

SecureDisc

Rimage Edition

Administrator's Guide

FOR USE WITH RELEASE 2.5 AND HIGHER

Automate. Secure. Deliver.



D I S C R E T E T E C H N O L O G I E S

www.discretetech.com ▪ sales@discretetech.com ▪ 703.310.6574 ▪ 3108 Columbia Pike | Suite 301 | Arlington VA 22204

Contents

Introduction	3
System Requirements	3
FIPS Information	3
Licensing Process	4
Software Download & Installation	5
Technical Notes	5
Encryption Password Integration	6
Encrypting with Rimage QuickDisc	8
Encrypting with Third-Party or Custom Applications	8
Encrypting Multiple Copies	8
Encrypting Spanned Data Sets	8
Forced-Encryption Mode	9
Handling Blank Passwords in Forced-Encryption Mode	9
Client on Board (CoB)	10
Automating the Customer Experience Using CoB	11
SecureDisc Console	12
SecureDisc Status Monitor	14
Software Activation & Image Packs	15
Software Deactivation & License Transfer	16
SecureDisc Clients Overview	17
SecureDisc Explorer Client	17
SecureDisc Resident Client	20
Troubleshooting Encryption Issues	22
Troubleshooting Decryption Issues	24
Copyright Information	29
End User License Agreement	30

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 Algorithm) module in CBC mode. The most popular SDR configuration ('Client on Board') creates a multi-session disc with both the encrypted data and an 'in the clear' (unencrypted) session containing 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
- 10 MB free disk space for program files
- Client application generating disc production jobs (e.g. QuickDisk or third-party software)

Disc Viewing:

Explorer Client

- Windows XP, Vista or Windows 7 (32-bit or 64-bit)
- DVD or CD reader
- Free disk space for caching the contents of the encrypted disc session

Resident Client

- Windows XP, Vista or Windows 7 (32-bit or 64-bit)
- 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.discretetech.com/FIPS>

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 Discrete Technologies (DT) 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.

DT 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

To be eligible for this option, customers must be running SecureDisc v.2.2 or later.

When replacing an older model with a new system, DT 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 DT. The customer will then send a Refill request from the new system after downloading and installing the demo version of SecureDisc software from [DiscreteTech.com/demos](#). DT 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 DT with documentation of system replacement by the manufacturer or an authorized service provider. Since the [Deactivation and License Transfer process](#) could not be completed, DT cannot validate the quantity of image licenses remaining on the system. Once the hardware change by the manufacturer has been verified by DT, DT 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 v1.x and Unlimited License Customers

DT no longer sells Unlimited licenses for any version of SecureDisc and no longer issues Image Pack refills for SecureDisc v1.x. Therefore, if a system with an Unlimited license must be replaced under scenario 2 above, the customer **must** upgrade to SecureDisc v2 (SAE customers are eligible for a 50% discount from the commercial price). DT 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.discretetech.com/demos>

Decompress the installer, launch the SDR installation program and 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](#).

Technical Notes

SDR version 2.5 introduces the following changes from all prior versions of the product:

- 1. SDR is no longer a 'plug-in' that operates within the Rimage Producer Software Suite (PSS) through the Rimage modifydisc.dll architecture. Instead, SDR is a Windows Service that processes jobs prior to PSS, then passes the modified job file to PSS for recording and printing. Consequently, there are some additional configuration options that must be set in order to properly trigger SDR to process job files. These are located in the new 'Trigger' tab in the [SecureDisc Console](#).**
- 2. In order for SDR to process jobs sent from XML API applications (including Rimage QuickDisc), SDR must make a change to the PSS configuration to moves the PSS services to a different communications port. This is completed automatically during SDR installation, but **REQUIRES A REBOOT AFTER SDR INSTALLATION IN ORDER TO COMPLETE SUCCESSFULLY.****
- 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.**

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 also creates an 'in the clear' (unencrypted) image to be recorded as a second session on the disc. This unencrypted session contains the contents of a special folder (by default, Rimage/SecureDisc/Client on Board) which typically 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)/DataPublisher (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*, the SecureDisc supported Formats are *Joliet*, *UDF 1.02* or *UDF 1.50*. Be sure you have selected one of these, the other Format options will not work with Client on Board encryption.
- Also 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.

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. Discrete Technologies recommends using the second method only as needed.

Client On Board (CoB)

SDR has the ability to record a non-encrypted session to an encrypted disc during processing. This function is enabled by default in version 2.13 and above. The non-encrypted session may contain the [SecureDisc Explorer Client](#) (which is included with SDR, and configured automatically), 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 that does not have the [SecureDisc Resident Client](#) software installed, the non-encrypted session is presented and allows the user to access the contents, including the [SecureDisc Explorer Client](#). Once the [SecureDisc Explorer Client](#) has launched, the user will be prompted for a password and the encrypted session will be accessible upon validation of the password value.

If the [SecureDisc Resident Client](#) has been installed on a computer, the non-encrypted CoB session will not be accessible and the user will automatically be prompted for a password as soon as the encrypted disc is detected by the [SecureDisc Resident Client](#).

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](#)).
- Enter a volume ID that Windows will use to identify the unencrypted session (16 character limit).
- Click on OK to save the settings and exit the Console.



The non-encrypted session will reduce the amount of available space on a blank disc by the size of the selected static folder content. The non-encrypted session is mastered in ISO9660 Level 2 with Joliet extensions, and cannot be changed. The non-encrypted session is exclusive of the format of the encrypted data.

NOTE ON SUPPORTED FORMATS: CoB is not currently supported with SDR 2.5 on any DVD format due to a lack of multi-session DVD support in Rimage PSS. This issue is being addressed by a Rimage Service Pack expected to be released in Q2 2011. See the [Troubleshooting Encryption](#) section for more information. CoB is never supported on DVD-R DL (Dual Layer), DVD+RW or BD-RE discs, due to format restrictions. SecureDisc will reject any attempt to record a CoB job to a DVD-R DL, DVD+RW or BD-RE disc.

NOTE ON RECORDING: Due to variations between recorders, we cannot guarantee that the CoB function will work properly if the encrypted session is very short (less than 600 kilobytes long). SecureDisc will write a warning message to the log if it detects a track that is too short. If you produce a disc with CoB enabled and the unencrypted session is unreadable, add more files to the encrypted session to bring it above 600 kilobytes.

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. Since this feature creates two distinct sessions on the disc, there are two parts to automating the user experience, which can be used depending on the disc contents and desired behavior.

Automating the Unencrypted Session

In Windows systems that do not have the [SecureDisc Resident Client](#) installed, Windows mounts the unencrypted session as a standard disc. The contents of the unencrypted session 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, SDR includes an `autorun.inf` file in the target path folder 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 Session

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 disc session 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 contents of the encrypted disc session were designed to launch automatically via `autorun.inf` in older versions of Windows, the user experience of the encrypted session will be identical to the behavior of the same data on an unencrypted CD launched in Windows 95.

Since many discs do not contain `autorun.inf` in the encrypted session 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 session files using instructions provided in the unencrypted session `autorun.inf` file.

This method allows a specific file or application to be launched automatically from the encrypted session 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 session) 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...

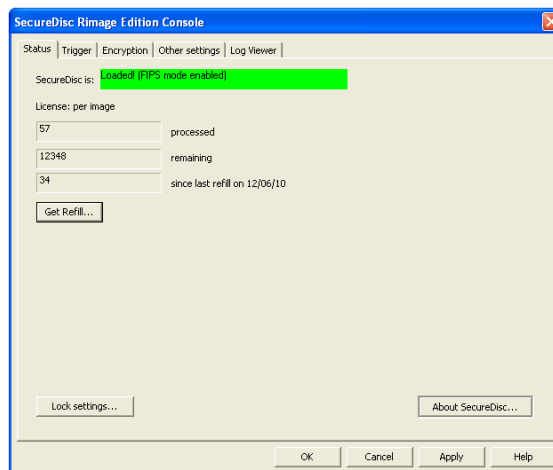
- Click this button to generate a refill request code. Refer to [Software Activation & Image Packs](#) section for more information

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



Trigger tab

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] **Contact Discrete to enable this Expansion Module**

- Enables monitoring a target folder to process Network Publisher (.NWP) and/or Data Publisher (.ORD) production orders directly. This Expansion Module provides direct processing of .NWP and/or .ORD production order files through SDR by designating a target folder to monitor.

PowerTools Emulation [Default status: Disabled] **Contact Discrete to enable this Expansion Module**

- Enables monitoring a target folder to process .IOF/.POF production orders directly. This Expansion Module provides direct processing of .IOF/.POF production order files through SDR by designating a target folder to monitor.

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

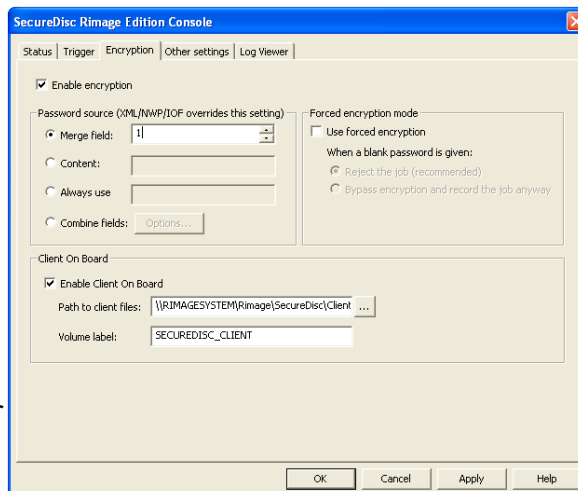
Enable Encryption [Default status: Enabled]

- 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 [Client On Board](#) section for further information.

Other settings tab

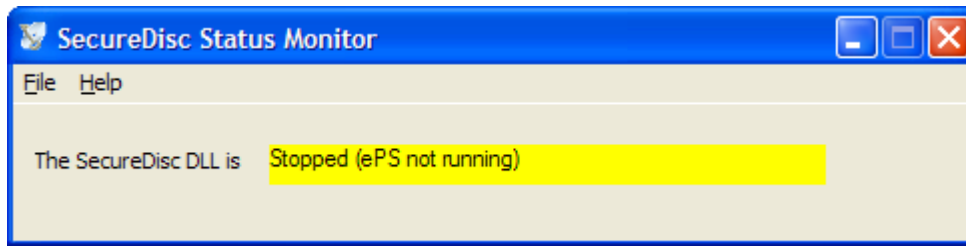
Network Logon Information [*Prior versions: Replaces the 'Modifydisc.dll Logon Information' function*]

- 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 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*
- Visit DiscreteTech.com/activation and paste the request code into the request form. Alternatively, paste the XML Request block into an email with your contact information and send to admin@discretetech.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*

SecureDisc 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>yeXdNftLTQApX5rLUXHl/G2M9mK8gcOzt5zMOmNmYNQD8=</FileID>
<RegData>YHlAGNEHlyb7JxDrS0AmvRpuwKJ1Sw62SCIN8G5CYhai8rn3uAac/XS3JxFoC
<RegStats>n3f2T17AFAZngTyBwgPdjIHdVIX9NYpujC14WwJ2PxHvCyl1yOqX1bvAOPX
</GTGIRegFile>
```

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

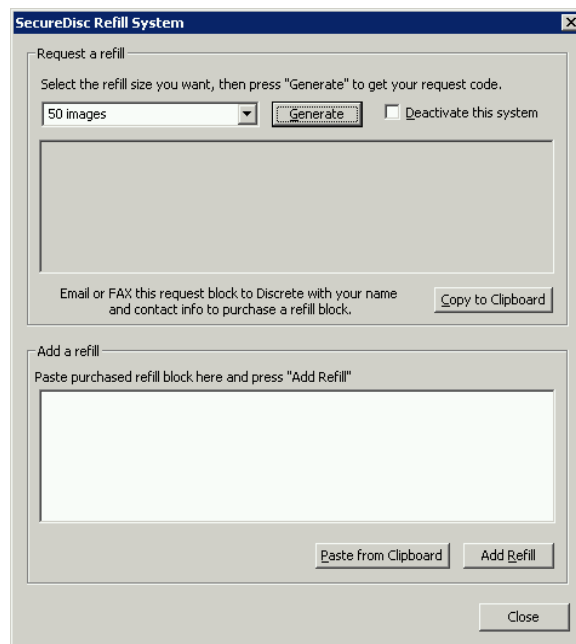
Add a refill

Paste purchased refill block here and press "Add Refill"

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*
- Visit DiscreteTech.com/activation and paste the request code into the request form. Alternatively, paste the XML Request block into an email with your contact information and send to admin@discretetech.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 www.discretetech.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](#).

Beginning with SDR version 2.13, 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 Transparency Server function in the Explorer Client and require the Resident Client to fully interact with the encrypted disc session. For this reason, SDR v2 customers 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 2000, XP, 7 and Vista (both 32-bit and 64-bit) 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.

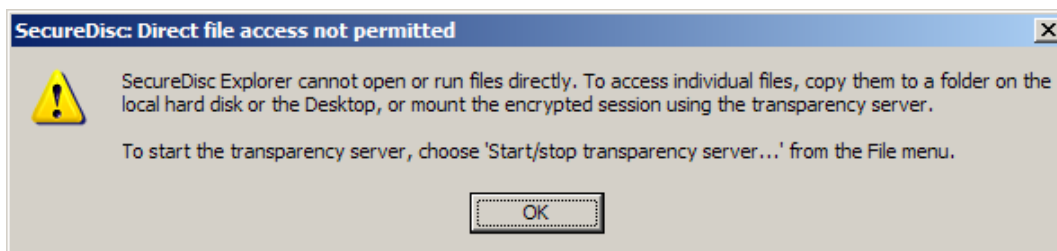
* For encrypted discs that contain individual files larger than 47 MB that need to be accessed from an application launched directly from the disc using our Transparency Server, all Windows versions require a one-time permissions change (which requires Administrator log-in) to increase the default web folder file size. Also, Windows XP default permissions may prevent non-Administrator users from fully accessing the optical drive, preventing decryption of the disc by a non-Administrator unless this permission is changed. 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 (SCDEplorer.exe) is typically present on the unencrypted ("in the clear") session of a disc produced by SDR using the Client on Board feature (unless the SCDEplorer.exe file is manually removed from the folder designated in the 'Path to Client Files' location of the [SecureDisc Console](#)). The default configuration in SDR 2.13 and greater includes 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 SCDEplorer.exe. The Explorer Client will start, check the disc and present a login box, similar to the one used in the Resident Client. 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 just as 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*: Un-mounts 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, un-mounts 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. This requirement will become more common as older PCs with the Resident Client installed are replaced with newer 64-bit Windows systems that cannot utilize the Resident Client. If customers are retaining older encrypted discs there may be a need to read an encrypted disc that Windows will not recognize since the disc has no Client on Board session for Windows to mount.

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 `SCDEplorer.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 `SCDEplorer.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, Vista and 7 (32- and 64-bit) 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.

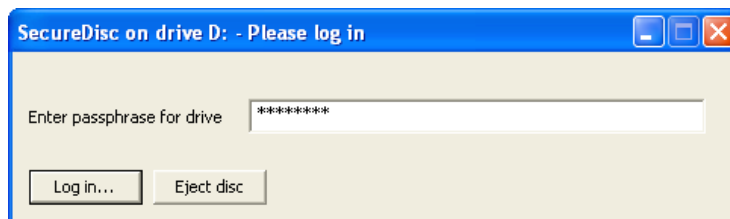
Resident Client Installation

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

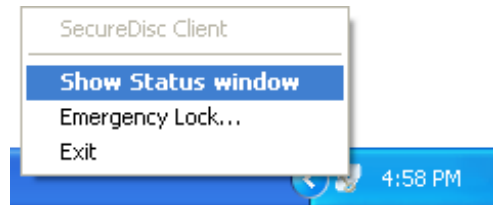
To read an encrypted disc, load the disc into an available reader. The Resident Client will automatically open and prompt for the password. Enter the password and click on Log In. To cancel password entry, click on Eject Disc.



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

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](#). For third-party applications producing Network Publisher (NWP format), Data Publisher (ORD format) or PowerTools (IOF/POF) production orders, purchase the appropriate Expansion Module and select the correct folder to monitor for incoming production orders.
2. Confirm that the *Enable encryption* box is checked on the *Encryption* tab.
3. Confirm that SecureDisc is Active (green) in the *Status* tab.

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 DVD production job generates an error [222] "Only one track can be recorded on a DVD".

Resolution:

Rimage PSS does not support recording a second session on DVD media, a necessary feature for utilizing the [Client on Board](#) feature. Disabling [Client on Board](#) will allow a DVD to be encrypted without an 'in the clear' session that includes the decryption client. This issue is being addressed by a Rimage Service Pack expected to be released in Q2 2011. Discrete Technologies has already tested the fix included in the Rimage Service Pack and confirmed that it corrects this issue, eliminating the error. Please contact Discrete Technologies for more information about this issue.

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 Canceled 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@discretetech.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?

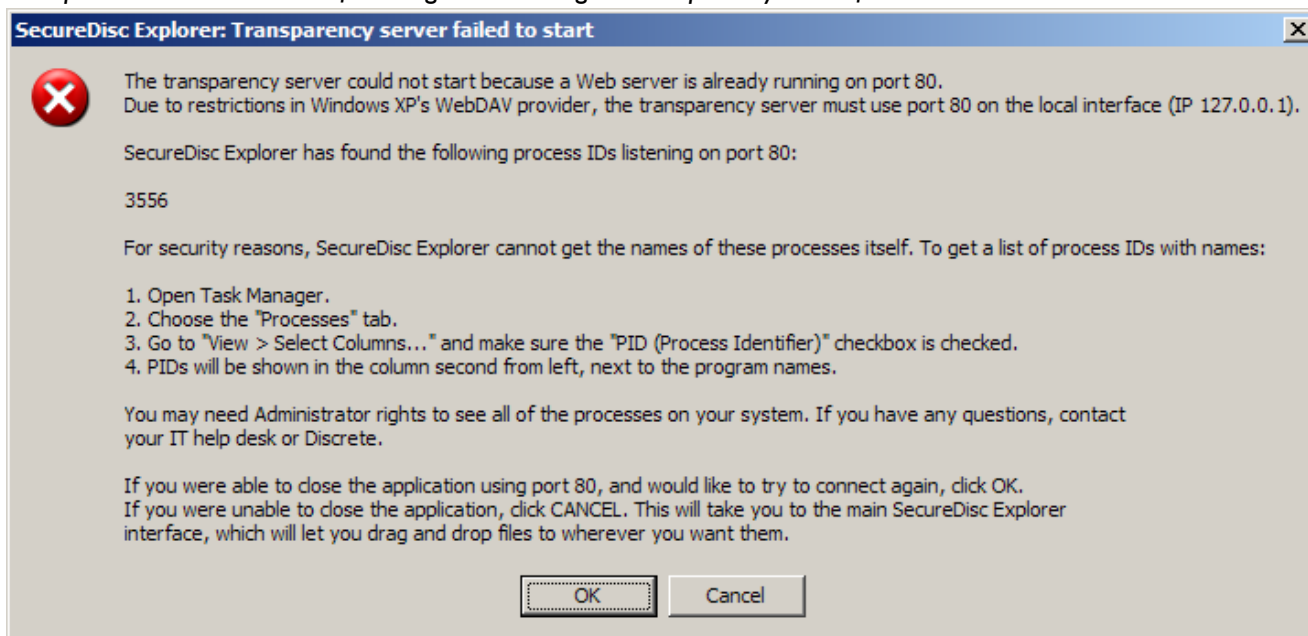
Resolution:

SecureDisc versions prior to 2.5 operated as a 'plug-in' to Rimage Production Server and consequently required a Production Server restart whenever certain SDR settings changes were made. Beginning with version 2.5, many SDR settings changes no longer require a Production Server restart. However, if a change requires a Production Server or system restart, you will be prompted accordingly.

Troubleshooting Decryption Issues

Issue:

The Explorer Client returns the following error message: “Transparency server failed to start”



Resolution:

The Explorer Client uses its built-in Transparency Server to provide drive-letter access to the encrypted session. Due to limitations in Windows' built-in WebDAV redirector, the Transparency Server *must* use port 80. The user can check Task Manager to find the Process ID number reported in the error message and close or uninstall the application (as applicable). Although very few desktop machines have a Web server installed by default, the most common are:

- *Internet Information Server (IIS)*, which is included with some versions of Windows. Stopping *IIS* requires Administrative privileges. Become an Administrator, then open a Command Prompt and type: `net stop w3svc` This will stop *IIS* and allow you to use the Explorer Client's WebDAV server. You may also remove *IIS* entirely, using the Control Panel. Instructions on how to do this vary, depending on which version of Windows you are running; see your Windows documentation for details.
- *Skype* can also be configured to use Port 80 for incoming connections which can conflict with the Explorer Client when both are running. *Skype* can be closed to eliminate the conflict, or it can be reconfigured as follows: Under **Tools > Options > Connections** or **Tools > Options > Advanced > Connection** de-select the option "Use ports 80 and 443 for incoming connections." Click Save and restart *Skype* to enact the change.

If the user fails to stop the conflicting Web server, SecureDisc Explorer will then report the following error:

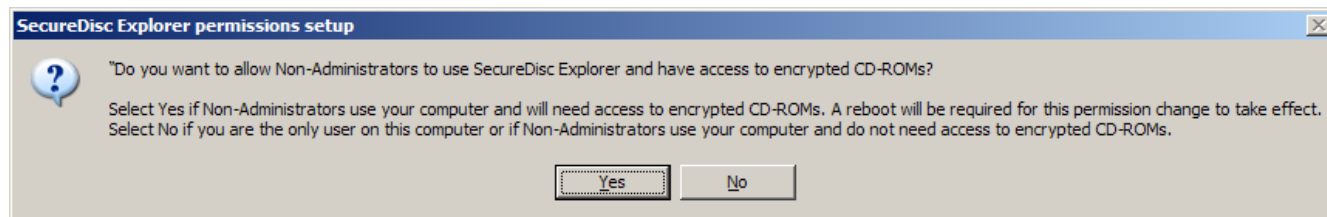
"SecureDisc Explorer cannot start the transparency server. Drive letter access will not be available."

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

[section continues]

Issue:

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



Non-Administrative User:



Resolution:

The Explorer Client requires direct device access to work, since it bypasses the Windows file-system layer entirely and reads the disc using raw SCSI commands. In Windows XP, the default permissions on CD-ROM class devices (which, despite the name, also includes more modern drives such as DVD recorders and Blu-Ray drives) are set to allow only Administrators direct access to the drive.

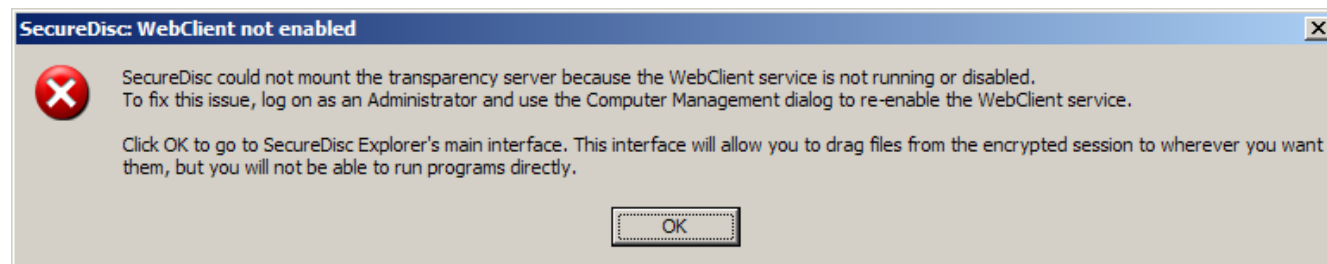
If you are running the Explorer Client as an Administrator on Windows XP machine with permissions set to defaults, then the Explorer Client will show the first dialog. Answering "Yes" will set new default permissions on the CD-ROM class which allows non-Administrators to access the local machine's optical drives directly. This *only* applies to CD-ROM class devices, as defined by Microsoft, and *will not* change permissions on your hard drives or any network shares. *You may need to reboot after applying the new permissions.*

If you are running the Explorer Client as a non- Administrator a Windows XP machine with permissions set to defaults, then the Explorer Client will show the second dialog. Clicking OK will close the Explorer Client, since access to the encrypted data is not possible on that PC without a permissions change.

Windows Vista and Windows 7 have more relaxed default permissions for CD-ROM class devices, and so neither of these messages should appear on a Windows Vista or Windows 7 machine unless the default device permissions were changed by an Administrator to restrict use of the optical drive/s in the local machine.

Issue:

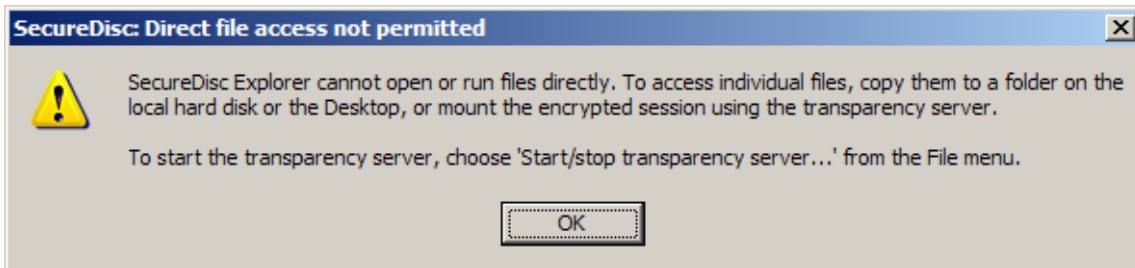
When attempting to decrypt a disc, I see a dialog stating that WebClient is not enabled.



[section continues]

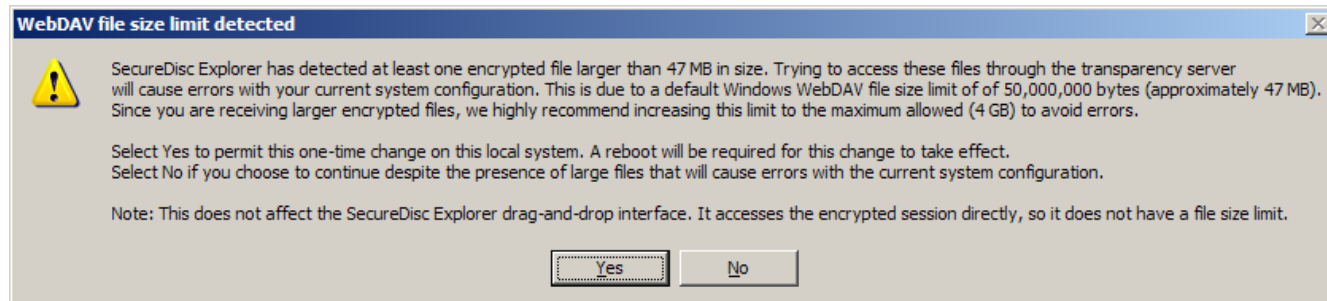
Resolution:

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. Since the Transparency Server cannot be mounted, clicking OK will produce a simple file list interface to allow copying of the encrypted files to another drive. Any applications or other executables in the encrypted session will not function directly from the disc without the Transparency Server. Double-clicking on any file in the SecureDisc Explorer window will produce the following dialog explaining this limitation:

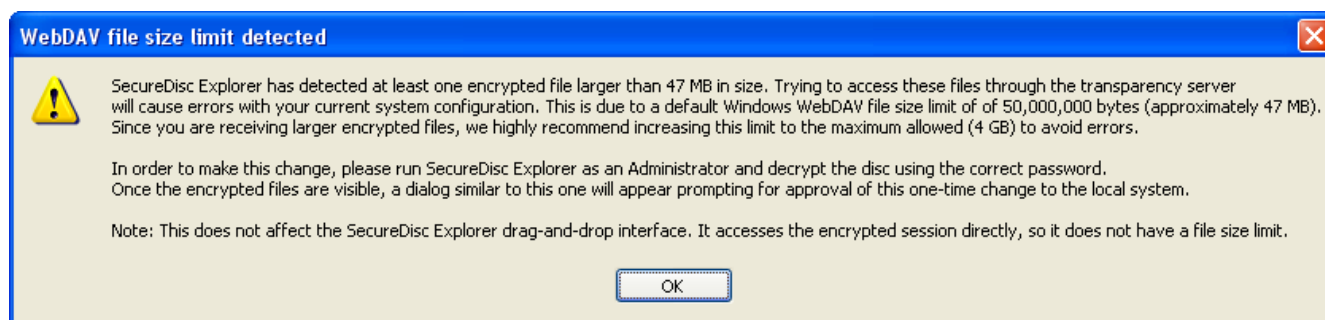


Issue:

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



Non-Administrative User:



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 (such as Explorer Client and/or a third-party application trying to copy a 47 MB or larger file from the encrypted session to another location), the client computer interprets this download as a denial of service attack and the download process fails. This can result in a variety of 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, a file larger than 47 MB is present and 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 set new default permissions to approve a one-time local registry change that will increase the maximum file size to approximately 4 GB. If approved, this change will require a system restart. It will only need to be made once and 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, a file larger than 47 MB is present and the Windows system file size limit is set to a value below the maximum allowed (4 GB), then the Explorer Client will show the second dialog.

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

Issue:

When using the Client on Board feature, the encrypted disc appears to be blank and no files are visible.

Resolution:

Due to variations between recorders, we cannot guarantee that the [Client on Board](#) function will work properly if the encrypted session is very short (less than 600 kilobytes long). If you produce a disc using Client on Board and the unencrypted session is unreadable, add more files to the encrypted session to bring it above 600 kilobytes. If the encrypted session is already larger than 600k but the disc is still unreadable and you are using QuickDisc to produce it, the primary cause is improper setting of the *Use Power Image* check box (in the *Disc* settings window). This check box has three possible states: checked, shaded or cleared (white). SecureDisc will only function on the cleared setting.

Copyright Information

Copyright © 2006 - 2010 Discrete Technologies LLC. All rights reserved.

SecureDisc Rimage Edition Administrator's Guide

The instructions given in this manual are generalized for installation on most Rimage models. While every effort has been made to describe any differences in machines, not all installations and their variables can be addressed in this documentation. If problems are experienced while installing this product, or if any questions arise about its operation, please contact us.

Discrete Technologies LLC cannot be held responsible for loss of data as a result of the use of this product, or guarantee the fitness of this product for a particular purpose other than what is described in this document.

To report errors or omissions in this manual, contact us at (703) 310-6574 or send an email to support@discretetech.com.

This manual, as well as the software described in it, is furnished under license and may only be used or copied in accordance with the terms of such license. The information contained in this manual is furnished for informational use only and is subject to change without notice.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior permission of Discrete Technologies, Inc.

SecureDisc is a trademark of Discrete Technologies LLC.

Microsoft, Windows, Windows XP, Windows Vista and Windows 7 are registered trademarks of Microsoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

This document and the software it describes are produced exclusively in the United States of America.

Twentieth Edition

December 2010

Software Version 2.5 and higher

Explorer Client version 1.2.6 and higher

Resident Client version 2.3 and higher

End-User License Agreement

END-USER LICENSE AGREEMENT FOR DISCRETE TECHNOLOGIES LLC SOFTWARE

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Discrete Technologies LLC (DT) for DT 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. DT 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. DT may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by DT policies and programs described in the user guide, in "on line" documentation and/or other DT 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 DT as part of the Support Services, DT may use such information for its business purposes, including for product support and development. DT 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, DT 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 DT 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 DT.

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 Discrete Technologies LLC, 3108 Columbia Pike, Suite 301, Arlington VA 22204 USA.

6. NO WARRANTIES. DT 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 DT 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, DT'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 DT for any reason, please contact Discrete Technologies LLC, 3108 Columbia Pike, Suite 200, Arlington, VA 22204 USA.