

SecureDisc

PC Edition User's Guide



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

Contents

Introduction	3
Installation	3
Software Activation & Image Packs	4
Using SecureDisc PC Edition	5
Client on Board (CoB)	6
SecureDisc Clients Overview	7
SecureDisc Explorer Client	7
SecureDisc Resident Client	9
Troubleshooting Decryption Issues	11
Copyright Information	16
End User License Agreement	17

Introduction

SecureDisc PC Edition (SDPC) is used for protecting and preventing access to content recorded on CD and DVD. Using 256-bit AES (Advanced Encryption Algorithm), SDPC encrypts the entire contents of any ISO or UDF disc image. SDPC is comprised of two parts: a drag-and-drop disc burning application that encrypts the disc image using the password provided; a “client” driver and helper application that is installed on the receiver’s computer to decrypt (read) the encrypted disc.

Requirements

Disc Creation:

- Windows XP, Vista or 7 (32-bit or 64-bit)
- 10MB free disk space for program files
- MMC Compliant DVD, CD, or BD-R recorder (most modern models)

Disc Viewing Client:

- Windows XP, Vista or 7 (32-bit or 64-bit)
- DVD or CD reader
- 1 MB free disk space for program files

Modes of Operation

- 256-bit Advanced Encryption Standard in CBC mode

FIPS Information

- SDPC contains an embedded, FIPS 140-2 validated encryption module
- For specific FIPS information, visit **DiscreteTech.com/FIPS**

Package Contents

- SDPC installation CD
- This Manual

Licensing

- SDPC is licensed for use on a single computer, and is sub-licensed on a per-encrypted-image basis
- SDPC clients may be distributed freely

Installation

Run the SDPC installation program and follow the wizard’s on-screen instructions. By default, only 10 encrypted images will be available. To purchase additional image packs, see “Software Registration & Image Packs.”

Software Activation & Image Packs

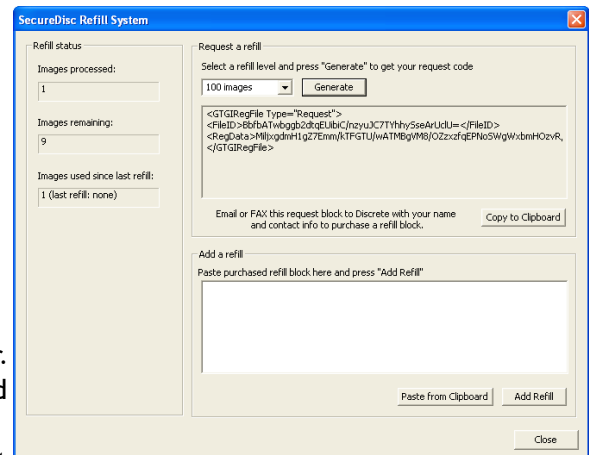
Encrypted discs produced using SDPC incur a per-encrypted-image charge. SDPC keeps a running count of encrypted images produced, and a total of purchased encrypted images available. The initial installation of SDPC includes a Qty. 10 encrypted image pack. Additional encrypted Image Packs (“refills”) may be purchased separately and applied at any time.

Encrypted Image Pack refills may only be used on the computer 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 a request code.

To register SDPC, 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 and to receive a unique serial number. If the software has been paid for, you will not be contacted by a sales representative.

Applying a Purchased Encrypted Image Pack

- Open SecureDisc
- Select *Tools* from the menu
- Click on *Refill status...*
- Select the number of refill images you want to purchase and click on *Generate*
- Click on *Copy to Clipboard*
- Paste the XML Request block into an email with your contact information and send to admin@discretetech.com. Put SDPC Refill in the Subject line along with your assigned serial number. Alternatively, visit **DiscreteTech.com/activation** and paste the request code and serial number
- A sales representative will contact you for payment information. Once your payment has been processed, a Refill code will be e-mailed to you
- Paste the refill code from the e-mail into the lower block
- Click on *Add Refill*



Using SDPC PC Edition (SDPC)

SDPC works similar to most disc burning software. Drag-and-drop the files you want to record into the tree area (left side) of the SDPC window. You may drop files, folders, or a combination of both. The status bar at the bottom of the window shows the size of the data you have dropped in.

Select the media type you want to use by clicking on *Media and image settings*. SDPC supports CD-R and RW, DVD±R and RW, DVD±R-DL (dual layer), and BD-R (25GB Blu-Ray Recordable). The disc format may also be selected. *Universal Hybrid* is the default and is universally compatible. Other selectable formats include ISO Level 1 and ISO Level 2 (no Joliet).

To encrypt the disc check the Encryption enabled option and enter a passphrase. Passphrases may be up to 255 characters; special characters are allowed. Discs that are not encrypted do not count against the encrypted image count.

To change the Volume ID, right-click on the disc icon at the top of the list and choose *Rename*.

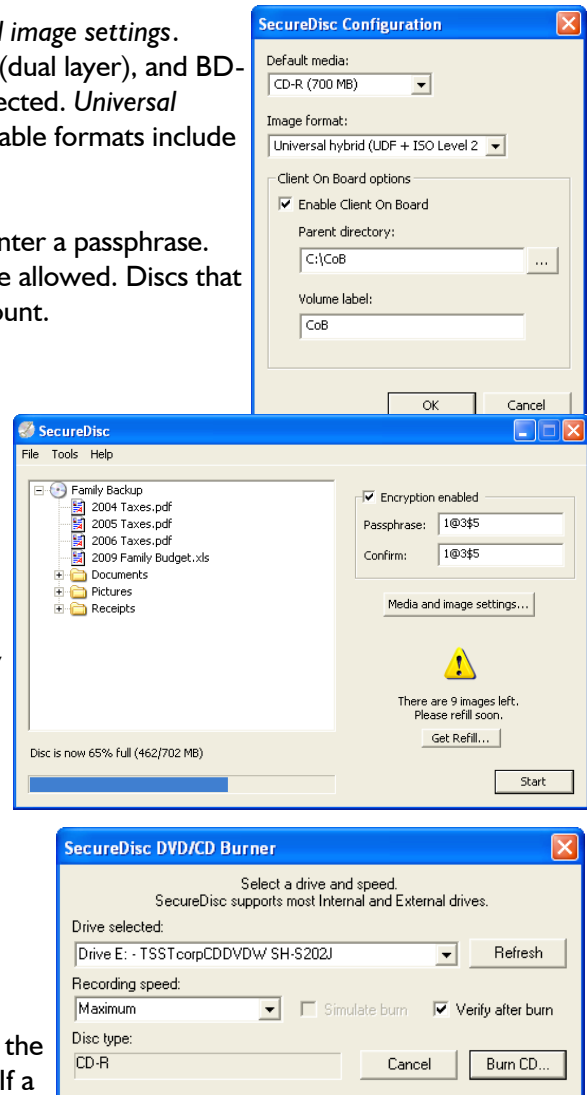
Click on Start to begin disc processing. SDPC will prepare and encrypt the data to be recorded. Once the disc information has been processed, you will be presented with the SDPC burning dialog.

SDPC does not modify source files. SDPC creates a temporary copy of the data set, encrypts it if requested, and burns the temporary data to the disc.

To burn the disc, select the recorder from the Drive selected list and click on Burn.

Simulate burn simulates the recording process without recording to the blank disc. *Verify after burn* verifies that the recorded disc matches the data that was recorded.

Burning progress is displayed in the status bar at the bottom of the main window. To cancel a process, click on the Cancel button. If a process cannot be stopped, the Cancel button will not appear.



Client On Board (CoB)

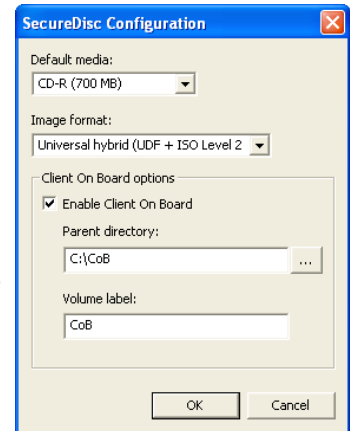
SDPC has the ability to record a non-encrypted session to an encrypted disc during processing. This function is enabled by default in version 2.4 and above. The non-encrypted session may contain the Explorer Client (which is included with SDR, and configured automatically), the Resident Client installer (if desired), and other static files that do not need to be secured (such as user documentation, disclaimers, etc.).

When an encrypted disc made with the CoB feature is inserted into a computer that does not have the Resident Client software installed, the non-encrypted session is presented and allows the user to access the contents, including the Explorer Client. Once the 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 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 Resident Client.

To use Client On Board, enable the option in SDPC settings by clicking on *Media and image settings*. Select the parent folder that contains the static content to be included. Be sure to include the SDPC Client installer in the folder. Set a volume ID (16 character limit).

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 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.



SDPC Clients Overview

In order to view discs encrypted with SDPC, the user must utilize a SecureDisc Client software application. There are two SecureDisc Clients: the Explorer Client and the Resident Client.

Beginning with SDPC version 2.3, the SecureDisc Explorer Client is included in the SDPC 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 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.

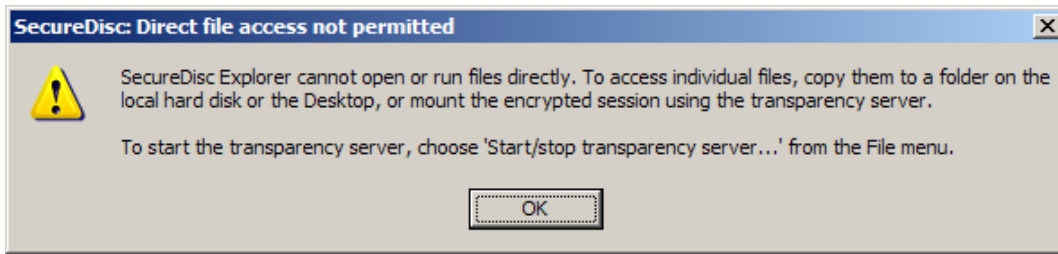
* For encrypted discs that contain individual files larger than 47 MB that need to be accessed from an application launched directly from the disc using our Transparency Server, all Windows versions require a one-time permissions change (which requires Administrator log-in) to increase the default web 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 (SCDExplorer.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 SCDExplorer.exe file is manually removed from the folder designated in the 'Path to Client Files' location of the SecureDisc Console). The default configuration in SDPC 2.4 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.

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, 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 SDPC Explorer window will produce this 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 SDPC logo will appear in the system tray, next to the clock. Double-click on the SDPC 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 SDPC v1 encrypted discs

This procedure is used in cases where a customer wants to read encrypted discs that were produced with SDPC v1 (or SDPC 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 SDPC 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 SDPC 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 Resident Client is compatible with Windows 2000, XP, Vista and 7 (32-bit ONLY) 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 SDPC 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, SDPC 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.

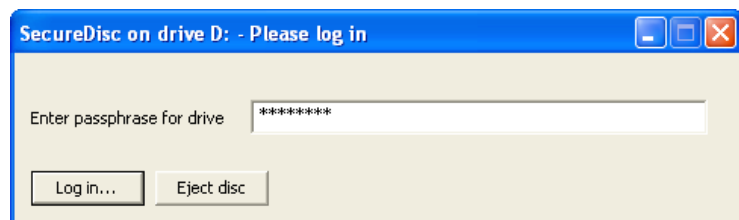
Resident Client Installation

Run the Resident Client installation program and follow the wizard's on-screen instructions. Administrative rights are required for installation, however, once installed the Resident Client is available for all local 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 SDPC 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.

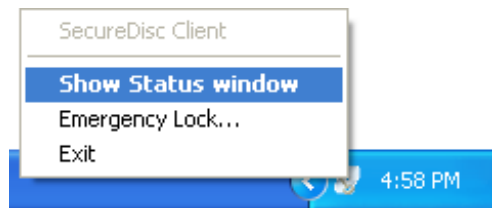


If an incorrect password is entered, the disc is automatically ejected and the client login window is closed. The Resident Client has no settings that require configuration. The Resident Client loads at system startup into the

system tray, next to the clock.

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

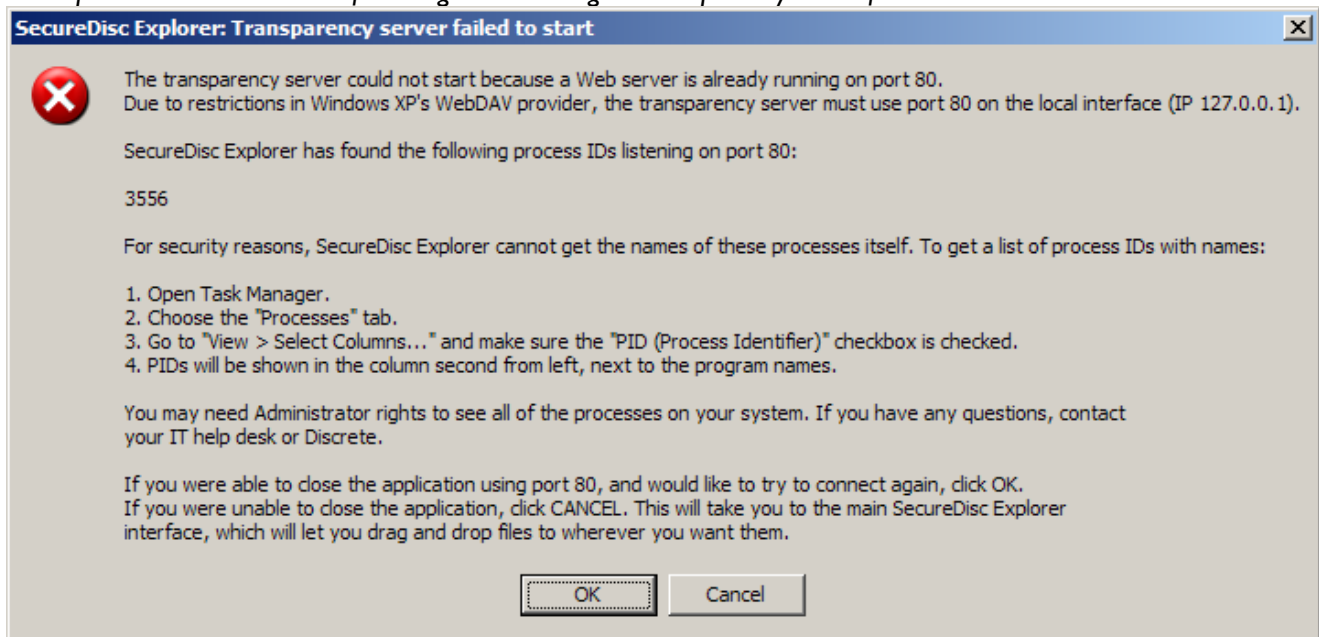
- *Show Status Window* displays the drives available and whether they contain an encrypted disc
- *Emergency Lock...* ejects all discs currently logged in and clears the password from memory. Ejecting a disc by any means automatically logs out the disc and clears the current password.



Troubleshooting 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, SDPC Explorer will then report the following error: "SecureDisc Explorer cannot start the transparency server. Drive letter access will not be available."

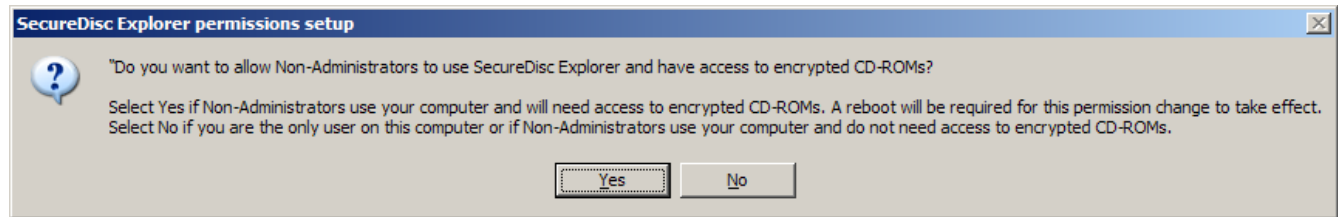
The Explorer Client will then provide a simple file list interface to allow copying of the encrypted files to another drive. Any applications or other executables in the encrypted session will not function directly from the disc without the Transparency Server. Double-clicking on any file in the SecureDisc 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 2000 and 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.

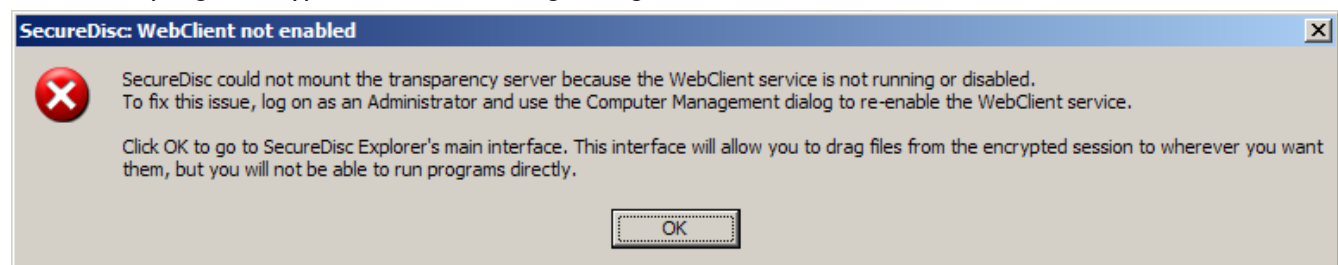
If you are running the Explorer Client as an Administrator on a 2000 or XP machine, and the permissions are set to defaults, then the Explorer Client will show the first dialog. Answering "Yes" will set new default permissions on the CD-ROM class which allows non-Administrators to access the local machine's 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 on a 2000 or XP machine, and the permissions are 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 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 will appear on a Windows Vista or Windows 7 machine.

Issue:

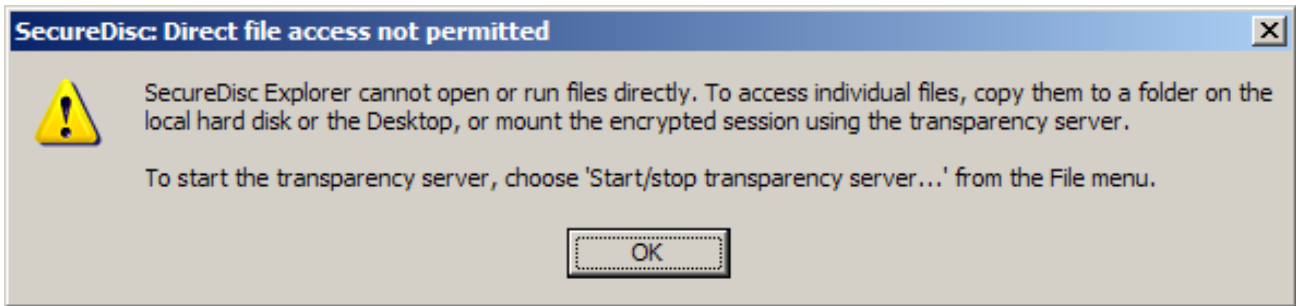
When attempting to decrypt a disc, I see a dialog stating that WebClient is not enabled.



[section continues]

Resolution:

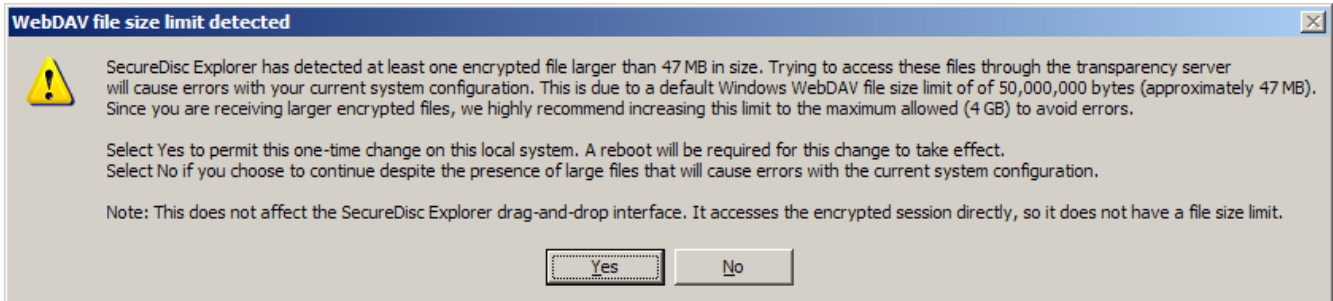
The Explorer Client uses its built-in Transparency Server to provide drive-letter access to the encrypted session. This requires the built-in Windows WebClient to be running as a service on the system. The WebClient service can be enabled by an Administrative user through the Computer Management dialog. 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 SDPC Explorer window will produce the following dialog explaining this limitation:



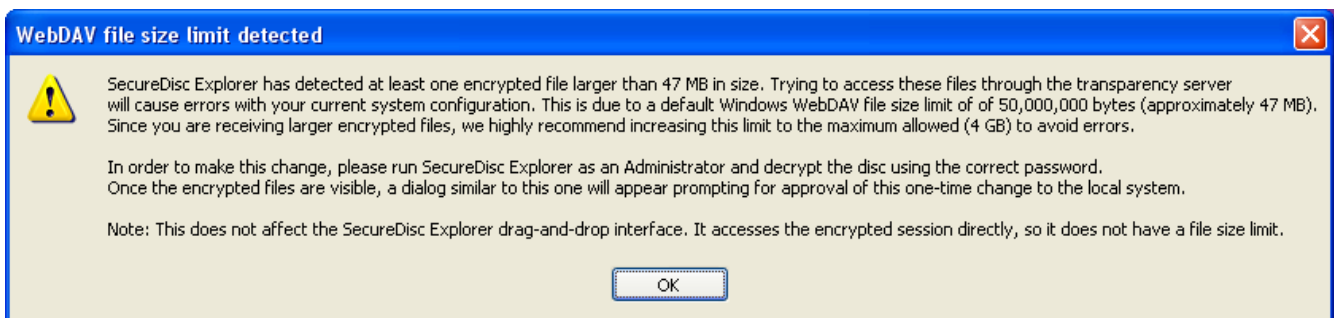
Issue:

When accessing the contents of the encrypted disc, I see a SDPC 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 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 the encrypted session, including I/O and 'access violation' errors. To resolve this issue, the SDPC 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 SDPC 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

SDPC Utilities

Reading a Disc Track

SDPC can read and save disc tracks as ISO images:

- Click on Tools then Read Image from Disc to access the Read Tracks window
- Select the reader from the Drive selected list
- Click on the desired track
- Enter a destination path and file name for the track in the Save track as box
- Click on Read disc
- Track read status is displayed in the status bar at the bottom of the main window

Recording a Disc Track

SDPC can record ISO images directly to the recorder:

- Click on Tools then Burn Image to Disc
- Select the disc image you want to record
- Select the recorder from the Drive selected list and click on Burn
- Burning progress is displayed in the status bar at the bottom of the main window

Encrypting a Disc Track

SDPC can encrypt an existing ISO image and optionally record it. SDPC saves the encrypted image as a separate file, and does not modify the source image.

- Click on Tools then Encrypt Image
- Select a Source Image
- Select the Encrypted Image to save as
- Select a Passphrase
- Click on OK
- Encryption status is displayed in the status bar at the bottom of the main window

Decrypting or Verifying a Disc Track

SDPC can verify or decrypt an existing encrypted ISO image. SDPC saves the decrypted image as a separate file, and does not modify the source image.

- Click on Tools then Decrypt Image
- Select a Source Image
- Select the Decrypted Image to save as
- Select a Passphrase
- Click on OK
- To only perform image verification, select Verify only
- Status is displayed in the status bar of the main window

Copyright Information

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

SecureDisc PC Edition User's Guide

The instructions given in this manual are generalized for installation on most servers. 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.

Seventh Edition

August 2010

Software Version 2.4 and higher

Explorer Client version 1.2.5 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 2000, Windows XP, 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, Second Floor, 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, Second Floor, Arlington, VA 22204 USA.