SCDExplorer.exe` file to any location on the local PC (such as the Windows Desktop)
3. Remove the Client on Board disc and place the older encrypted disc in the drive.
4. Double-click on the `SCDExplorer.exe` application to launch it.
5. The Explorer Client will search all local optical drives for a SecureDisc encrypted session and when located, will automatically prompt for the password.
6. Once logged in, the Explorer Client will attempt to mount a built-in Transparency Server to provide full drive letter access to the encrypted session. Please refer to the Troubleshooting Decryption Issues section for any issues that may arise.

SecureDisc Resident Client

The SecureDisc Resident Client is compatible with Windows XP and later (32- and 64-bit, including Windows 7, 8, and 10) and requires installation on the recipient PC. Initial installation requires Administrator rights. Once installed, the Resident Client can be used by any user logged in to the computer regardless of rights and permissions.

The Resident Client installs two parts—a "filter" driver and a "helper" application. The filter driver is placed in the Windows filter driver stack and acts as a wedge between the operating system's CD-ROM hardware driver and the system's CD-ROM file system driver. The helper application is what the user sees—it displays drive status and handles routing the disc password to the filter driver.

When a disc is inserted, the filter driver checks to see if the SecureDisc encryption header is present. If the header is not present, it changes to by-pass mode, where the disc is directly accessible by the CD-ROM driver. If a SecureDisc header is found, the filter driver notifies the helper client to prompt for a password. The password is then sent from the helper application to the filter driver.

The filter driver runs the entered password through a proprietary one-way function. This generates a unique fingerprint keyed to each individual disc. If the result matches a fingerprint stored in the header on the encrypted disc, the password is correct. If not, the password is bad and the disc is ejected. If the correct password is entered, SecureDisc uses data present in the disc header to retrieve the decryption key. The filter driver enters decryption mode, and decrypts blocks of the disc as they are requested.

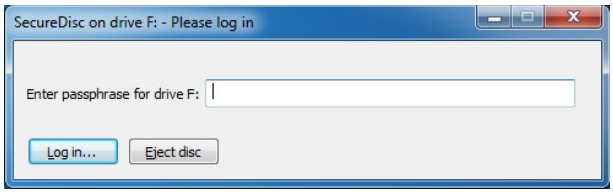
The plaintext password is not stored anywhere on the user's computer. Once a disc is ejected, the filter driver flushes any variables used to decrypt a disc. The decryption key itself is randomly chosen and stored encrypted on the disc with 256-bit AES – no two disc images will ever have the same key, even if the plaintext password is the same.

Resident Client Installation

Run the SecureDisc Client installation program and follow the wizard’s on-screen instructions. Administrative rights are required for installation, however, once installed SecureDisc Client is available for all users. Rebooting is required after installation. Silent installation is available for automated deployment by adding the “/s” switch when running the installer from a command line or script.

Removing or upgrading the SecureDisc Resident Client always requires the user to reboot their computer to remove the installed version of the filter driver.

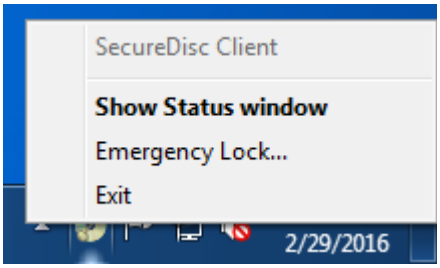
Using the Resident Client



To read an encrypted disc, load the disc into an available reader. The Resident Client will automatically open and prompt for the password. Enter the password and click on Log In. To cancel password entry, click on Eject Disc.

If an incorrect password is entered, the disc is automatically ejected and the client login window is closed.

The SecureDisc client has no settings that require configuration. The SecureDisc Client loads at system startup into the system tray, next to the clock.



Right-click on the SecureDisc logo to view the context menu:

- *Show Status Window* displays the drives available and whether they contain an encrypted disc

- *Emergency Lock...* ejects all discs currently logged in and clears the password from memory. Ejecting a disc by any means automatically logs out the disc and clears the current password.

Troubleshooting Encryption Issues

NOTE: If the problem you are experiencing is not fully addressed by the Resolutions in this section, please visit our Support site and complete a SecureDisc Rimage Edition Trouble Ticket.

Issue:
SDR is installed but does not seem to be functioning- discs are being produced on the Rimage system but they are not encrypted and no errors are occurring.
Resolution:

1. Confirm that the *Listen for Rimage XML orders* box is checked in the *Trigger* tab of the SecureDisc Console (versions 2.5.1-2.8.10a) or in the SecureDisc Service Configuration application (version 3.0).
2. Confirm that the *Enable encryption* box is checked on the *Encryption* tab.
3. Confirm that SecureDisc is Active (green) in the *Status* tab.
4. If sending jobs through the Network Publisher interface, confirm that jobs are not being sent through Rimage Software Suite 9.0's Watch Server. If they are, please see the Network Publisher Emulation section for information on how to configure SecureDisc correctly.

Issue:
Third party software package does not have a provision to enable the "recording modification" option.
Resolution:
Consider using Forced-Encryption Mode.

Issue:
Submitting a disc production job generates an error [302] "XML Order parsing exception"
Resolution:
There may be an issue with SecureDisc parsing the specific XML data generated from your third-party application. To report this issue to Discrete:

1. Open *Rimage System Manager*, select *Production Server* in the left pane, then select the "*Server Orders*" tab in the right pane.
2. Send whichever job was causing the XML error.
3. When the error occurs, the job will be listed as Cancelled in the *Server Orders* tab. Right-click on the job entry and select "*Show order*". This will open a new window with the job's XML source in it.
4. Click "*Copy All*" and then paste the order source into an email or text file, and send it to support@gtgi.com.

Issue:
SDR reports that it cannot access data files, a merge file or label file.
Resolution:

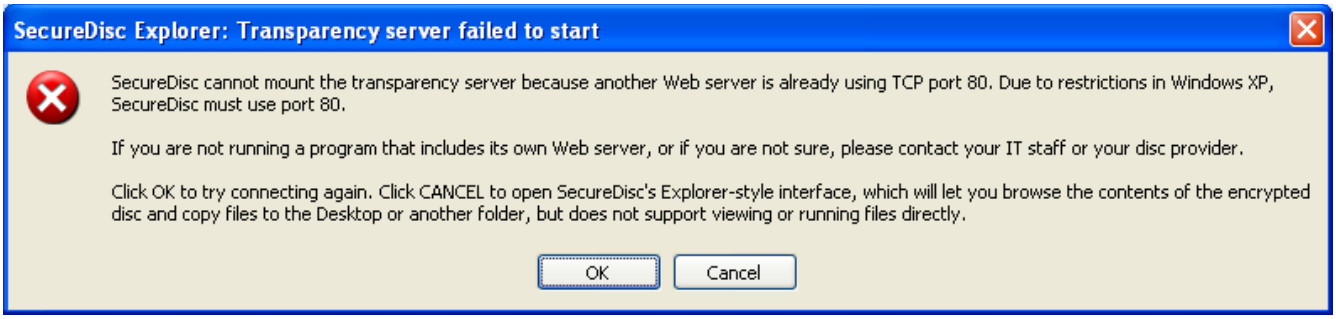
Merge files or label files that reside on a network share point may need to be accessed by a user account with specific rights. Set the *Network Logon Information* values in the *Other settings* tab of the SecureDisc Console.

Issue:
In a previous version of SecureDisc, I was prompted to restart Production Server after making settings changes. I am no longer prompted to do so. Do I need to manually start and stop Production Server?
Resolution:
SecureDisc versions prior to 2.5 operated as a 'plug-in' to Production Server (ePS) and consequently required an ePS restart when many SDR settings changes were made. Beginning with version 2.5, many SDR settings changes no longer require this. However, if a change requires an ePS restart, you will be prompted accordingly.

Troubleshooting Decryption Issues

NOTE: If the problem you are experiencing is not fully addressed by the Resolutions in this section, please visit our Support site and complete a SecureDisc Decryption Trouble Ticket.

Issue:
The Explorer Client returns the following error message: "Transparency server failed to start"



Resolution:
The Explorer Client uses its built-in Transparency Server in conjunction with the built-in Windows WebDAV redirector to provide drive-letter access to the encrypted session. Due to limitations in Windows XP's built-in WebDAV redirector, the Transparency Server *must* use port 80 there. The most common program causing this issue is Skype, which has an internal Web server of its own. Also, a few corporate desktop installs of Windows XP have Internet Information Server (IIS), Microsoft's Web hosting software, enabled by default. *These programs must be reconfigured or disabled for the Explorer Client to work properly, which may require Administrator privileges.*

If the user cannot reconfigure or disable the conflicting Web server, SecureDisc Explorer will then report the following error:

"SecureDisc Explorer cannot start the transparency server. Drive letter access will not be available."

SecureDisc Explorer will then provide a file list interface to allow copying of the encrypted files to another drive. Applications in the encrypted session will not function directly from the disc without the Transparency Server. Double-clicking on any file in the Explorer window will produce a dialog explaining this limitation.

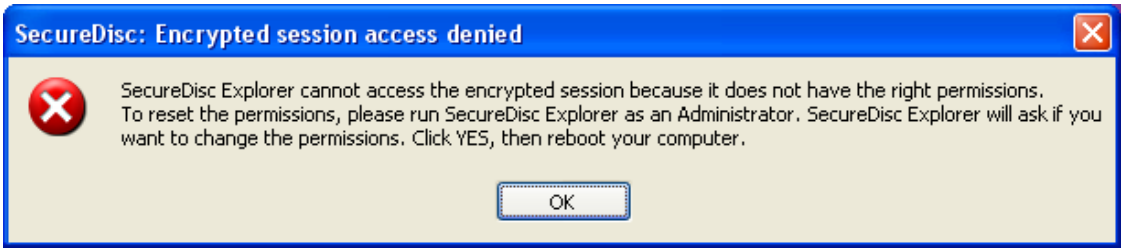
Windows 7 and later have an improved WebClient that will allow connections on any port, not just port 80, and so this limitation does not apply to them. The Resident Client will automatically detect the Windows version and use this feature when present.

Issue:

When attempting to decrypt a disc, my system displays one of the following dialogs regarding permissions. Why?

Administrative User:

Non-Administrative User:

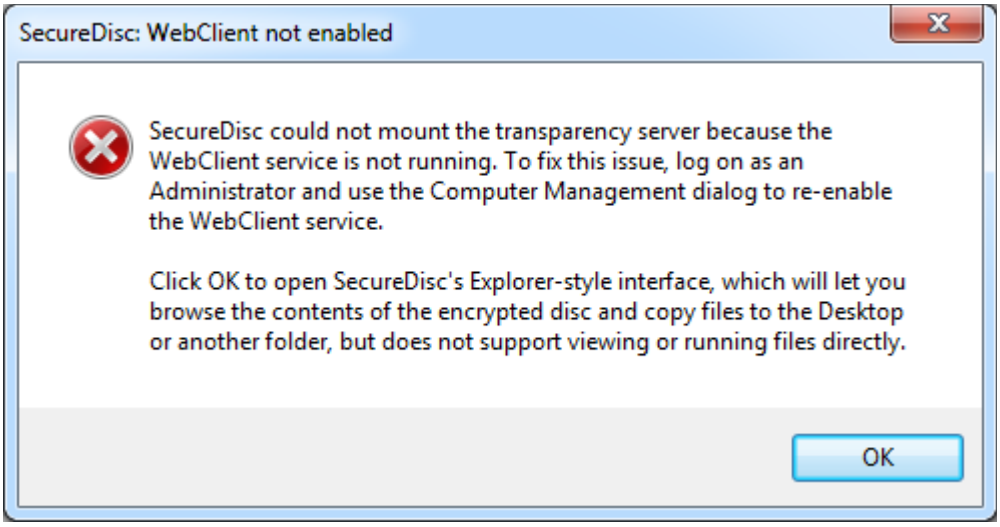


Resolution:

These messages only appear with discs encrypted using SDR versions before 2.5. Due to changes in the Client on Board implementation in SDR 2.5.1 and higher, the permission change these dialogs are warning about is no longer required unless you are using Explorer Client to read discs made with an older version of SDR.

If you do need to decrypt a disc encrypted with an older version of SDR, you are getting this message because SecureDisc Explorer requires write access to the CD/DVD device to work properly with these older discs. Clicking Yes on the Administrator version of this prompt will grant SCSI pass-through access on CD/DVD devices to *all users* on the computer, which may be a security risk. If this is unacceptable, we recommend using the Resident Client to read discs encrypted with older versions of SecureDisc.

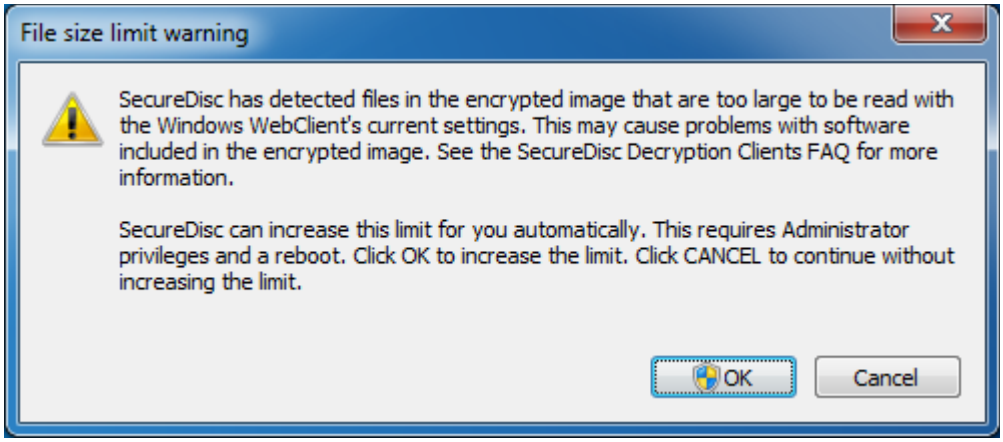
Issue:
When attempting to decrypt a disc, I see a dialog stating that WebClient is not enabled.



Resolution:
The Explorer Client uses its built-in Transparency Server to provide drive-letter access to the encrypted session. This requires the built-in Windows WebClient to be running as a service on the system. The WebClient service can be enabled by an Administrative user through the Computer Management dialog or the Services snap-in. Applications in the encrypted session will not function directly from the disc without the Transparency Server.

If you only need to access data files (and do not need to launch a viewer or other software directly from the disc), click OK to go to SecureDisc Explorer's list interface, which allows copying of the encrypted files to another drive.

Issue:
When accessing the contents of the encrypted disc, I see a SecureDisc Explorer file size limit warning dialog. Why?



Resolution:
Windows sets a default file size limit of approximately 47 MB (50,000,000 bytes) in the built-in WebDAV client used by our Transparency Server. This limit was chosen arbitrarily by Microsoft to prevent potential web-based security attacks when working with remote sites. If the WebDAV server attempts to transfer a file over the size limit, the client computer interprets this download as an error, and the download process fails. This can result in a variety of other errors when working with third-party applications launched from (or accessing files located in) the encrypted session, including I/O and 'access violation' errors. To resolve this issue, the SecureDisc Explorer Client scans the encrypted session once mounted and will produce one of these dialogs if it detects any file 47 MB or larger in the encrypted session.

If you are running the Explorer Client as an Administrator, if a file larger than 47 MB is present and if the Windows system file size limit is set to a value below the maximum allowed (4 GB), then the Explorer Client will show the first dialog. Answering “Yes” will make a one-time configuration change that will increase the maximum file size to approximately 4 GB. If approved, this change will require a system restart. Once completed, this change will allow all users on the local system to access larger files on SecureDisc encrypted discs via the Explorer Client.

If you are running the Explorer Client as a non-Administrator, and the conditions mentioned above are present, then the Explorer Client will show the second dialog and allow you to apply the configuration change described above.

Issue:
I get a message titled “SecureDisc: 'invalid address' bug detected.”

Resolution:
This error is caused by a faulty Windows network provider. The faulty provider is misinterpreting the mount request and returning this error instead of passing the request on to the next provider.

We have specifically found this issue with older versions of Novell's *NetIdentity* product, which ships with Novell Client for Windows XP. If you are using Novell Client on Windows XP, please upgrade to the latest version (4.91 SP5 as of this writing).

If the system is not running a Novell Client, there may be another web client ahead of WebClient in the Network Provider list that is incorrectly interpreting the mount request. Advanced users may choose to edit the System Registry (***always do so with caution as incorrect registry entries can cause serious Windows stability problems***) to move the WebClient entry in front of the other Network Providers.

The specific registry location in Windows XP is:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order\
ProviderOrder
```

Appendix A: Password retrieval using ODBC

Overview

With the optional ODBC access module, SecureDisc Rimage Edition can retrieve passwords from a local or remote database using Windows' built-in Open Database Connectivity (ODBC) support. This can be used along with user-defined merge fields to request a password without ever having to expose the plaintext password inside the merge file or the encrypted image.

The ODBC access module ships with SecureDisc Rimage Edition, but is licensed separately and is not enabled by default.

Activating the ODBC access module

To activate the ODBC access module, perform the following steps:

1. Open the SecureDisc Console and switch to the Encryption Tab.
2. Change the encryption method to “ODBC”. The ODBC Setup... button will become available.
3. Click on ODBC Setup... The odbcchooser dialog will appear.
4. Click on “Get License...” This will present the standard Discrete licensing applet, as described earlier in this document.
5. To generate a license request, click “Generate”. Send the resulting code by email to ***support@gtgi.com***. If you have already paid for the ODBC license, Discrete will return an activation code within 1 business day. If not, a Discrete sales specialist will contact you.
6. Paste the returned activation code into the bottom pane of the Discrete licensing applet, and click “Add Refill”.
7. Ensure that the status indicator in the odbcchooser window has turned green. If it has not, please contact Discrete for assistance.

Configuring the ODBC access module

Prerequisites

To access a database via ODBC, you must have the following items ready:

1. The type of SQL database in use (Microsoft SQL Server, Oracle, PostgreSQL, MySQL, etc.)
2. An ODBC driver for the SQL database. Windows typically ships with drivers for SQL Server, Access, and several flat-file formats. If you are not sure which ODBC driver to use, ask your system administrator.
    1. **Important note for 64-bit Windows users:** SecureDisc Rimage Edition is a 32-bit

application, and as such, requires the use of 32-bit ODBC drivers. A few databases, such as PostgreSQL, have 64-bit drivers available as an option, but they will not work properly with SecureDisc.

3. Login information for the database in question.
4. A query to use for retrieving a password. For more information on this topic, see "Constructing an SQL query" below.

Connecting to the database

To connect to a database:

1. If you were provided with a connection string by your system administrator, enter it in the connection string field and click the "Verify/Create..." button to ensure that it works properly. If it does, skip to "Constructing an SQL query" below.
2. If you do ***not*** have a connection string to use, make sure the connection string field is blank, and then click on the "Verify/Create..." button.
3. Odbcchooser will ask you if you want to use a DSN, or if you want to build a connection string especially for SecureDisc.
    1. Use the first option if you have a pre-defined connection you want to use. This will take you to the Windows Data Sources Control Panel, which will fill in a connection string based on the data in the DSN.
    2. The second option will build a connection string by querying the ODBC driver directly for what parameters it needs. This is recommended for advanced users and situations where a DSN is undesirable.
    3. To use the second option, select a driver corresponding to your SQL database and click OK. The ODBC driver's setup dialog will appear. Fill in the fields as per the instructions provided by your system administrator.
4. If a successful connection is made, the completed, verified connection string will appear in the connection string field.
5. Click OK to return to the SecureDisc Console.
6. Click OK or Apply to save your changes.

Constructing an SQL query

Any SQL SELECT query may be used, as long as it returns one column (which is expected to contain the password for the job in question).

The ODBC access module provides several keywords for use in queries. These keywords allow pertinent data from the job to be inserted into the query. All keywords start with a $ (dollar sign).

The keywords supported are as follows:

- $orderid – The current job's order ID, as provided by the submitter.
- $mediatype – The current job's media type (CDR, DVDR, etc.)
- $merge1-merge*nn*: Merge fields from the first record of the merge file. If no merge file is provided with the job, and any of these keywords are present, the job will fail.

An example of a conforming query is as follows:

```
SELECT password FROM scdpasswd WHERE branchname = '$merge4';
```

This query refers to a test table whose schema is

```
CREATE TABLE scdpasswd (
      branchname VARCHAR PRIMARY KEY,
      password VARCHAR NOT NULL
);
```

When a particular `branchname` is provided in merge field 4 of a job, it will be used to look up the matching password in the `scdpasswd` table. If the query returns no data, SecureDisc will handle the job as if it were given a blank password; see the Forced Encryption Mode section for more details.

More complex queries are possible; the only requirement is that the result contains only one column.

For more information on SQL syntax, contact your system administrator, or consult your SQL database's documentation.

End-User License Agreement

END-USER LICENSE AGREEMENT FOR GTGI SOFTWARE

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Global Technologies Group, Inc. (GTGI) for GTGI software product(s), which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. The SOFTWARE PRODUCT is licensed as follows:

Installation and Use. GTGI grants you the right to install and use a single copy of the SOFTWARE PRODUCT on your computer running an operating system for which the SOFTWARE PRODUCT was designed [e.g., Windows XP, Windows 7, etc.].

Backup Copies. You may make copies of the SOFTWARE PRODUCT as may be necessary for backup and archival purposes.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Maintenance of Copyright Notices. You must not remove or alter any copyright notices on all copies of the SOFTWARE PRODUCT.

Distribution. You may not distribute copies of the SOFTWARE PRODUCT to third parties.

Prohibition on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Rental. You may not rent, lease, or lend the SOFTWARE PRODUCT.

Transfer. You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA.

Support Services. GTGI may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by GTGI polices and programs described in the user guide, in "on line" documentation and/or other GTGI provided materials. Any supplemental software provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this EULA. With respect to technical information you provide to GTGI as part of the Support Services, GTGI may use such information for its business purposes, including for product support and development. GTGI will not utilize such technical information in a form that personally identifies you. Paid Support Services are bound to the original purchaser and are NON-TRANFERRABLE.

Not For Resale Product. If the Product is labeled “Not For Resale,” then you may not resell, or otherwise transfer for value, the SOFTWARE PRODUCT.

Compliance with Applicable Laws. You must comply with all applicable laws regarding use of the SOFTWARE PRODUCT.

3. TERMINATION. Without prejudice to any other rights, GTGI may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT.

4. COPYRIGHT. All title, including but not limited to copyrights, in and to the SOFTWARE PRODUCT and any copies thereof are owned by GTGI or credited sources. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by GTGI.

5. U.S. GOVERNMENT RESTRICTED RIGHTS. The SOFTWARE PRODUCT is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Global Technologies Group, Inc., 3108 Columbia Pike, Suite 301, Arlington VA 22204 USA.

6. NO WARRANTIES. GTGI expressly disclaims any warranty for the SOFTWARE PRODUCT. THE SOFTWARE PRODUCT AND ANY RELATED DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT REMAINS WITH THE END-USER.

7. LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, in no event shall GTGI or its affiliates be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE PRODUCT.

In any case, GTGI's entire liability under any provision of this EULA shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT. You are not authorized to use this software if your state or jurisdiction does not allow the exclusion or limitation of liability.

8. MISCELLANEOUS. This EULA is governed by the laws of the Commonwealth of Virginia, USA.

9. Contact. Should you have any questions concerning this EULA, or if you desire to contact GTGI for any reason, please contact Global Technologies Group, Inc., 3108 Columbia Pike, Suite 301, Arlington, VA 22204 USA.