



Secure Global Desktop™ User Guide

**A guide to using the Secure
Global Desktop Client
Interface**



Last Updated: **December 17, 2004**
Version 4.0

©1999-2004 Tarantella Inc. All rights reserved.

The information contained in this document represents the current view of Tarantella Inc. on the issues discussed as of the date of publication. Because Tarantella Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Tarantella Inc., and Tarantella Inc. cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. TARANTELLA INC. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Tarantella Inc.

Secure Global Desktop and Secure Global Desktop License Policy Manager are trademarks or registered trademarks of Tarantella Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other company, product and brand names are trademarks of their respective owners.

Contact Tarantella

Tarantella Inc.
425 Encinal Street,
Santa Cruz,
California 95061-1900

Technical Support

For technical queries, write to support@tarantella.com.

General Enquiries

For general enquiries, write to info@tarantella.com.

Secure Global Desktop User Guide

Abstract

This book addresses an end user's interaction with Secure Global Desktop. It explains how to get started with the Secure Global Desktop Launch Pad. It also explains the concepts and provides help for using the Secure Global Desktop Launch Pad. In addition, it provides steps for troubleshooting.

ABOUT THIS BOOK	1
What's in this book?	1
Intended audience	1
Using this book	1
<i>Book conventions.</i>	2
<i>Related resources.</i>	2
<i>Send us your comments</i>	2
<i>Printing this book</i>	3
GETTING STARTED	4
What's in this chapter?	4
What is Secure Global Desktop?	4
<i>Secure Global Desktop and Terminal Services</i>	4
<i>Secure Global Desktop and you</i>	4
<i>Secure Global Desktop Clients</i>	5
What's new	7
<i>Launch Pad</i>	7
Secure Global Desktop user features	7
Using Secure Global Desktop Launch Pad for the first time	7
<i>View the Secure Global Desktop Launch Pad Web Site</i>	8
<i>Download and install client</i>	8
<i>Log on to Secure Global Desktop using Launch Pad</i>	9
<i>Launch applications for the first time</i>	9
SECURE GLOBAL DESKTOP CONCEPTS	10
What's in this chapter?	10
Concepts	10
Tarantella Client download	10
<i>Why do I need a client?</i>	10
<i>How big is the client?</i>	11
<i>Where do I get a Client?</i>	11
<i>What do I need to know before I download a client?</i>	11
Client upgrade	11
<i>Why do I need a client upgrade?</i>	11
<i>How can I download a new client?</i>	11
Accessing Secure Global Desktop	12
<i>Can I access Secure Global Desktop from a public network or public client?</i>	12
Accessing remote applications.	12
<i>Favorites</i>	12

<i>Applications</i>	12
<i>Start menu</i>	12
<i>Desktop</i>	13
<i>File Associations</i>	13
Launch Pad and seamless operations	13
<i>When should I use the Launch Pad?</i>	13
Launch Pad URL switches	14
<i>Single Port Relay</i>	14
<i>Launch Pad Style</i>	14
File associations	15
<i>How can I enable file associations from the Launch Pad?</i>	15
<i>When are file associations created on my computer?</i>	15
<i>How can I override the file associations</i>	16
Shortcuts	16
<i>Who owns the shortcuts?</i>	16
<i>Where do I create shortcuts?</i>	16
<i>What happens when I log on to the domain?</i>	17
<i>Will applications from different servers exhibit different behaviors?</i>	17
<i>When does Secure Global Desktop create shortcuts?</i>	17
<i>When do shortcuts refresh?</i>	17
<i>What happens with a refresh event?</i>	17
Multiple applications per session	18
<i>Why can I see multiple applications but only one session on Connections page?</i> .	18
Client Groups	18
<i>What is a Client Group?</i>	18
<i>Are Client Group shortcuts any different from User shortcuts?</i>	18
<i>Client Groups and printers</i>	19
Client drive access	19
<i>What is Internet File Sharing (IFS)?</i>	19
<i>How does IFS drive lettering work?</i>	19
<i>Why can there be an occasional delay or lag in saving and opening files?</i>	19
Printing	19
<i>What printers does Secure Global Desktop support?</i>	19
<i>Why are the printer names different from the original printer's names?</i>	20
<i>Can jobs print with high quality color and high resolution?</i>	20
<i>Can there be other loss of printer functionality, like print preview?</i>	20
<i>Why are some print jobs different from their print previews?</i>	20
Disconnect and reconnect	20
<i>What are the disconnect and reconnect features?</i>	20
<i>How is the disconnect feature influenced by idle time?</i>	21
<i>What is the remote connect feature?</i>	21

<i>Why can multiple applications exist in a single session?</i>	21
Idle Time	21
<i>What is idle time?</i>	21
<i>What is the time-out property?</i>	22
<i>How do I keep from losing work due to idle time restrictions?</i>	22
Shadowing	22
<i>What is shadowing?</i>	22
<i>Can you explain the shadowing prompt and its relevance?</i>	22
Application Behavior	22
<i>Do applications behave the same on different operating systems?</i>	22
Privacy	23
<i>How can shadowing affect privacy?</i>	23
<i>What management information does Secure Global Desktop log that relates to me?</i> 23	
Removing the Tarantella Client	23
<i>Can I uninstall the Secure Global Desktop Client?</i>	23
<i>Can I delete any leftover shortcuts?</i>	23
<i>Can I delete the Secure Global Desktop browser cache?</i>	24
LAUNCH PAD HELP	25
What's in this chapter?	25
Secure Global Desktop Launch Pad	25
<i>Introduction</i>	25
<i>Installing the Tarantella Connection Manager</i>	26
<i>Logging on to Secure Global Desktop Application Launch Pad</i>	26
Secure Global Desktop Application Launch Pad Pages	27
<i>Favorites</i>	27
<i>Applications</i>	27
<i>Connections</i>	27
<i>Options</i>	28
<i>Download Client</i>	29
<i>About</i>	29
Tarantella Connection Manager	29
TROUBLESHOOTING	31
What's in this chapter?	31
Errors and common queries	31
<i>Logon fails with "null" error</i>	31
<i>Launch Pad Favorites page is not displayed</i>	32
<i>Corrupt installation detected error</i>	33
<i>IFS error</i>	33

- Launch Failed error* 34
- Load Balancing Failed error.*..... 35
- Correct icons not displayed.*..... 35
- Unable to launch applications.* 35
- Tarantella Connection Manager icon* 36
- Application prompts for password.*..... 36
- Application shortcuts.*..... 36
- Netscape error.*..... 37
- IE setting for SharePoint server* 38
- Unable to launch applications on Windows 95.*..... 39
- Security settings error* 39

- ABOUT US.** 40
 - What's in this chapter?** 40
 - About Tarantella.** 40
 - About Secure Global Desktop from Tarantella** 40
 - Other sources of information** 40

- ABBREVIATIONS.** 41
 - What's in this appendix?** 41
 - Abbreviations** 41

About This Book

What's in this book?

This book explains how to get started with the Secure Global Desktop Launch Pad. It explains the concepts and provides help for using the Secure Global Desktop Launch Pad. It also provides steps for troubleshooting.

Intended audience

This book is primarily intended for users of the applications in a Secure Global Desktop team.

Using this book

This book is organized as follows:

TABLE 1. Contents and description

Chapter/Appendix	Brief Description
" <u>Getting Started</u> "	This chapter provides information on what is Secure Global Desktop and helps you get started with the Launch Pad.
" <u>Secure Global Desktop Concepts</u> "	This chapter explains the terms and concepts you should be familiar with to be able to use Secure Global Desktop applications effectively.
" <u>Launch Pad Help</u> "	This chapter provides an introduction to the Launch Pad and step-by-step procedures for installing the Tarantella Connection Manager, logging on to the Launch Pad, and performing operations using the Launch Pad.
" <u>Troubleshooting</u> "	This chapter explains the troubleshooting steps and answers your queries on some common issues.
" <u>About Us</u> "	This chapter provides information about Tarantella and Secure Global Desktop.
" <u>Abbreviations</u> "	This appendix lists some common relevant abbreviations.

Book conventions

Book conventions used throughout this book are as follows:

TABLE 2. Book Conventions

This...	Indicates...
Abbreviated menu command	Menu commands in text may be abbreviated rather than full. For example, the text may ask you to click Download , and the screen may show a Download Now button.
Successive menu choices	Successive menu choices may appear with a greater than sign (>) between the items that you will select consecutively.
Bold text	This shows the names of menu items, dialog boxes, dialog box elements, and commands.
<code>Courier text</code>	Code examples appear in courier text. It may represent text you type or data you read.
<variable name>	Variables that you must place in a text may appear between a greater-than and a lesser-than sign. When you type the command, replace this string with your own information. For example, for C:\Document and Settings\<<your name>\Start Menu, John Smith might type something like C:\Document and Settings\JohnSmith\Start Menu.
Text in <i>italics</i>	Reference to other documents.

 **NOTE**

Notes contain additional useful information. Pay special attention to information highlighted this way.

Related resources

The following books make up the complete Secure Global Desktop documentation.

- Secure Global Desktop Installation Guide
- Secure Global Desktop Administrator Guide
- Secure Global Desktop User Guide

Send us your comments

Send us your comments on the Secure Global Desktop™ User Guide, version 4.0.

Tarantella Inc. welcomes your comments and suggestions on the quality and usefulness of this publication. Your feedback is an important part of the information used for updating documentation. Please send us your input regarding any of the following:

- Did you find any errors?
- Is the information clear?
- Do you need more information? If so, where should it be?

- Are the examples correct? Do you want more examples?
- What features of this manual did you like?

If you find any errors or have any other suggestions to improve the quality of this publication, please indicate the chapter, section, and page number (if available).

You can submit comments to us in the following ways:

- Email
documentation@tarantella.com
- U.S. Mail:
Technical Publications
Tarantella Inc.
425 Encinal Street,
Santa Cruz,
California 95061-1900

If you would like a reply, please include your name, address, and telephone number.

Printing this book

This guide is optimized for printing on Letter page size (8.5 inches by 11 inches). If you would like to print on any other page size, select the **Fit to page** check box in the Print window before you print this guide.

Getting Started

What's in this chapter?

This chapter provides information on what is Secure Global Desktop and helps you get started with the Launch Pad.

What is Secure Global Desktop?

Secure Global Desktop™ from Tarantella® enables system administrators to manage end users, application servers, and centrally hosted Windows applications in a way that is simple, intelligent, and cost effective.

Secure Global Desktop and Terminal Services

Secure Global Desktop is an application-delivery management program that works within the network-centric, Server-based computing paradigm.

It is a server- and web-based computing solution that offers application provisioning and environment configuration from one familiar, easy-to-use Management Console.

With Secure Global Desktop you can use your application delivery resources more efficiently to achieve high-performance, cost-effective application delivery that is easy to deploy and manage.

Secure Global Desktop provides a cost-effective, intelligent, application-management solution for reducing the cost of deploying and maintaining application software.

Secure Global Desktop and you

Secure Global Desktop enhances your computing experience and your productivity by allowing you to run applications from remote servers.

The Secure Global Desktop Applications Launch Pad provides the following benefits for users:

Web-based access

Secure Global Desktop Application Launch Pad is a Web-based application portal that provides easy access to any remotely located provisioned application from your Web browser.

Fast setup

Secure Global Desktop provides an installation process that makes it easy to download the client software to your computer with clear instructions and familiar functionality. It takes only minutes to download the Tarantella Connection Manager client software and install it on your computer.

Quick launch

You can create desktop shortcuts and file associations that permit you to launch of your favorite applications or open documents with file associations with just one click.

Convenient and reliable printing

Secure Global Desktop provides printer driver support to ensure that your printing experience will be successful and uneventful. You can print to printers that are connected directly to your computer, or those located on the network.

Convenient file manipulation

You can save files to your local drives or to local network drives.

Expedited help

You can access the Secure Global Desktop online Help. You can also have your system administrator manage your remote session from anywhere on the network.

Secure Global Desktop Clients

A Secure Global Desktop v4.0 installation creates a team whose applications can be launched from computers with the any of the following operating systems:

- CE 2.12 or CE 4.x (CE .NET)
- Windows 95, Windows 98, Windows NT, Windows XP, Windows Me, Windows 2000, Windows 2003

The following table lists the availability of various Secure Global Desktop features on each of these operating systems:

TABLE 3. Secure Global Desktop Clients and Features

OS	File Associations	Client Groups	Connection Settings	Drive Sharing	Printer Redir	Shortcuts	SPR
CE 2.12	No	Yes	Yes	No	No	No	Yes
CE 4.x	No	Yes	Yes	Yes	Yes	No	Yes
Win 95	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win 98	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win NT	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win XP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win Me	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win 2K	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win 2K3	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The following table lists the availability of various connection settings on each operating system.

TABLE 4.

OS	Adjust Display	Bitmap Caching	Compression	Seamless Windows	Launch in existing connections	Reconnect	SPR	Logoff idle or disconnected connections	Drive and Printer sharing	Unidriver
CE 2.12	No	No	Yes	No	No	Yes	Yes	Yes	No	No
CE 4.x	No	No	Yes	No	No	Yes	Yes	Yes	Yes (Only on Windows 2003 server)*	No
Win 95	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win 98	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win NT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win XP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win Me	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win 2K	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Win 2K3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

* To enable this setting on Windows 2003 servers select the Native option from the Connection Settings page.

Browsers

The Launch Pad can be accessed on Windows 95, Windows 98, Windows NT, Windows XP, Windows Me, Windows 2000, Windows 2003 using any of the following browser versions:

- Internet Explorer 5.5 or higher
- Netscape Navigator 4.75

If a user launches the Launch Pad using Netscape, the user should do the following after finishing work with the Launch Pad:

- Close the Launch Pad window
- Close all browser windows on the client computer.

If the user does not close the browser window, another user who logs on to the Launch Pad using Netscape on the same computer is logged on as the previous user.

If a browser window is left open, any other user who tries to logon to the Launch Pad is not taken to the Logon page of the Launch Pad, but is directly logged on as the previous user and the browser displays the Favorites page for the previous user.

For example, a user John logs on to the Launch Pad using Netscape Navigator and opens another browser window for surfing. John then closes the Launch Pad window and leaves the other window open. Now, another user Richard tries to logon to the Launch Pad by typing the URL of the

Launch Pad in a new browser window on the same computer. Richard is directly logged on to the Launch Pad as John without authentication. Instead of the Logon page, the Favorites page is displayed giving Richard access to all the applications that are assigned to John.

What's new

Launch Pad

Tarantella Client Version

A user can find out the client version by placing the mouse over the Tarantella Connection Manager tray icon when there are no active connections. The tool tip displays the client version for v4.0 client.

File Associations

The administrators can make file associations, associating certain file extensions with applications on the Application Servers. The users can now open their documents directly in applications on Application Servers if they enable file associations. The users can enable file associations from the Options page of the Launch Pad.

Tarantella Connection Manager

The Tarantella Connection Manager now displays the following options on right-click:

- **Refresh shortcuts and file associations** instead of **Refresh shortcuts**.
- **Delete all client settings** instead of **Delete all shortcuts**.

Secure Global Desktop user features

The user experience pertains to a user's perception of Secure Global Desktop, and Secure Global Desktop offers:

- Reliable printer support at the local, server, and network levels
- Flexible and secure file saving at the local and network levels
- Seamless windows support to display a screen without the WTS frame
- Versatile application launch capabilities from a shortcut, browser, or Windows Start menu
- Ability to open documents directly in applications on Application Servers through file associations
- Efficient handling of public terminals through settings in the console
- Automatic log on and pass-through authentication
- Disconnect and reconnect options that can temporarily disconnect from and reconnect to an existing session
- Connection settings for varied user experience and bandwidth

Using Secure Global Desktop Launch Pad for the first time

From this section, you learn how to:

["View the Secure Global Desktop Launch Pad Web Site"](#)

["Download and install client"](#)

["Log on to Secure Global Desktop using Launch Pad"](#)

"Launch applications for the first time"

View the Secure Global Desktop Launch Pad Web Site

When to use this?

You must access the Secure Global Desktop Launch Pad Web site in order to download the Tarantella Connection Manager.

How this works

To view the Secure Global Desktop Launch Pad Web site:

1. Open your Web browser using either Microsoft Internet Explorer, version 5.5 or higher, or Netscape Navigator 4.75 (Not Netscape 6.x)
2. Enter the URL that opens your Secure Global Desktop Application Launch Pad. For example:

`http://<webserver-name>/LaunchPad`

where webserver-name is the name of the computer where your Administrator has installed the Secure Global Desktop Web Server Role.

NOTE

If you do not have this information, contact your system administrator.

Download and install client

You can use this function to download and install the client software prior to logging on to the Launch Pad.

NOTE

You will need local administrator rights to install the Tarantella Connection Manager. If you do not have this right, please ask your system administrator to install it for you.

From the Launch Pad:

1. From the navigation bar, click **Download Client**.
2. Click **Download Now**.
3. Select a download option.
 - It may be best to select **Run this program from its current location** from the **File Download** dialog box and click **OK**.
 - You may choose the **Save this program to disk** option, download the file and then open the SGD-TSE-Client400.exe file, from the location to which you downloaded it to install the client.
4. On the **Welcome** panel of the Tarantella Connection Manager Installation Wizard, click **Next**.
5. From the **Destination Folder** panel, click **Browse** to choose a destination directory or accept the default setting. Click **Next**.
6. After installation, from the **Installation Complete** panel, click **Finish**.

7. If you are prompted to reboot, reboot the computer and connect back to the Launch Pad.
8. If you are not asked to reboot your client, click **Done** and the Launch Pad **Log On** page appears next.

Log on to Secure Global Desktop using Launch Pad

The Secure Global Desktop Application Launch Pad is your interface to Secure Global Desktop and it contains a link to the **Log On** page.

1. If you are not on the Logon page, access the Secure Global Desktop Application Launch Pad and click **Log On**.
2. Enter information in the following fields:
 - **Logon Name:** Generally this is the logon name you use to logon to your domain. If you are having problems logging on, please contact your administrator.
 - **Password:** This password belongs to the user that you specified in the Logon Name
 - **Log on to:** This identifies the domain to which you belong. If you do not know your domain, ask your system administrator.
3. If your system administrator provides automatic logon privileges to you, you will see the **Automatically log on from this computer** check box on the **Log On** page. Select this option to log on from this PC in the future without typing your logon name and password.
4. Click **Log On**.

Launch applications for the first time

You use the Secure Global Desktop Application Launch Pad page to initiate an application launch.

To launch one of the applications:

1. "[Log on to Secure Global Desktop using Launch Pad](#)" and from the navigation bar, click **Favorites** or **Applications**.
2. Click an application's name or its icon.

Tarantella Connection Manager talks to the Load Balancer to find the Application Server that has the least load and your launch request is directed to an Application Server. The application you choose runs from that server and displays on your computer.

Related Information

If you attempt to use an application before you download the client, Secure Global Desktop redirects you to the **Download Client** Page. For more information, refer to "[Download and install client](#)".

Secure Global Desktop Concepts

What's in this chapter?

This chapter explains the terms and concepts you should be familiar with to be able to use Secure Global Desktop applications effectively.

Concepts

This section explains the following Secure Global Desktop Concepts.

- "[Tarantella Client download](#)"
- "[Client upgrade](#)"
- "[Accessing Secure Global Desktop](#)"
- "[Accessing remote applications](#)"
- "[Launch Pad and seamless operations](#)"
- "[Launch Pad URL switches](#)"
- "[File associations](#)"
- "[Shortcuts](#)"
- "[Multiple applications per session](#)"
- "[Client Groups](#)"
- "[Client drive access](#)"
- "[Printing](#)"
- "[Disconnect and reconnect](#)"
- "[Idle Time](#)"
- "[Shadowing](#)"
- "[Application Behavior](#)"
- "[Privacy](#)"
- "[Removing the Tarantella Client](#)"

Tarantella Client download

Why do I need a client?

You must install a Tarantella Client on any device that you will use to launch remote applications.

How big is the client?

The Secure Global Desktop Windows client is about 3MB.

Where do I get a Client?

You can download the client directly from a Secure Global Desktop Launch Pad Web site (ask your administrator for the URL) or you can ask your Secure Global Desktop administrator to push the Tarantella Client to the client computers using a third-party tool. If you access the URL from your client computer, Secure Global Desktop determines if the correct version of the client is already present on your client computer. If it is absent, Secure Global Desktop prompts you to download new software.

What do I need to know before I download a client?

You need administrator rights to download and install the client.

Client upgrade

Why do I need a client upgrade?

You need a Tarantella Client upgrade on the Client computers, where the Secure Global Desktop users log on, to upgrade from Canaveral iQ v2.0 (or later) to Secure Global Desktop v 4.0. This upgrade allows the system to use all the features available in the Secure Global Desktop upgrade. The new client uninstalls the old client and then installs the new client. You do not have to reboot the computer generally.

When the administrator upgrades the team to Secure Global Desktop v4.0, if you have already upgraded to Tarantella Connection Manager v2.1, the Tarantella Connection Manager v4.0 task bar icon appears green instead of the usual maroon when there are no active connections. This is to indicate that a newer version of the client is available for download. After downloading the latest client, the Tarantella Connection Manager task bar icon appears maroon when there are no active connections. When there are active connections, the Tarantella Connection Manager task bar icon always appears blue.

How can I download a new client?

You need to be an administrator on the local computer to install the client. You can download the new client from the Launch Pad. For more information, refer to "[Download and install client](#)". The shortcuts remain functional after the client install as before the Client upgrade.

NOTE

An upgrade does not delete the user settings. That is, the user still connects to the same Web Server after the upgrade, and has the same shortcuts.

Native Windows Client Connections

The Native RDP Client Connections feature in Secure Global Desktop TSE v4 enables you to run server-based applications without having to install any additional client software (besides thenative

Microsoft RDP client) on the client device. While there is no need to install any client software from Tarantella, you still must have the Microsoft Terminal Services Advanced Client (TSAC) ActiveX control properly registered on your client machine. This ActiveX control resides in a DLL file named MSTSACX.DLL. Windows XP has this ActiveX installed by default, however for other Windows operating systems it is not installed by default. If this ActiveX control is not already installed by default, it gets seamlessly installed on your machine as long as the security settings of your Internet Explorer are configured to allow download of ActiveX controls.

NOTE

 **NOTE**

The TSAC ActiveX control and hence the Native RDP Client Connection feature for Windows will not work if the security settings on the Internet Explorer for Active X controls and plug-ins are not configured to enable “Run Active X controls and plug-ins” and “Script ActiveX controls marked safe for scripting”.

Native Client on Macintosh

The Native RDP Client Connections feature in Secure Global Desktop TSE v4 enables you to run server-based applications without having to install any additional client software (besides the native Microsoft RDP client) on the client device. Launching SGD-TSE applications from a Macintosh client machine requires the Microsoft Remote Desktop Connection Client for Mac to be installed on the machine. More information can be obtained at this Microsoft Websites Mac section: <http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient>. In addition to this client, a SGD-TSE plug-in from Tarantella has to be downloaded and installed in order to use Macintosh machines. This plug-in is currently only tested on Safari 1.1 (v100) and higher browser running on OS X version 10.3.

Accessing Secure Global Desktop

Can I access Secure Global Desktop from a public network or public client?

Your Secure Global Desktop administrator can set up ports that permit you to access Secure Global Desktop through the firewalls. The ports you need opened are: TCP port 4660, 3389, and 80 outbound from your firewall or proxy. Once your administrator arranges for you to log on to Secure Global Desktop from outside, you need to decide how you will access Secure Global Desktop.

If you access Secure Global Desktop from your own home computer, you will access Secure Global Desktop from a relatively secure location.

If you access Secure Global Desktop from an Internet café or from another publicly located computer, then you need to be aware of some special security precautions. For optimal security, you must follow these rules:

1. You must choose not to save the password for applications that you launch. This means, when you view the Secure Global Desktop Application Launch Pad and you see the setting **Automatically log on from this computer**, you need to clear the check box.
2. You must close all applications and exit the browser application after you finish your work.

3. You must delete all shortcuts. To do this, right-click the Tarantella Connection Manager tray icon, and choose **Delete all client settings**.

Accessing remote applications

Favorites

You can launch applications from the Secure Global Desktop Application Launch Pad Web site **Favorites** page. To do this, enter the URL of the Secure Global Desktop Application Launch Pad in the browser, click **Favorites** from the navigation bar on the left side of the Web page, and click on the required application's icon.

Applications

You can launch applications from the Secure Global Desktop Application Launch Pad Web site **Applications** page. To do this, enter the URL of the Secure Global Desktop Application Launch Pad in the browser, click **Applications** from the navigation bar on the left side of the web page, and click on the required application's icon.

Start menu

You can launch applications from the Windows Start menu if your administrator permits you to use this option. To launch an application from the Start menu, select **Start>Programs><Secure Global Desktop Team Name>**, and click on the required application's icon. If permitted, you can specify the applications that show up on your Start menu from the **Options** page of your Launch Pad.

Desktop

You can launch applications from the Windows desktop of your client computer if your administrator permits you to use this option. You can specify the applications that appear on your desktop from the **Options** page of your Launch Pad.

File Associations

If you have the v4.0 Tarantella Connection Manager, and the administrator enables file associations, you can open a document in the associated application on the Application Server by simply double-clicking a document. Thus, from the **Options** page of your Launch Pad, configure the applications that you can use to open documents.

Launch Pad and seamless operations

With Secure Global Desktop applications, the functions of the local and remote applications are almost identical, and your experience using the local and remote applications appears identical. You will not notice when applications are running from the server.

If your Secure Global Desktop administrator prohibits you from using this option, your application sessions will appear in a shell, which will look like a frame.

When should I use the Launch Pad?

You do not need to use a browser to launch and use server-based applications via Secure Global Desktop, but you will need to use the browser under the circumstances listed below.

When changing settings

You need access to a number of customizable settings from the browser; for example, connection settings, settings that indicate which applications will appear on the shortcuts, on the desktop, or in the favorites.

Initially, administrators configure default values for these settings. Later, you can customize these settings. You would change these settings from the Secure Global Desktop Application Launch Pad.

When reconnecting to an application

Secure Global Desktop enables you to disconnect from an application session. When you disconnect from an application session, that session stops running on your client computer, but it continues to run on the server. To execute a disconnect operation, go to the Launch Pad and use the **Connections** page to select and disconnect the application, or go to the task bar on your desktop, right click the Tarantella Connection Manager icon, and select **Disconnect all sessions**.

Secure Global Desktop enables you to reconnect to a disconnected application session. To execute a reconnect operation, go to the Launch Pad and use the **Connections** page to select and reconnect the application, or go to the **Options** page of the Launch Pad and select **Always** from the **Reconnect On Launch** list.

The **Reconnect On Launch** field can be set to:

- **Always**, creates a static connection preference. If you select **Always**, Secure Global Desktop will always reconnect your disconnected session when you select an application that has an associated disconnected instance. For example, if you have a disconnected Word session and you attempt to connect to Word, Secure Global Desktop will automatically reconnect your disconnected Word session.
- **Never**, creates a static connection preference. If you select **Never**, Secure Global Desktop will never reconnect your disconnected session when you select an application even if it has an associated disconnected instance.
- **Default**, permits your reconnect options to fluctuate with the property selection made by your Secure Global Desktop administrator. The Always and Never options create a static connection preference.

When connecting to an application on another client computer

Secure Global Desktop enables you to connect to an application session that you left running on another client computer. This is useful, for example, if you leave a session running in the office, but forget to save, and then want to continue with the same session at home so that there is no loss of work.

Launch Pad URL switches

Launch Pad URL switches are options you can specify to override all other settings. You can specify URL switches for the use of the following:

- Single Port Relay
- Launch Pad Style

Single Port Relay

The administrator can configure the Firewall or DNS to make a decision on the use of Single Port Relay. The administrator can route the appropriate clients based on the policies to a URL with Single Port Relay On or Off.

However, you may be a roaming user, trying to connect to your corporate applications. You are sure that the location are connecting from has a locked down firewall, that is the required ports are closed. You can use the URL switch to get all sessions via the Single Port Relay irrespective of what other policies may say.

In this case, the Launch Pad URL you will use will be \\<Secure Global Desktop Web Server Name>\LaunchPad\?relay=1.

Launch Pad Style

In general, the Secure Global Desktop Administrator sets the Launch Pad style for all members of a team. However, you can override the settings and change the appearance of the Launch Pad in terms of style when you access it. To do this, you can add `style=<style number>` in the query string and the query string must begin with a question mark (?).

The valid values for the style number are the digits 1, 2, and 3. The style associated with each follows:

- 1= full (with banner, side-bar action list, and highlighted page content)
- 2= no banner (with side-bar action list and highlighted page content)
- 3= minimal (with highlighted page content and neither side-bar actions nor banner)

The first example that follows shows a generic Launch Pad URL and the second example shows a URL that is qualified using the `style=` parameter. In this case, the second URL specifies a Launch Pad style that has no banner.

\\<Secure Global Desktop Web Server Name>\LaunchPad\

\\<Secure Global Desktop Web Server Name>\LaunchPad\?style=2

! **NOTE**

URL routing is a very powerful and flexible tool that is generic in nature and most applications such as firewalls, DNS, Web Server can make use of it.

File associations

The File Association feature in Secure Global Desktop enables you to launch applications on the Secure Global Desktop Application Servers directly from the documents. You can open files by double-clicking the files that have file associations to remote applications. File Associations allow opening an existing file without first opening the application on remote Application Servers.

If you enable file associations, when you double-click a file that is associated with an application on an Application Server, the file automatically opens in the application on the remote Application Server.

How can I enable file associations from the Launch Pad?

If the Administrator settings allow you to enable file associations, you can use the Launch Pad to select applications for file association. You can enable file associations for applications from the **Options>Update>Update Application Options** page by selecting the check box in the **File Associations** column for the relevant applications.

On the other hand, if the Administrator settings make the application settings binding on you, the file associations made by the Administrator will be created on your computer.

When are file associations created on my computer?

If the file associations are enabled, they are created on your computer whenever you or any other user:

- Runs the Launch Pad and logs in
- Reboots the computer
- Logs on to a computer as a different windows user
- Clicks the **refresh applications list** link on the Launchpad
- Right-clicks the Tarantella Connection Manager icon on the Task Manager and selects **Refresh shortcuts and file associations**
- Launches an application when the Tarantella Connection Manager is not running

! **NOTE**

If multiple Secure Global Desktop users use the same computer as a single windows user, then the settings of the last user logged on govern the file associations created on the computer.

How can I override the file associations

If you log on to a computer as a local administrator, you can override the Secure Global Desktop file associations on the computer by reverting to the local file associations by:

- Right clicking the Tarantella Connection Manager in the task bar and selecting **Delete all client settings** from the shortcut menu.
- Editing the Registry to delete the relevant keys.
- From the **Options>Update>Update Application Options** page, by clearing the check box in the **File Associations** column for the appropriate application.
- Exiting the Connection Manager, by right clicking the **Tarantella Connection Manager** in the task bar, and selecting **Exit** from the shortcut menu.
- Uninstalling Tarantella Connection Manager from the computer.

Editing the Registry

To edit the registry to revert to the local file associations:

1. Select **Start>Run**.
2. Enter `regedit` in the **Open** field and click **OK**.
3. In the Registry Editor, expand **HKEY_CURRENT_USER>Software>Classes** in the left pane.
4. Right-click the file association folder that you want to delete, and select **Delete** from the shortcut menu.
5. Repeat the previous step for each file association you want to delete.

Shortcuts

Who owns the shortcuts?

Secure Global Desktop creates shortcuts on a per user basis. Therefore, you own your shortcuts and you cannot access another user's shortcuts.

Where do I create shortcuts?

You can create shortcuts in the Windows Start menu and/or on the client desktop.

! **NOTE**

Secure Global Desktop creates only one shortcut for two or more applications that have the same name in the Windows menu and on the desktop. However, you can see all the applications on the Favorites and Applications pages of the Launch Pad.

What happens when I log on to the domain?

You receive application access based on your domain affiliations. Because Secure Global Desktop leverages the domain for user information, Secure Global Desktop automatically creates your shortcuts based on your membership in different user groups or organizational units. In addition, if the computer belongs to a Client Group, the Client Group shortcuts are also available on your desktop. However, your shortcuts always override the Client Group shortcuts. You receive application access automatically when you log on to your client computers.

Will applications from different servers exhibit different behaviors?

Yes, the applications exhibit different behaviors based on the operating system installed on the hosting server. Tarantella Clients support shortcuts for these operating systems: Windows 95, Windows 98, NT 4.0, Windows Me, Windows 2000, Windows XP, and Windows 2003.

When does Secure Global Desktop create shortcuts?

Secure Global Desktop has an ability to create shortcuts at the following times:

- When you log on to the Secure Global Desktop Application Launch Pad
- When you reboot the computer
- When you log on to your computer
- When you refresh your shortcuts from the Connection Manager
- After you change your Secure Global Desktop Application Launch Pad shortcut preferences from the **Options** page, when you click **refresh application list**.

NOTE

Condition 3 above will work correctly only if you have logged on to the Secure Global Desktop Application Launch Pad at least once before you attempt these actions.

When do shortcuts refresh?

Secure Global Desktop has an ability to refresh shortcuts at the following times:

- When you right-click the Tarantella Connection Manager tray icon and then click **Refresh shortcuts and file associations**.
- When you log on to a client computer, the logon event triggers a refresh. Shortcuts will refresh if you have previously logged on to the Secure Global Desktop Application Launch Pad or if the administrator has pushed the shortcuts
- When you click the **refresh application list** link that appears on the **Favorites** or **Applications** page of the Launch Pad.

What happens with a refresh event?

Secure Global Desktop keeps track of all the shortcuts that it creates. However, if you copy a shortcut from its original location to some other location, then Secure Global Desktop becomes unaware of this instance; therefore, Secure Global Desktop will be unable to delete or refresh the

shortcut instance that was the result of the copy event. Secure Global Desktop will delete and refresh the shortcut instance that was the source for the copy event.

Multiple applications per session

Why can I see multiple applications but only one session on Connections page?

The first application you launch, creates a connection with an Application Server. If the administrator has made the appropriate settings to enable multiple applications per session, depending on the settings made in the Secure Global Desktop team, your next session may launch in the same session to optimize performance. This is called session affinity.

In such a case, the Connection page displays one connection for all the sessions that are launched in the session. When you disconnect or log off a session, all the applications running in that session are disconnected or logged off. Similarly, when you reconnect a disconnected session, or connect to a session on another client computer, all the applications running in the session are reconnected.

Client Groups

What is a Client Group?

A Client Group is a group of client computers, sorted on the basis of certain criteria specified by the Secure Global Desktop administrator. The Client Group shortcuts are created on the computer that has a Tarantella Connection Manager on it. However, these Client Group applications are not available to you on the Launch Pad if they are not assigned to you. The administrator can specify settings such that:

- All applications are launched with specific connection settings.
- You cannot save your password on the client computer.
- Your shortcuts are not created on the client computer.
- You cannot launch applications directly on an Application Server by double-clicking documents as file associations are disabled.
- You cannot see the Tarantella Connection Manager tray icon.
- You have to use a specific printer for your printing tasks.

Are Client Group shortcuts any different from User shortcuts?

The administrator normally pushes a suitable client to a computer that is a part of a Client Group to create Client Group shortcuts on the computer.

When you try to launch a Client Group application, you are prompted for your User Name, Domain, and Password. You can launch the application only if the administrator has assigned the application to you either directly or indirectly.

The administrator can disable user shortcuts for Client Groups.

Client Groups and printers

The Administrator can add printers to a Client Group and the Client Group default printer overrides the client default printer.

The default printer is assigned to an application in the following order of priority:

1. Default printer in the Client Group
2. Default printer on the client
3. Any printer of Client Group
4. Any printer on the client
5. Default printer on the server

Client drive access

What is Internet File Sharing (IFS)?

Secure Global Desktop enables you to work with files from your local hard drive (to save or open the files) even though you are using these files with applications that reside on the servers. This Secure Global Desktop feature is called Internet File Sharing (IFS).

How does IFS drive lettering work?

The applications you use are running on the Application Servers and the drives you use may be located on your client computer. With this situation, the Secure Global Desktop server needs to identify the client drives on your desktop. To identify the drives, the operating system on the server assigns a drive letter to the drive on your client. The server assigns drive letters based on decisions made by your Secure Global Desktop administrator who establishes a range of valid drive letters. When saving a file to your local drive, you will see an alias name assigned to your drive. For example, when saving to your C: drive, you will see the following label, C on Client. C on Client represents your local C drive.

Why can there be an occasional delay or lag in saving and opening files?

Because your data files often reside on your client computer and the application runs from the server computer, you might notice a delay when you open a file. This delay might reflect the size of the file, the bandwidth used by the network connection, or some non-specific network latency. Nevertheless, in many instances you will experience no latency.

Printing

What printers does Secure Global Desktop support?

Secure Global Desktop allows you to print to any printer that is accessible from your client computer. Hence, if you can print to a printer from a local application, then you can print to that printer from a Secure Global Desktop server-based application.

Why are the printer names different from the original printer's names?

At any given time, multiple users can connect to the same Application Server. In order to recognize individual user's printers, Secure Global Desktop creates unique printer identifiers. To do this, Secure Global Desktop adds information to each printer's name.

Can jobs print with high quality color and high resolution?

Secure Global Desktop is unique in that it enables you to print images that have high quality color and high resolution to printers that support these capabilities. Secure Global Desktop does *not* limit the quality of your print jobs just because your applications are running from the server.

Can there be other loss of printer functionality, like print preview?

When using server-based applications via Secure Global Desktop, it is possible that you will see some missing functionality while printing. Specifically, print preview may not be accurate, the duplex printing might not work, and the paper-tray selection feature may not work. These limitations can exist when an administrator chooses to use only the Secure Global Desktop Unidriver, which is a proxy for the actual client printer driver. When your required vendor-specific driver is on the server and the administrator permits its use, you will not lose printer functionality.

Why are some print jobs different from their print previews?

When Secure Global Desktop does not have the actual client's vendor-specific printer driver on the server, Secure Global Desktop can still accommodate print preview requests. It does this by generating a print preview based on the Secure Global Desktop Universal printer driver. Later, when Secure Global Desktop executes the actual print job, it uses the client's actual vendor-specific printer driver. Because Secure Global Desktop displays and prints the jobs with different drivers, the actual print job may look different from the print preview. An administrator can eradicate this disparity by installing the client's vendor-specific printer driver on the server.

Disconnect and reconnect

What are the disconnect and reconnect features?

Secure Global Desktop enables you to disconnect from an application session without exiting the applications associated with that session. This feature keeps all of the applications associated with a session running on the server. It enables you to reconnect to the session and all the related applications later or from a different client computer. You can disconnect from an application session from the Launch Pad **Connections** page.

How is the disconnect feature influenced by idle time?

If the administrator sets an idle time property for disconnected sessions, then it can log off a disconnected session that remains idle for too long. For this reason, it is a good idea to perform a save on all application sessions before you place a terminal session in a disconnected state.

What is the remote connect feature?

The remote connect feature allows you to connect to your active sessions on other client computers without first disconnecting the sessions from the other computers. This is useful when you need to continue work from the previous session, but are not physically able to access the other client computer. You can remote connect to an application session from the Launch Pad **Connections** page.

Why can multiple applications exist in a single session?

Secure Global Desktop can run multiple applications in a single session to optimize performance. Moreover, Secure Global Desktop performs many functions at the session level rather than at the application level. For example, when you execute a session disconnect, all applications that are running in that session are disconnected. Conversely, when you reconnect to the session, all of that session's applications also become available.

Additionally, if you are running more than one session, you may notice that applications from one session remain available on your desktop after applications from a disconnected session disappear.

Idle Time

What is idle time?

Idle time, as used in Secure Global Desktop, is the time elapsed since the most recent transmission of a keystroke or mouse click from your computer to the server that is hosting your application session. Secure Global Desktop manages the duration of idle time to keep applications available for use and to ensure that applications are not considered busy when they are actually abandoned.

Your Secure Global Desktop administrator sets the idle time duration that defines an abandoned session. If you leave an application idle for that defined duration, then Secure Global Desktop terminates that application session. Before Secure Global Desktop terminates the session, it prompts you to save all of your work, and if you fail to save your work in response to this prompt; any unsaved data is lost.

In summary, an idle time property evaluates a period of inactivity between a Client and a WTS server. Idle time parameters exist, separately, for both active and disconnected sessions, and the idle time parameters can be of different durations. When a session is idle for a duration that exceeds the idle time, the WTS session terminates and all of a user's unsaved application data is lost.

What is the time-out property?

A time-out property evaluates a period of inactivity between a user/administrator and a Web page. Time-out parameters exist, separately, for both Secure Global Desktop Application Launch Pad

and Management Console Web pages, and time-out parameters can be different for both of these Web pages.

When a Web page times out, the user or administrator needs to restart a new browser, then visit Console or Launch Pad again, and then the user or administrator must re-enter his or her password in order to continue working with the Web page.

How do I keep from losing work due to idle time restrictions?

Similar to working with desktop applications, you can save your work manually and regularly, or if the application supports it, you can configure an application to save your work regularly and automatically. If you establish a practice that saves your work regularly, you may lose little or no data in the event of an idle time-out.

Shadowing

What is shadowing?

Shadowing is the ability of an administrator to view and control your session. Administrators can view any user's application session and guide that user through any problem.

Can you explain the shadowing prompt and its relevance?

A Shadowing prompt ensures that you are aware that your Secure Global Desktop administrator or a technical support representative wants to watch your session's behavior. Depending on the corporate privacy policy, this may or may not be of relevance.

Application Behavior

Do applications behave the same on different operating systems?

You may see some behavior that you do not understand and this may reflect the behavior of RDP in different Windows operating systems. If you always receive applications from the same Application Server or if all of the Application Servers run on the same operating system, you will see no difference in the way the application runs. However, if your site uses Application Servers that use different operating systems, you may notice differences in the way the application runs.

Attributes that may differ include:

- Icons
- The application's version
- Seamless windows
- Launch behavior and messages during launch
- Application Server not available message

The following explains why these differences appear.

For either a Secure Global Desktop or an RDP session, all the applications run on the server; only a picture (a bitmap) of the application, which is running on server, appears on the client. Hence, if

the Application Servers have different operating systems, then there may be certain differences in the behavior (look and feel) of the application on the client.

Additionally, if different versions of applications exist on different servers, then you will see a difference in the look and feel of the applications.

In addition, the file associations may be different between different application servers. For example, you run Outlook from application server 'A' and this server may open BMP file attachments using Microsoft Paint; however, you may later run Outlook from application server 'B' and this server may open BMP file attachments using PaintShopPro or PhotoShop.

Privacy

How can shadowing affect privacy?

Shadowing capabilities enable administrators to monitor your activities. When an administrator or technical support representative uses the Secure Global Desktop shadowing feature and attempts to shadow your session, you will receive a prompt to allow or deny the shadow request. The administrator will be able to shadow your session only if you allow it.

What management information does Secure Global Desktop log that relates to me?

Secure Global Desktop logs application usage information that it uses to generate business intelligence reports. It logs information like who used an application, at what time, for how long, and from which client computer. Administrators want this information so they can keep track of the number of application licenses that they require and they can avoid keeping too few or too many application licenses. Nonetheless, if you have questions about this, you can contact your Secure Global Desktop administrator.

Removing the Tarantella Client

Can I uninstall the Secure Global Desktop Client?

You can remove the Secure Global Desktop Client software by using the Microsoft Add/Remove Programs utility to remove the Tarantella Connection Manager program. However, if your client computer is running Windows 2003, Windows 2000, Windows XP, or Windows NT 4.0, you can uninstall the software only if you are an administrator on your computer.

Can I delete any leftover shortcuts?

When you uninstall the Tarantella Client, the client removes application shortcuts that it created on the client computer. If you created some shortcuts for Secure Global Desktop applications and did not use the Secure Global Desktop utilities provided to do this, Secure Global Desktop will not remove these shortcuts. If you find some unwanted shortcuts after Secure Global Desktop deletes the Tarantella Client, you can manually delete these shortcuts using the same standard windowing operations that you used to create them.

Can I delete the Secure Global Desktop browser cache?

For security purposes, you might also want to delete any temporary files from your browser.

Launch Pad Help

What's in this chapter?

This chapter provides an introduction to the Launch Pad and provides step-by-step procedures for installing the Tarantella Connection Manager, logging on to the Launch Pad, and using the Launch Pad. In addition, it lists some common useful abbreviations and their meanings.

Secure Global Desktop Launch Pad

This section consists of the following subsections.

["Introduction"](#)

["Installing the Tarantella Connection Manager"](#)

["Logging on to Secure Global Desktop Application Launch Pad"](#)

Introduction

When you first log on to the Secure Global Desktop Application Launch Pad, you see several options. This Secure Global Desktop Application Launch Pad introduction provides an overview of the organization of the Secure Global Desktop Application Launch Pad. This document addresses each of these subjects in detail later.

Favorites

The **Favorites** page provides a place to store the applications that you use frequently. This will represent a subset of all of the applications you can use.

Applications

The **Applications** page provides a place where you have access to all applications provisioned by the administrator.

Connections

The **Connections** page provides information on your active or disconnected sessions.

Options

The **Options** page enables you to customize the appearance and behavior of your version of the Secure Global Desktop Application Launch Pad.

Download Client

The **Download Client** page enables you to trigger a download of the Tarantella Connection Manager.

About

The **About** page provides information about the Secure Global Desktop version and build, and it provides Tarantella contact information.

Installing the Tarantella Connection Manager

To operate the Secure Global Desktop Application Launch Pad, you must have a Connection Manager on your client computer. You will receive the Connection Manager in one of two ways, depending on the preference of your Secure Global Desktop administrator. The Secure Global Desktop administrator can choose to push the Connection Manager to your computer or can choose to have you download the software.

If the Secure Global Desktop administrator pushes the software to your computer, the software will install when you reboot your PC.

If the Secure Global Desktop administrator has you download the software, you must have local administrative privileges.

From the Launch Pad:

1. Click **Download Client** from the navigation bar.
2. From the **Download Client** page, click **Download Now**.
3. Select a download option.
 - It may be best to select **Run this program from its current location** from the **File Download** dialog box and click **OK**.
 - You may choose the **Save this program to disk** option, download the file and then open the SGD-TSE-Client400.exe file, from the location to which you downloaded it to install the client.
4. On the **Welcome** panel of the Tarantella Connection Manager Installation Wizard, click **Next**.
5. From the **Destination Folder** panel, click **Browse** to choose a destination directory or accept the default setting. Click **Next**.
6. After installation, from the **Installation Complete** panel, click **Finish**.
7. If you are prompted to reboot, reboot the computer and connect back to the Launch Pad.
8. If you are not asked to reboot your client, click **Done** and the Launch Pad **Log On** page appears next.

Logging on to Secure Global Desktop Application Launch Pad

Your Secure Global Desktop administrator controls the appearance of your logon page. To logon to the Launch Pad:

1. On the **Log On** page, enter information in the following fields:
 - **Logon Name:** This is a mandatory field. Generally this is the logon name you use to logon to your domain. If you are having problems logging on, please contact your administrator.

 **NOTE**

*Do not enter the UPN name in the **Logon Name** field.*

- **Password:** This password belongs to the user that you specified in the Logon Name.
 - **Log on to:** This identifies the domain to which you belong. If you do not know your domain, ask your system administrator.
-

 **NOTE**

Cookies should be enabled to log on to the Launch Pad.

2. If your system administrator provides automatic logon privileges to you, you will see the **Automatically log on from this computer** check box on the **Log On** page. Select this option to log on from this PC in the future without typing your logon name and password.
 3. Click **Log On**.
-

 **NOTE**

*In order to receive the **Automatically log on from this computer** option, the Secure Global Desktop administrator must permit password persistence.*

Secure Global Desktop Application Launch Pad Pages

Favorites

Your Secure Global Desktop administrator regulates the appearance of this feature. If your Secure Global Desktop administrator permits you to use favorites, you will be able to see a **Favorites** link in the navigation bar, and you will be able to use the Favorites feature.

The favorites feature enables you to segregate your favorite applications from your general applications. The segregation enables you to create a smaller, more convenient set for everyday use.

You can view your favorite applications as you can in other Windows applications. You can list applications by icons, listing, or details. You set this preference on the **Options** page.

Applications

On the **Applications** page, you will always be able to view a listing of all of your applications.

You can view your applications as you can in other Windows applications. You can list applications by icons, listing, or details. You set this preference on the **Options** page.

Connections

This page lists the connections that you are running.

Each connection you establish appears on a separate row of the **Active Connections** or **Disconnected Connections** table. For example, if you see three rows on the **Disconnected Connections** table, then your system is managing three terminal sessions.

Each terminal session may run more than one application, and session affinity, will encourage applications to launch in the same session whenever possible.

Two situations may make this not possible:

- If a terminal session is in a disconnected state, Secure Global Desktop will add no more application sessions to that session
- If an application you require is only available on a terminal server other than the terminal server that hosts your current session, then a new terminal server session will host that application.

Options

Your Secure Global Desktop administrator regulates the appearance of this feature. Your Secure Global Desktop administrator may permit you to change the properties of the following objects.

Favorites Page

The Secure Global Desktop administrator may permit you to use this. If you can use this page, you can customize the appearance of the application entries on the page. The applications can appear as icons, a simple list, or a detailed list.

Application Page

You can always see this page. You can customize the appearance of the application entries on the page. The applications can appear as icons, a simple list, or a detailed list.

Connection Settings

Your Secure Global Desktop administrator can build several connection setting profiles and can designate one profile to be the Default profile.

You can select one specific connection profile or you can select the default profile. The default profile becomes a somewhat dynamic profile. This profile changes automatically when the Secure Global Desktop administrator selects a new profile to be a default profile. Therefore, if the environment in which Secure Global Desktop runs changes and the Secure Global Desktop administrator changes the connection settings to optimize the performance of Secure Global Desktop, then those who have a Default connection setting will have their connection settings updated automatically.

Reconnect on Launch

Your Secure Global Desktop administrator controls the Reconnect on Launch feature and the way it operates in the Enterprise. The Secure Global Desktop administrator may permit you to use the Reconnect on Launch feature.

This is how the Reconnect on Launch feature works.

When you launch an application from the **Favorites** or the **Applications** page of the Launch Pad, the value of the reconnect option determines whether to reconnect a disconnected session (that has the same application) or to restart a new application session. For example, if you have a disconnection Word session and you click on a Word icon to launch the application; this action triggers the reconnect decision.

If the launch reconnects the disconnected session, then all applications associated with that session are reconnected. For example, if the disconnected session had one copy of a Word document, one copy of a Visio document, and one copy of an Excel document, then the reconnected session would make the Word, Visio, and Excel documents available.

Where you Launch your Applications

You can launch your application from the Application Launch Pad, from a Desktop Shortcut, from the Start menu, or by double-clicking a file that has file association to an application to Application Servers. Clicking an application name in this area, displays the application details, including the file associations for the application.

Download Client

You can receive a client in one of two ways, you may download and install the client or the Secure Global Desktop administrator may push the client to your computer.

In order to download and install a client, you must have Administrator privileges on your client computer.

If you have Administrator privileges on your computer, click **Download**, select the **Run this program from its current location** option, and click **OK**. Follow the instructions in the dialog boxes to complete the installation. For more information, refer to "[Installing the Tarantella Connection Manager](#)".

If you do not have Administrator privileges on your computer, ask the Secure Global Desktop administrator to push the Tarantella Client to the User computers. Because the Secure Global Desktop administrator has Administrator privileges, the administrator can execute this install.

About

You can see the version and build number of your Secure Global Desktop product on this page. You can also see how to contact Tarantella technical support or sales groups.

Tarantella Connection Manager

The Tarantella Connection Manager appears on the Windows task bar in the system tray. You may see the Windows clock in this same area. When your cursor hovers above the icon, you will see the Tarantella Connection Manager name.

The Tarantella Connection Manager works with a right-click on your mouse. It does not work with a left click.

This section discusses the actions you can trigger when you right click on the Tarantella Connection Manager.

Go to <Team Name>

This feature will take you to the Launch Pad associated with that Team Name.

Refresh shortcuts and file associations

This feature enables you to refresh all of your shortcuts and file associations conveniently, on demand.

NOTE

When you log on to a session, Secure Global Desktop automatically refreshes your shortcuts and file associations.

Delete all client settings

This feature deletes all Secure Global Desktop created shortcuts from your desktop and from your Start menu. It also deletes the file associations from the registry.

Disconnect all sessions

This feature puts all current sessions in disconnected state.

Logoff all sessions

This feature exits all your application sessions from both the client and the server.

Exit

This allows you to exit the Tarantella Connection Manager.

Troubleshooting

What's in this chapter?

This chapter explains the troubleshooting steps and answers your queries on some common issues.

Errors and common queries

This section deals with the following issues.

- ["Logon fails with "null" error"](#)
- ["Launch Pad Favorites page is not displayed"](#)
- ["Corrupt installation detected error"](#)
- ["IFS error"](#)
- ["Launch Failed error"](#)
- ["Load Balancing Failed error"](#)
- ["Correct icons not displayed"](#)
- ["Unable to launch applications"](#)
- ["Tarantella Connection Manager icon"](#)
- ["Application prompts for password"](#)
- ["Application shortcuts"](#)
- ["Netscape error"](#)
- ["IE setting for SharePoint server"](#)
- ["Unable to launch applications on Windows 95"](#)
- ["Security settings error"](#)

Logon fails with "null" error

Issue

Logon to Launch Pad fails with "null" error.

Symptom

The Launch Pad displays "null" error when you try to logon to the Launch Pad.

Cause

One of the reasons this happens is when you try to logon to the Launch Pad after the administrator deletes you as a user from the domain, and then adds a user with the same logon name to the domain.

Resolution

Contact the administrator.

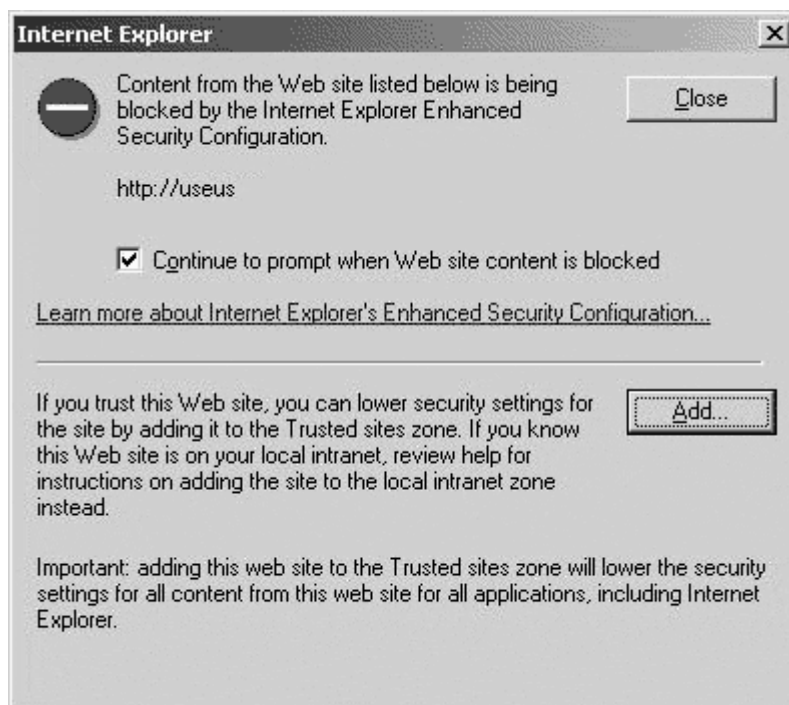
Launch Pad Favorites page is not displayed

Issue

Launch Pad Favorites page is not displayed after logon.

Symptom

Using Internet Explorer 6.0 on Windows 2003, when you access the Launch Pad Web site, the following window appears.



If you click **Close**, you are able to access the **Log On** page. However, after logon, the **Favorites** page appears blank.

Cause

This is due to the Internet Explorer Enhanced Security Configuration setting.

Resolution

Remove the enhanced security setting from the client computer. To do this:

1. Close the browser window.
2. Select **Start>Control Panel>Add/Remove Programs>Add/Remove Windows Components**.

3. Clear the **Internet Explorer Enhanced Security Configuration** check box.
4. Click **Next**.
5. Log on again to the Launch Pad.

Alternatively, if the Internet Explorer Enhanced Security Configuration setting is in accordance with the organizational policy, click **Add** on the window that appears when you access the Launch Pad Web site to add the site to the Trusted Sites list.

! NOTE

This problem also occurs when you launch a provisioned Internet Explorer application on an Application Server with Internet Explorer Enhanced Security Configuration setting. In that case, contact the administrator.

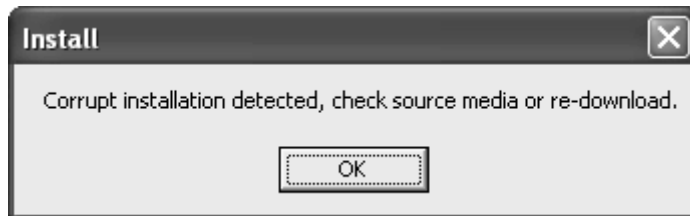
Corrupt installation detected error

Issue

Install error window displays while downloading client software.

Symptom

When attempting to download and install the Client from the Secure Global Desktop Applications Launch Pad, the process fails and you get an Install error sometimes.



Cause

This may happen if you try to run the program from its current location.

Resolution

You should download the software by saving it on the your computer, and then run SGD-TSE-Client400.exe to install the client software.

IFS error

Issue

File associations are not working even though I have enabled them.

Symptom

The following message box is displayed when you try to open a document with file association.



Cause

This error message appears if Secure Global Desktop IFS is not running, or if the RDP IFS is enabled. For file associations to work, the connection settings for the application should be such that they allow IFS.

Resolution

Contact your administrator.

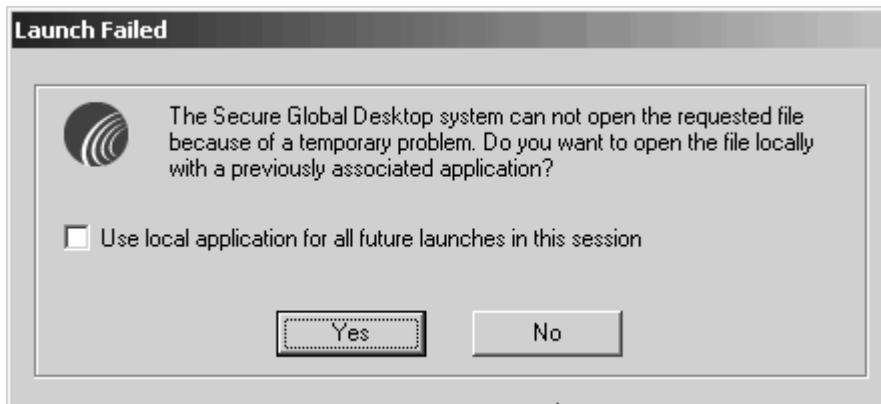
Launch Failed error

Issue

Application launch fails while opening a file with file associations.

Symptom

The following message box is displayed when you try to open a document with file association.



Cause

This error message appears if the file association does not exist on the Application Server.

Resolution

You can choose to open the file with another application on the Server, or open a local application for the current session.

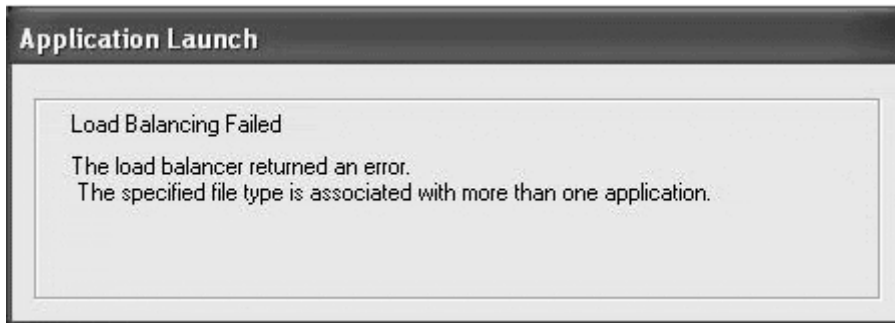
Load Balancing Failed error

Issue

Application launch fails while opening a file with file associations.

Symptom

The following message box is displayed when the user tries to open a document with file association.



Cause

The administrator has changed file associations.

Resolution

Contact your administrator.

Correct icons not displayed

Issue

The correct icons according to file associations are not displayed.

The correct icons are not displayed for the documents after removing file association for documents for an application.

Cause

This is standard Windows behavior after changing icons.

Resolution

1. Press **Ctrl+Alt+Del** and click **Task Manager**.
2. Click the **Processes** tab.
3. Select **explorer.exe** and click **End Process**.
4. Click **Start>Run**.
5. Type **explorer** in the **Open** field and click **OK**. The correct icons should now be displayed.

Unable to launch applications

Issue

Unable to license application sessions.

Symptom

A message box appears with the “Unable to license application sessions error”.

Cause

The base key may have expired and the administrator has not activated the system using the Activation Key, or the number of licenses for the application are exceeded.

Resolution

Contact the Administrator.

Tarantella Connection Manager icon

Issue

Tarantella Connection Manager tray icon not visible.

Symptom

Tarantella Connection Manager tray icon is not visible on the Task bar even when connected to the Launch Pad, though Secure Global Desktop shortcuts are present.

Explanation

The administrator may have made the client computer a part of a Client Group and hidden the icon.

Solution

Contact the Secure Global Desktop administrator, this is as designed.

Application prompts for password

Issue

Application prompts for password to unlock computer.

Symptom

If you launch an application through Secure Global Desktop, when you return to the application after some time, either the **Unlock Computer** window or a blank screen may be displayed.

Cause

This happens as the server is locked down if after launching applications from a Windows Server 2003 Application Server, you leave a session remain idle for a considerable amount of time — may be about 10 minutes, depending upon the settings on the server.

Resolution

In the **Password** field of the **Unlock Computer** window, enter your password and click **OK**. If a blank screen is displayed, click on the blank screen, type the password, and press **Enter**. The application is displayed as before the server was locked down.

Application shortcuts

Issue

There are some extra shortcuts on the Windows start menu and desktop.

My shortcuts are not created.

Symptom

You can see some shortcuts that are not visible on the Launch Pad Applications and Favorites pages. When you try to launch these applications you are unable to launch them even after you enter your User Name, Password, and Domain in the authentication dialog box.

You have enabled shortcuts for applications visible on the Launch Pad but shortcuts are not created.

Explanation

These are not your application shortcuts, but Client Group shortcuts that are created as the computer you are using is part of a Client Group. If the Client Group applications are not assigned to you as a user, either directly or indirectly, you will not be able to launch them.

Your shortcuts are not created on the computer as the administrator has disabled them for the Client Group to which your client computer belongs.

Solution

Contact your system administrator.

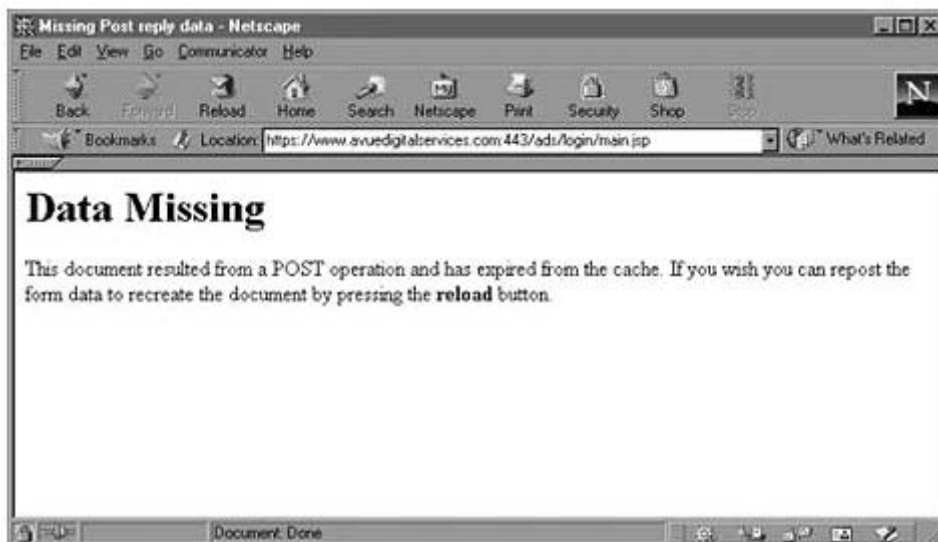
Netscape error

Issue

Some operations in Launch Pad when using Netscape Browser show “Data Missing” error.

Symptom

The following error is displayed forcing you to click **Reload**.



Cause

This is due to the memory cache setting in Netscape.

Resolution

Increase the memory cache setting in Netscape to prevent this error from recurring.

Launch the Netscape browser.

1. Select **Edit>Preferences**. The **Preferences** window appears.
2. In the left pane, expand **Advanced**, and select **Cache**.
3. In the **Memory Cache** field, enter a higher value.
4. Click **OK**.

IE setting for SharePoint server

Issue

Cannot log on to Launch Pad Web part in SharePoint Portal Server.

Symptom

Even after entering correct credentials on the Logon page, you are not able to logon to Launch Pad Web part in SharePoint Portal Server and are returned to the Logon page.

Cause

Internet Explorer settings on your computer do not allow third party cookies.

Resolution

Open Internet Explorer and change settings to allow third party cookies by changing either the Privacy settings or the Security settings.

Changing Privacy Settings

1. Select **Tools>Internet Options**.
2. Click the **Privacy** tab.
3. Move the **Privacy Preferences** slider down to set the privacy level for Internet to **Low**.
4. Click **OK** to allow all third party cookies.

Changing Security Settings

1. Select **Tools>Internet Options**.
2. Click the **Security** tab.
3. Select **Trusted Sites** Web content zone and click **Sites** to open the **Trusted sites** window.
4. In the **Add this Web site to the zone** field, enter the domain or IP address of the Launch Pad Web site.

 **NOTE**

You can contact the Secure Global Desktop administrator to get this IP address.

5. Click **Add** to add the site and then click **OK** to exit the **Trusted sites** window.
6. Click **Custom Level** to open the **Security Settings** window.
7. In the **Reset custom settings** area, select **Low** from the **Reset to** list.
8. Click **OK** to exit the **Security Settings** window.
9. Click **OK** to save the settings.

Unable to launch applications on Windows 95

Issue

Unable to launch applications from a client computer that has Windows 95.

Symptom

When you launch an application from a computer with Windows 95, you get the "Talking to Load Balancer" message, but the message disappears and no application is launched.

Cause

This happens because you need WS2_32.dll to launch applications and this dll is not installed with Windows 95. WS2_32.dll has a dependency on WS2help.dll; that should also be present on the computer.

Resolution

Download WS2_32.dll and WS2help.dll from the Microsoft Web site or any other Web site. You can also upgrade the Internet Explorer.

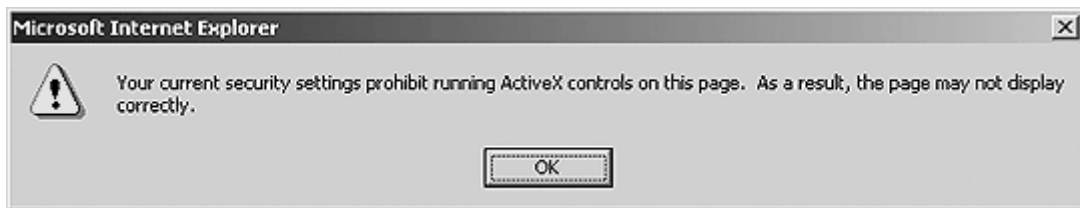
Security settings error

Issue

Insufficient rights, security settings of browser.

Symptom

The following message box is displayed when you try to launch the Launch Pad.



Cause

This is because of the security settings of the browser.

Resolution

Make the appropriate security settings.

1. Open the Internet Explorer.
2. Select **Tools>Internet Options**, and click the **Security** tab.
3. Click **Custom Level** and for **Scripting of Java applets** security setting, select the **Enable** option.
4. Click **OK**.

About Us

What's in this chapter?

This chapter provides information about Tarantella Inc. and Secure Global Desktop.

About Tarantella

Tarantella, Inc. (NASDAQ:TTLAE) is a leading provider of purpose-built application access and deployment software to nearly 12,000 customers' sites worldwide. Tarantella enables organizations to access and manage information, data and applications across all platforms, networks and devices. Tarantella bridges the gap between vendors, ensuring that customers have complete access to business-critical information. Using Tarantella's software, customers realize the benefits of secure corporate data, maximizing return on existing IT assets and improved productivity. The company markets its products through key industry partnerships and a worldwide network of consultants and resellers. Tarantella is headquartered in Santa Cruz, Calif.

About Secure Global Desktop from Tarantella

Secure Global Desktop makes central deployment and management of server-based Windows applications simple, intelligent, and cost effective. Serving both enterprises and service providers, Secure Global Desktop increases the efficiency of IT operations and improves business performance.

Other sources of information

You can find more information, as follows:

TABLE 5. Sources of information and their availability

Source	Availability
Tarantella Inc.	+1 831 427 7222
Technical Support Center	Visit www.tarantella.com/support
Local Sales Office	Visit http://www.tarantella.com/about/offices/
Email to Tarantella	info@tarantella.com
Tarantella on the Web	http://www.tarantella.com

Abbreviations

What's in this appendix?

This appendix lists some common relevant abbreviations.

Abbreviations

This section addresses the abbreviations that appear in this guide. Most of the abbreviations relate to Microsoft technologies, communications protocols, or other technologies. Many administrators are familiar with these abbreviations.

TABLE 6. Abbreviations

Abbreviation	Meaning
ADSI	Active Directory Service Interfaces
API	Application Programming Interface
ASP	Active Server Pages
COM	Component Object Model
DCOM	Distributed COM
HTML	Hypertext Markup Language
IFS	Internet File Sharing
IT	Information Technology
NAT	Network Address Translator
NTLM	NT LAN Manager
MTS	Microsoft Transaction Server
OLE	Object Linking and Embedding
OU	Organizational Unit
PC	Personal Computer
RDP	Remote Desktop Protocol
SMB	Server Message Block
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
UI	User Interface
UPN	User Principal Name

TABLE 6. Abbreviations

Abbreviation	Meaning
WMI	Windows Management Instrumentation
XML	Extensible Markup Language