SecureDisc

Decryption Guide

DISCRETE TECHNOLOGIES

A GTGI COMPANY

www.discretetech.com · sales@gtgi.com · 703.486.0500 · 3108 Columbia Pike | Suite 301 | Arlington VA 22204

Contents

Introduction

SecureDisc is used for protecting content recorded on CD, DVD and/or Blu-Ray media by restricting access to the content via a decryption key. SecureDisc encrypts the entire contents of an ISO or UDF disc image using a FIPS 140-2 validated 256-bit AES (Advanced Encryption Standard) module in CBC mode.

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. Your disc provider may have given you either or both of these clients to use; please install and use the client they recommend.

System Requirements

Explorer Client

- Windows XP or higher (32-bit or 64-bit; supports Windows 10)
- DVD or CD reader
- Free disk space for caching the contents of the encrypted disc session
- Does not require administrator privileges in most cases. See Troubleshooting Decryption Issues for more information.

Resident Client

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

FIPS Information

- SecureDisc Resident Client contains an embedded, FIPS 140-2 validated encryption module
- For specific FIPS information, visit http://www.gtgi.com/products/securedisc-client.

SecureDisc Explorer Client

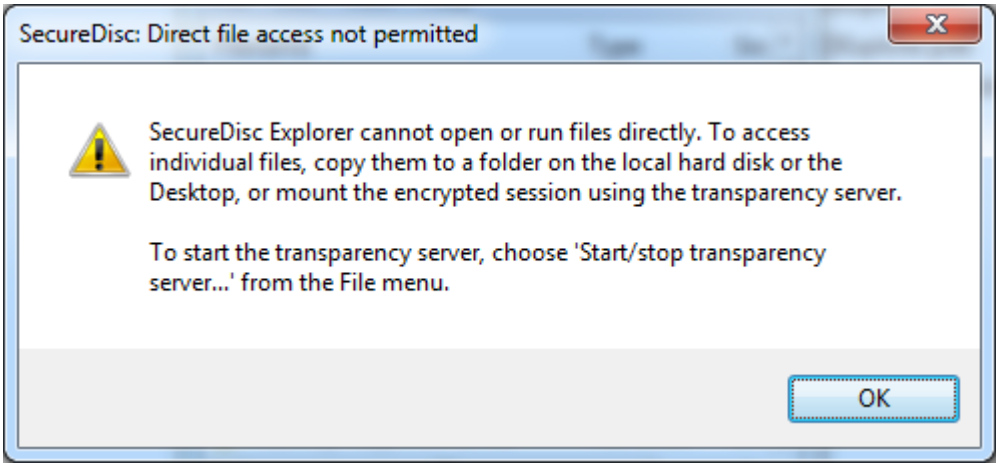
The SecureDisc Explorer Client is compatible with Windows XP and later (both 32-bit and 64-bit, including Windows 7, 8.x, and 10) and does not install on the recipient PC. Typically, it does not require Administrator rights for utilization.* It is designed to provide access to the encrypted session by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

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

Launching the Explorer Client

By default, the Explorer Client (SCDExplorer.exe) is set up to launch automatically from a SecureDisc-encrypted disc. If the Explorer Client is not automatically launched, open the disc in Windows Explorer and double-click on SCDExplorer.exe. The Explorer Client will start, check the disc and present a login box. Enter your password here, and either press Enter or click OK.

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



The Transparency Server

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

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

Tray icon

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

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

Using the Explorer Client to read SecureDisc v1 encrypted discs

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

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

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

SecureDisc Resident Client

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

The Resident Client installs two parts: A "filter" driver and a "helper" application. The filter driver is placed in the Windows CD-ROM 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 bypass 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.

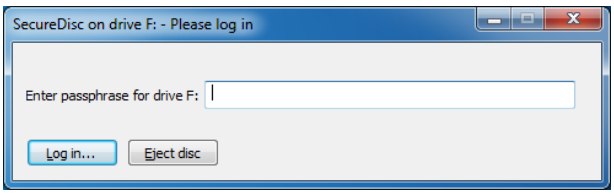
Resident Client Installation

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

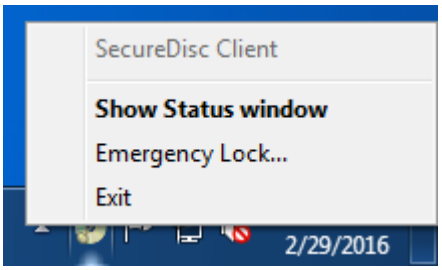
To read an encrypted disc, load the disc into an available CD or DVD drive. The Resident Client will automatically open and prompt for the password. Enter the password and click on Log In. To cancel password entry, click on Eject Disc.



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:

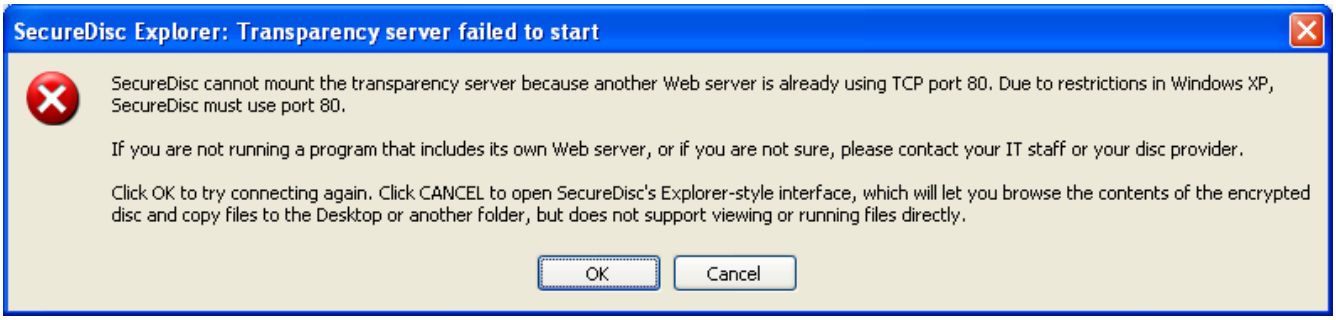
- *Show Status Window* displays the drives available and whether they contain an encrypted disc

- *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

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

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



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

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

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

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

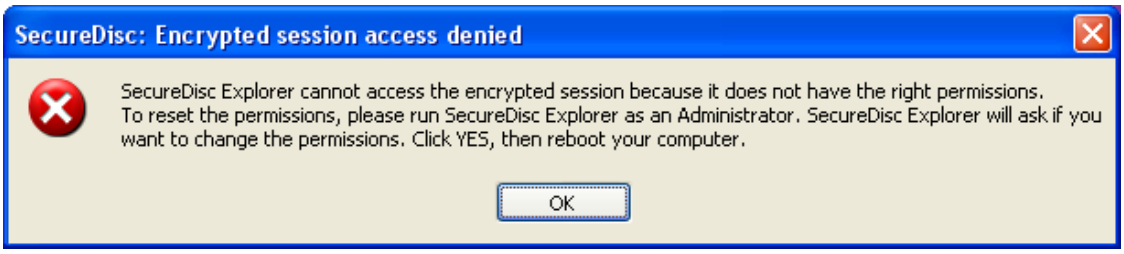
Windows 7 and later have an improved WebClient that will allow connections on any port, not just port 80, and so this limitation does not apply to them. The Resident Client will automatically detect the Windows version and use this feature when present.

Issue:

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

Administrative User:

Non-Administrative User:

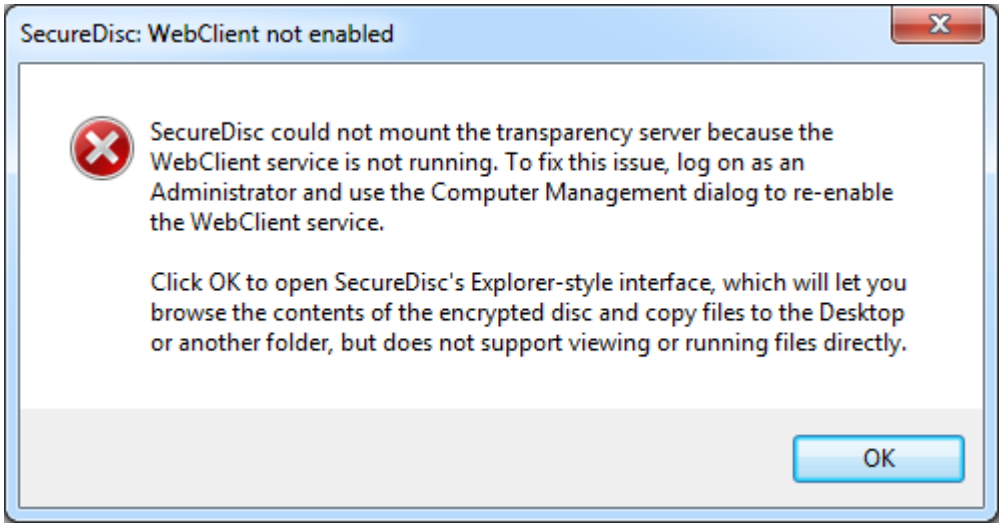


Resolution:

These messages only appear on Windows XP, and when using discs encrypted using older versions of SecureDisc. To work properly with older discs, SecureDisc Explorer requires write access to the CD/DVD device. Clicking Yes on the Administrator version of this prompt will grant SCSI pass-through access on CD/DVD devices to *all users* on the computer, which may be a security risk. If this is unacceptable, we recommend using the Resident Client to read discs encrypted with older versions of SecureDisc.

Windows 7, 8, and 10 all use more relaxed CD-ROM device permissions for limited users on the system console, so this set of messages should not appear on those versions of Windows.

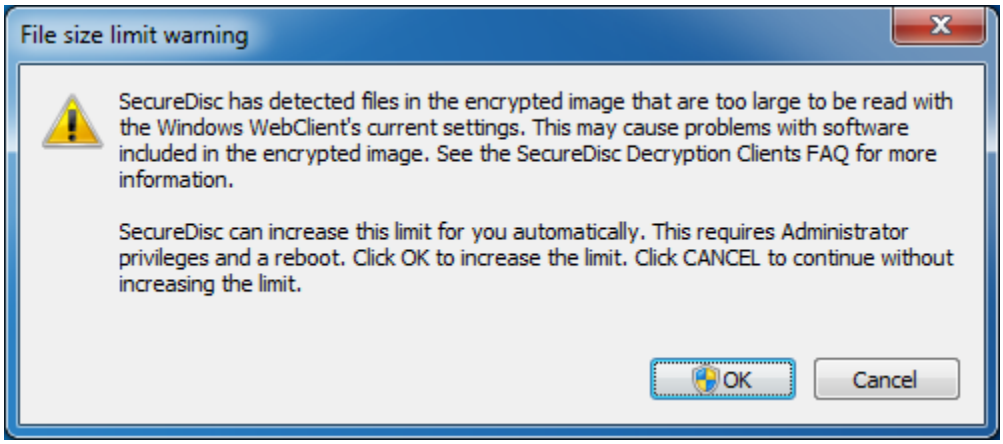
Issue:
When attempting to decrypt a disc, I see a dialog stating that WebClient is not enabled.



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

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

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



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

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

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

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

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

We have specifically found this issue with older versions of Novell's *NetIdentity* product, which ships

with Novell Client for Windows XP. If you are using Novell Client on Windows XP, please upgrade to the latest version (4.91 SP5 as of this writing).

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

The specific registry location in Windows XP is:

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

Copyright Information

SecureDisc Decryption Guide

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

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

March 2016 Edition
Explorer Client version 1.5 and higher
Resident Client version 3.0 and higher

End-User License Agreement

END-USER LICENSE AGREEMENT FOR GTGI SOFTWARE

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

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

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

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

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

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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