Secure*Disc*

Decryption Guide

Automate. Secure. Deliver.

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

Contents

Introduction

SecureDisc is used for protecting and preventing access to content recorded on CD, DVD and/or Blu-Ray media. SecureDisc 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 SecureDisc mode ('Client on Board') creates a multi-session disc containing both the encrypted data and an 'in the clear' (unencrypted) session containing files that are accessible prior to decryption.

System Requirements

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
- Administrative privileges may be required on some Windows systems to access the encrypted disc and/or utilize the SecureDisc Transparency Server

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
- Administrative privileges for initial installation

FIPS Information

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

SecureDisc Clients Overview

In order to view the encrypted contents of discs produced with SecureDisc, the user must utilize a SecureDisc Client software application. There are two SecureDisc Clients: the Explorer Client and the Resident Client. Each has different requirements and decrypts the disc using a different process. Most discs encrypted with newer versions of SecureDisc contain an 'in the clear' (Windows mountable) session containing the Explorer Client. In most cases, this makes installation of the Resident Client unnecessary. However, in rare cases of certain Windows configurations there may be a need to install the Resident Client in order to fully interact with the encrypted disc contents.

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 SecureDisc using the Client on Board feature. This session also contains 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 SecureDisc Explorer window will produce this dialog explaining the limitation:
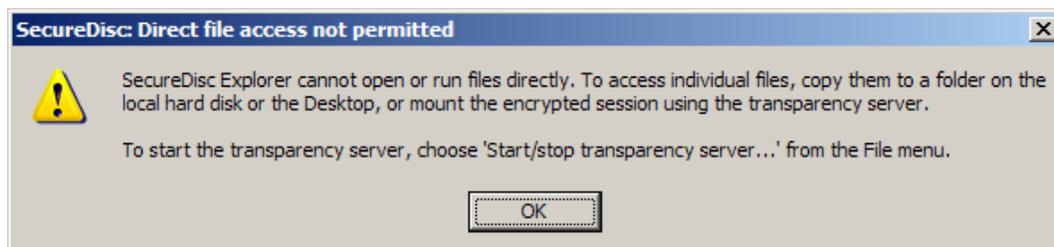
The Transparency Server

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 SecureDisc logo will appear in the system tray, next to the clock. Double-click on the SecureDisc logo to restore the Explorer client window, or right-click for more options:
  - *Restore*: Restores the Explorer Client window.
  - Start/stop transparency server: Unmounts the drive letter being used for encrypted-disc access, then stops the Transparency Server. *Make sure any files and folders on the drive letter are closed before using this option.*
  - *Exit:* Closes the Explorer Client, unmounts and stops the Transparency Server, and ejects the disc.

Using the Explorer Client to read SecureDisc v1 encrypted discs

This procedure is used in cases where a customer wants to read encrypted discs that were produced with SecureDisc v1 (or SecureDisc v2 with the Client on Board feature disabled), and do not have a Resident Client installed on their system. This requirement will become more common as older PCs with the Resident Client installed are replaced with newer systems or upgraded to a new O/S. 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 SCDExplorer.exe file to any location on the local PC (such as the Windows Desktop)
  3. Remove the Client on Board disc and place the older encrypted disc in the drive.
  4. Double-click on the SCDExplorer.exe application to launch it.
  5. The Explorer Client will search all local optical drives for a SecureDisc encrypted session and when located, will automatically prompt for the password.
  6. Once logged in, the Explorer Client will attempt to mount a built-in Transparency Server to provide full drive letter access to the encrypted session. Please refer to the Troubleshooting Decryption Issues section for any issues that may arise.

SecureDisc Resident Client

The SecureDisc Resident Client is compatible with Windows XP, Vista and 7 (32-bit or 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.
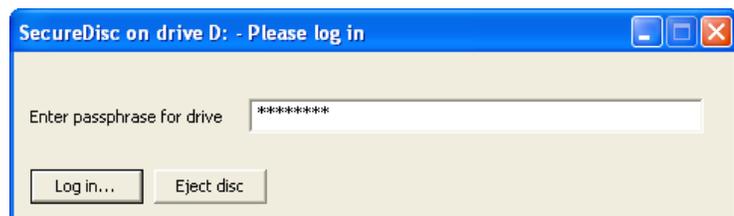
If an incorrect password is entered, the disc is automatically ejected and the client login window is closed. The SecureDisc client has no settings that require configuration. The SecureDisc Client loads at system startup into the system tray, next to the clock.

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 Decryption Issues

Issue:
The Explorer Client returns the following error message: "Transparency server failed to start"
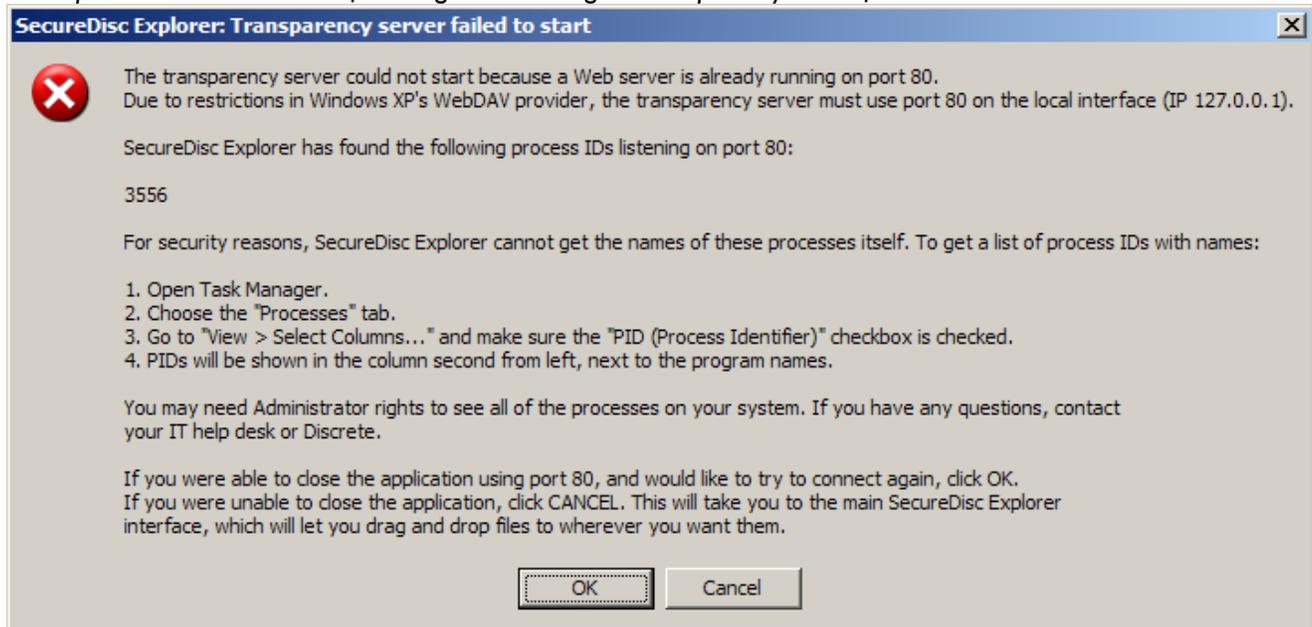
Resolution:
The Explorer Client uses its built-in Transparency Server to provide drive-letter access to the encrypted session. Due to limitations in Windows' built-in WebDAV redirector, the Transparency Server *must* use port 80. The user can check Task Manager to find the Process ID number reported 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:

SecureDisc Explorer permissions setup

"Do you want to allow Non-Administrators to use SecureDisc Explorer and have access to encrypted CD-ROMs?

Select Yes if Non-Administrators use your computer and will need access to encrypted CD-ROMs. A reboot will be required for this permission change to take effect. Select No if you are the only user on this computer or if Non-Administrators use your computer and do not need access to encrypted CD-ROMs.

Yes   No

Non-Administrative User:

SecureDisc: Encrypted session access denied

SecureDisc Explorer cannot access the encrypted session because it does not have the right permissions. To reset the permissions, please run SecureDisc Explorer as an Administrator. SecureDisc Explorer will ask if you want to change the permissions. Click YES, then reboot your computer.

OK

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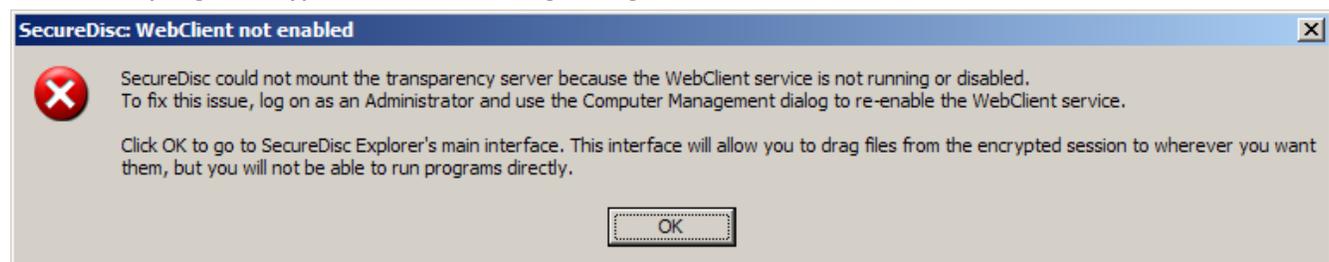
If you are running the Explorer Client as an Administrator on a Windows XP machine, and the permissions are set to defaults, then the Explorer Client will show the first dialog. Answering "Yes" will set new default permissions on the CD-ROM class which allows non-Administrators to access the local machine's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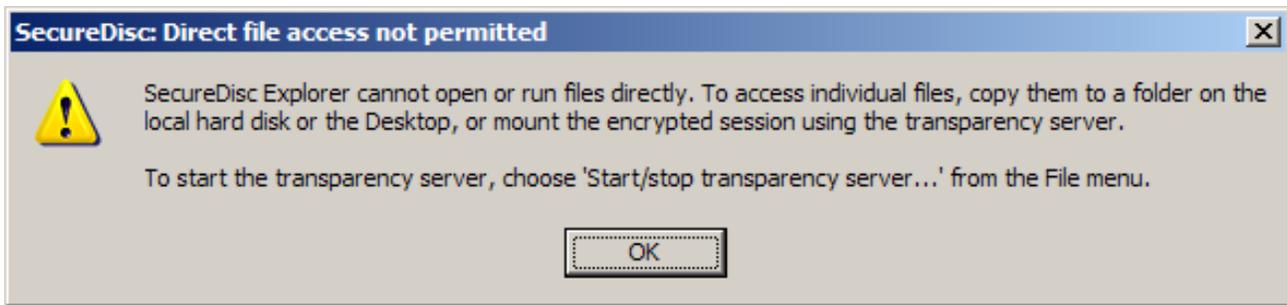
Issue:

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

SecureDisc: WebClient not enabled

SecureDisc could not mount the transparency server because the WebClient service is not running or disabled. To fix this issue, log on as an Administrator and use the Computer Management dialog to re-enable the WebClient service.

Click OK to go to SecureDisc Explorer's main interface. This interface will allow you to drag files from the encrypted session to wherever you want them, but you will not be able to run programs directly.
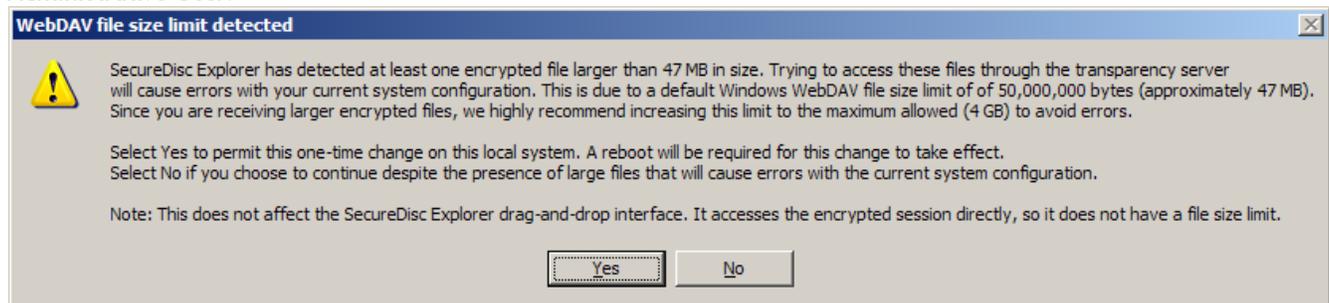
OK

[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 without the WebClient service active, 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:
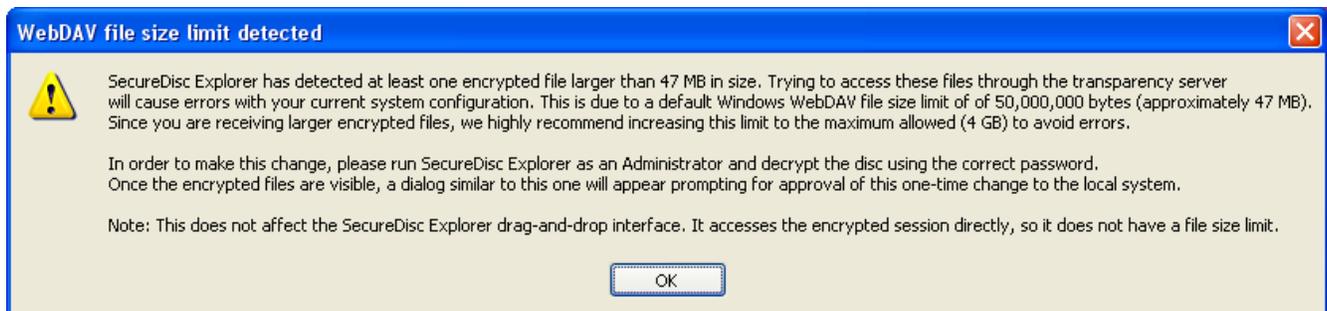
SecureDisc: Direct file access not permitted

SecureDisc Explorer cannot open or run files directly. To access individual files, copy them to a folder on the local hard disk or the Desktop, or mount the encrypted session using the transparency server.

To start the transparency server, choose 'Start/stop transparency server...' from the File menu.

OK

Issue:

When accessing the contents of the encrypted disc, I see a SecureDisc Explorer file size limit warning dialog titled 'WebDAV file size limit detected.' Why?

Administrative User:

WebDAV file size limit detected

SecureDisc Explorer has detected at least one encrypted file larger than 47 MB in size. Trying to access these files through the transparency server will cause errors with your current system configuration. This is due to a default Windows WebDAV file size limit of of 50,000,000 bytes (approximately 47 MB). Since you are receiving larger encrypted files, we highly recommend increasing this limit to the maximum allowed (4 GB) to avoid errors.

Select Yes to permit this one-time change on this local system. A reboot will be required for this change to take effect.
Select No if you choose to continue despite the presence of large files that will cause errors with the current system configuration.

Note: This does not affect the SecureDisc Explorer drag-and-drop interface. It accesses the encrypted session directly, so it does not have a file size limit.

Yes   No

Non-Administrative User:

WebDAV file size limit detected

SecureDisc Explorer has detected at least one encrypted file larger than 47 MB in size. Trying to access these files through the transparency server will cause errors with your current system configuration. This is due to a default Windows WebDAV file size limit of of 50,000,000 bytes (approximately 47 MB). Since you are receiving larger encrypted files, we highly recommend increasing this limit to the maximum allowed (4 GB) to avoid errors.

In order to make this change, please run SecureDisc Explorer as an Administrator and decrypt the disc using the correct password.
Once the encrypted files are visible, a dialog similar to this one will appear prompting for approval of this one-time change to the local system.

Note: This does not affect the SecureDisc Explorer drag-and-drop interface. It accesses the encrypted session directly, so it does not have a file size limit.

OK

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 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 initiate a one-time local registry change that will increase the maximum file size to approximately 4 GB. 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 and no changes can be made to the file size limit until an Administrator is logged in and the disc has been accessed using the correct password, which will result in the first dialog appearing to allow the one-time permissions change.

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:
The encrypted disc appears to be blank and no files are visible.
Resolution:
Please contact your disc provider immediately, there may have been a problem in the disc production cycle that produced an improperly formatted disc.

Copyright Information

Eighth Edition
December 2010
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 polices 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.